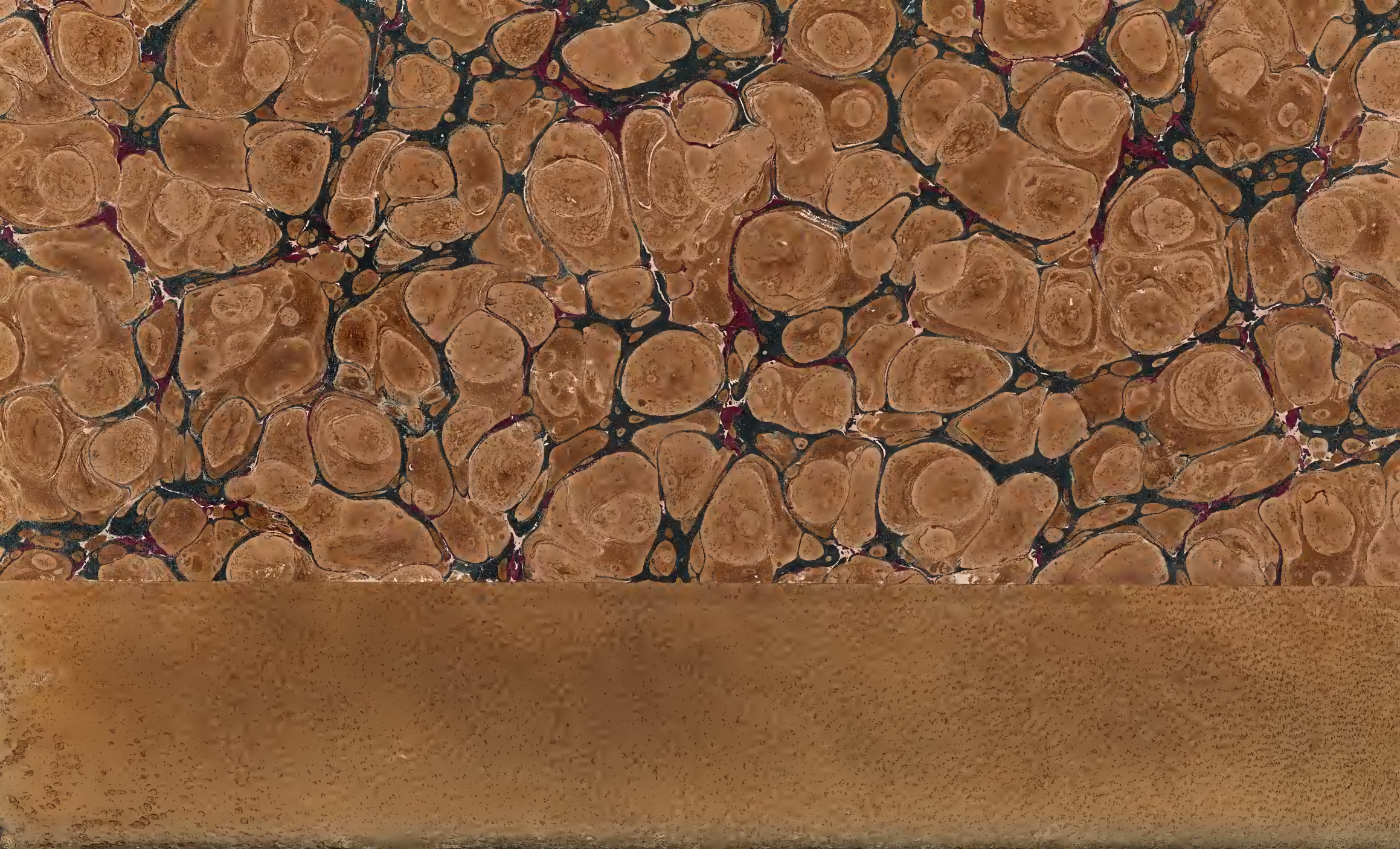
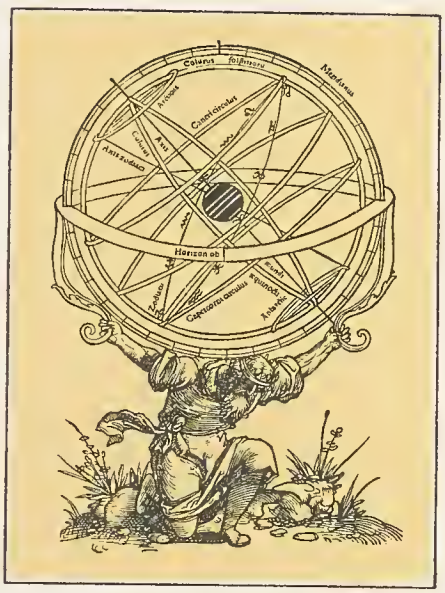


Very rare first edition!

The Dibner Library
of the History of
Science and Technology

SMITHSONIAN INSTITUTION LIBRARIES



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

SERENISSIMO

PRINCIPI AC DOMINO

CAROLO GVILIELMO FERDINANDO

BRVNOVICENSIVM AC LVNEBVRGENSIVM

DVCI

PRINCEPS SERENISSIME

Summae equidem felicitati mihi duco, quod Celsissimo nomini *Tuo* hoc opus inscribere mihi permittis, quod vt *Tibi* offeram sancto pietatis officio obstringor. Nisi enim *Tua* gratia, Serenissime Princeps, introitum mihi ad scientias primum aperuisset, nisi perpetua *Tua* beneficia studia mea vsque sustentauissent, scientiae mathematicae, ad quam vehementi semper amore delatus sum, totum me deuouere non potuissem. Quin adeo eas ipsas meditationes, quarum partem hoc volumen exhibet, vt suscipere, per plures annos continuare literisque consignare liceret, *Tua* sola benignitas effecit, quae vt, ceterarum curarum expers, huic imprimis incumbere possem praestitit. Quas quum tandem in lucem emittere cuperem, *Tua* munificentia cuncta, quae editionem remorabantur, obstacula remouit. Haec *Tua* tanta de me meisque conatibus merita gratissima potius mente tacitaque admiratione reuoluere, quam iustis dignisque laudibus celebrare

possum. Namque non solum tali me muneri haud parem sentio, sed et neminem ignorare puto, solennem *Tibi* esse tam insignem liberalitatem in omnes qui ad optimas disciplinas excolendas conferre videntur, neque eas scientias, quae vulgo abstrusiores et a vitae communis vtilitate remotiores creduntur, a patrocinio *Tuo* exclusas esse, quum *Tu* ipse intimum scientiarum omnium inter se et necessarium vinculum mente illa sapientissima omniumque quae ad humanae societatis prosperitatem augendam pertinent peritissima, penitus perspexeris. Quodsi *Tu*, Princeps Serenissime, hunc librum, et gratissimi in *Te* animi et laborum nobilissimae scientiae dicatorum testem, insigni illo fauore, quo me tamdiu amplexus es, haud indignum iudicaueris, operam meam me non inutiliter collocasse, eiusque honoris, quem prae omnibus in votis habui, compotem me factum esse, mihi gratulabor

PRINCEPS SERENISSIME

Brunouici mense Julio 1801.

Celsitudinis Tuae
seruus addictissimus
C. F. Gauss.

PRAEFATIO

Disquisitiones in hoc opere contentae ad eam Matheseos partem pertinent, quae circa numeros integros versatur, fractis plerumque, surdis semper exclusis. Analysis indeterminata quam vocant seu Diophantaea, quae ex infinitis solutionibus problemati indeterminato satisfacientibus eas seligere docet, quae per numeros integros aut saltem rationales absoluuntur (plerumque ea quoque conditione adiecta vt sint positiui) non est illa disciplina ipsa, sed potius pars eius valde specialis, ad eamque ita fere se habet, vt ars aequationes reducendi et soluendi (Algebra) ad vniuersam Analysin. Nimirum quemadmodum ad *Analyseos* ditionem referuntur omnes quae circa quantitatum affectiones generales institui possunt disquisitiones: ita numeri integri (fractique quatenus per integros determinantur) obiectum proprium ARITHMETICAE constituunt. Sed quum ea, quae Arithmetices nomine vulgo traduntur, vix vltra artem numerandi et calculandi (i. e. numeros per signa idonea e. g. secundum systema decadicum exhibendi, operationesque arithmeticas perficiendi) extendantur, adiectis nonnullis quae vel ad Arithmeticam omnino non pertinent (vt doctrina de logarithmis) vel saltem

numeris integris non sunt propria sed ad omnes quantitates patent: e re esse videtur, duas Arithmeticae partes distinguere, illaque ad Arithmeticam elementarem referre, omnes autem disquisitiones generales de numerorum integrorum affectionibus propriis *Arithmeticae Sublimiori*, de qua sola hic sermo erit, vindicare.

Pertinent ad Arithmeticam Sublimiorem ea, quae Euclides in Elementis L. VII sqq. elegantia et rigore apud veteres consuetis tradidit: attamen ad prima initia huius scientiae limitantur. Diophanti opus celebre, quod totum problematis indeterminatis dicatum est, multas quaestiones continet, quae propter difficultatem suam artificiorumque subtilitatem de auctoris ingenio et acumine existimationem haud mediocrem suscitant, praesertim si subsidiorum quibus illi vti licuit tenuitatem consideres. At quum haec problemata dexteritatem quandam potius scitamque tractationem, quam principia profundiora postulent, praetereaque nimis specialia sint raroque ad conclusiones generaliores deducant: hic liber ideo magis epocham in historia Matheseos constituere videtur, quod prima artis characteristicae et Algebrae vestigia sistit, quam quod Arithmeticam Sublimiorem inuentis nouis auxerit. Longe plurima recentioribus debentur, inter quos pauci quidem sed immortalis gloriae viri P. DE FERMAT, L. EVLER, L. LA GRANGE, A. M. LE GENDRE (vt paucos alios praetream) introitum ad penetralia huius diuinae scientiae aperuerunt, quantisque diuitiis abundent patefecerunt. Quaenam vero inuenta a singulis his geometris profecta

sint, hic enarrare supersedeo, quum e praefationibus Additamentorum quibus ill. La Grange Euleri Algebram ditauit operisque mox memorandi ab ill. Le Gendre nuper editi cognosci possint, insuperque pleraque locis suis in his Disquisitionibus Arithmeticis laudentur.

Propositum huius operis, ad quod edendum iam annos abhinc quinque publice fidem dederam, id fuit, vt disquisitiones ex Arithmetica Sublimiori, quas partim ante id tempus partim postea institui, diuulgarem. Ne quis vero miretur, scientiam hic a primis propemodum initiis repetitam, multasque disquisitiones hic denuo resumtas esse, quibus alii operam suam iam nauarunt, monendum esse duxi, me, quum primum initio a. 1795 huic disquisitionum generi animum applicaui, omnium quae quidem a recentioribus in hac arena elaborata fuerint ignarum, omniumque subsidiorum per quae de his quidpiam comperire potuissem expertem fuisse. Scilicet in alio forte labore tunc occupatus, casu incidi in eximiam quandam veritatem arithmeticam (fuit autem ni fallor theorema art. 108), quam quum et per se pulcherrimam aestimarem et cum maioribus connexam esse suspicarer, summa qua potui contentione in id incubui, vt principia quibus inniteretur perspicerem, demonstrationemque rigorosam nanciscerer. Quod postquam tandem ex voto successisset, illecebris harum quaestionum ita fui implicatus, vt eas deserere non potuerim; quo pacto, dum alia semper ad alia viam sternebant, ea quae in quatuor primis Sectionibus huius operis traduntur ad maxi-

mam partem absoluta erant, antequam de aliorum geometrarum laboribus similibus quidquam vidissem. Dein copia mihi facta, horum summorum ingeniorum scripta euoluendi, maiorem quidem partem meditationum mearum rebus dudum transactis impensam esse agnoui: sed eo alacrior, illorum vestigiis insistens, Arithmeticam vlterius excolere studui; ita variae disquisitiones institutae sunt, quarum partem Sectiones V, VI et VII tradunt. Postquam interiecto tempore consilium de fructibus vigiliarum in publicum edendis cepi: eo lubentius, quod plures optabant, mihi persuaderi passus sum, ne quid vel ex illis inuestigationibus prioribus supprimerem, quod tum temporis liber non habebatur, ex quo aliorum geometrarum labores de his rebus, in Academiarum Commentariis sparsi, edisci potuissent; quod multae ex illis omnino nouae et pleraeque per methodos nouas tractatae erant; denique quod omnes tum inter se tum cum disquisitionibus posterioribus tam arcto nexu cohaerebant, vt ne noua quidem satis commode explicari possent, nisi reliquis ab initio repetitis.

Prodiit interea opus egregium viri iam antea de Arithmetica Sublimiori magnopere meriti, *Le Gendre Essai d' une theorie des nombres, Paris a. VI*, in quo non modo omnia quae hactenus in hac scientia elaborata sunt diligenter collegit et in ordinem redegit, sed permulta insuper noua de suo adiecit. Quum hic liber serius ad manum mihi peruenerit, postquam maxima operis pars typis iam exscripta esset; nullibi, vbi rerum analogia occasionem dare potuisset,

eius mentionem iniicere licuit; de paucis tantummodo locis quaedam obseruationes in Additamentis adiungere necessarium videbatur, quas vir humanissimus et candidissimus benigne vt spero interpretabitur.

Inter impressionem huius operis, quae pluries interrupta variisque impedimentis vsque in quartum annum protracta est, non modo eas inuestigationes, quas quidem iam antea susceperam, sed quarum promulgationem in aliud tempus differre constitueram, ne liber nimis magnus euaderet, vlterius continuaui, sed plures etiam alias nouas aggressus sum. Plures quoque, quas ex eadem ratione leuiter tantum attigi, quum tractatio vberior minus necessaria videretur (e. g. eae quae in artt. 37, 82 sqq. aliisque locis traduntur), postea resumtae sunt, disquisitionibusque generalioribus quae luce perdignae videntur locum dederunt (Conf. etiam quae in Additamentis de art. 306 dicuntur). Denique quum liber praesertim propter amplitudinem Sect. V in longe maius quam exspectaueram volumen excresceret, plura quae ab initio ei destinata erant, interque ea totam Sectionem *octauam* (quae passim iam in hoc volumine commemoratur, atque tractationem generalem de congruentiis algebraicis cuiusuis gradus continet) resecare oportuit. Haec omnia, quae volumen huic aequale facile explebunt, publici iuris fient, quamprimum occasio aderit.

Quod, in pluribus quaestionibus difficilibus, demonstrationibus syntheticis vsus sum, analysinque per quam erutae sunt suppressi, imprimis

breuitatis studio tribuendum est, cui quantum fieri poterat consulere oportebat.

Theoria diuisionis circuli, siue polygonorum regularium, quae in Sect. VII tractatur, *ipsa* quidem *per se* ad Arithmeticam non pertinet, attamen eius *principia* vnice ex Arithmetica Sublimiori petenda sunt: quod forsan geometris tam inexspectatum erit, quantum veritates nouas, quas ex hoc fonte haurire licuit, ipsis gratas fore spero.

Haec sunt, de quibus lectorem praemonere volui. De rebus ipsis non meum est iudicare. Nihil equidem magis opto, quam vt iis, quibus scientiarum incrementa cordi sunt, placeant, quae vel hactenus desiderata explent, vel aditum ad noua aperiunt.

CONTENTA

DISQVISITIONES ARITHMETICAE

SECTIO PRIMA

DE

NVMERORVM CONGRVENTIA IN GENERE.

1. Si numerus a numerorum b, c differentiam metitur, b et c *secundum* a *congrui* dicuntur, sin minus, *incongrui*: ipsum a *modulum* appellamus. Vterque numerorum b. c, priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur.

Hae notiones de omnibus numeris integris tam positiuis quam negatiuis *) valent, neque

*) Modulus manifesto semper *absolute* i. e. sine omni signo est sumendus.

vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2. Omnia numeri dati a residua secundum modulum m sub formula $a+km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post tradenuus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quiuis intuendo poterit perspicere.

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum vbi opus erit in clausulis adiungentes, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$ *).

3. Theor. *Propositis m numeris integris successiuis, a, $a+1$, $a+2 \ldots a+m-1$, alioque A, illorum aliquis huic secundum modulum m congruus erit, et quidem vnicus tantum.*

Si enim $\frac{A-a}{m}$ integer, erit $a \equiv A$, sin fractus, sit integer proxime maior, (aut quando est negatiuus, proxime *minor*, si ad signum non respiciatur) $= k$, cadetque $A+km$ inter a et

*) Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam inuenitur adoptauimus. Ob eandem cauſsam ill. Le Gendre in comment. infra saepius laudanda ipsum aequalitatis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur limitari dubitauimus.

$a + m$, quare erit numerus quaesitus. Et manifestum est omnes quotientes $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$ etc. inter $k-1$ et $k+1$ sitos esse; quare plures quam vnus integri esse nequeunt.

4. Quisque igitur numerus residuum habebit tum in hac serie, $0, 1, 2, \ldots m-1$, tum in hac, $0, -1, -2, \ldots -(m-1)$, quae *residua minima* dicemus, patetque, nisi 0 fuerit residuum, bina semper dari, *positiuum* alterum, alterum *negatiuum*. Quae si magnitudine sunt inaequalia, alterum erit $< \frac{m}{2}$, sin secus vtrumque $= \frac{m}{2}$, signi repectu non habito. Vnde patet, quemuis numerum residuum habere moduli semissem non superans quod *absolute minimum* vocabitur.

E. g. -13 secundum modulum 5, habet residuum minimum positiuum 2, quod simul est absolute minimum, -3 vero residuum minimum negatiuum; $+5$ secundum modulum 7 sui ipsius est residuum minimum positiuum, -2 negatiuum, simulque absolute minimum.

5. His notionibus stabilitis eas numerorum congruorum proprietates quae prima fronte se offerunt colligamus.

Qui numeri secundum modulum compositum sunt congrui, etiam secundum quemuis eius diuisorem congrui.

Si plures numeri eidem numero secundum eundem modulum sunt congrui, inter se erunt congrui (secundum eundem modulum).

Haec modulorum identitas etiam in sequentibus est subintelligenda.

Numeri congrui residua minima habent eadem, incongrui diuersa.

6. *Si habentur quotcunque numeri A, B, C, etc. totidemque alii a, b, c, etc. illis secundum modulum quemcunque congrui, $A \equiv a$, $B \equiv b$,* etc. *erit* $A + B + C +$ *etc.* $\equiv a + b + c +$ *etc.*

Si $A \equiv a$, $B \equiv b$ *erit* $A - B \equiv a - b$.

7. *Si* $A \equiv a$, *erit quoque* $kA \equiv ka$.

Si k numerus positiuus, hoc est tantummodo casus particularis propos. art. praec., ponendo ibi $A = B = C$ etc., $a = b = c$ etc. Si k negatiuus, erit $-k$ positiuus, adeoque $-kA \equiv -ka$, vnde $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, *erit* $AB \equiv ab$. Namque $AB \equiv Ab \equiv ba$.

8. *Si habentur quotcunque numeri A, B, C, etc. totidemque alii a, b, c etc. his congrui,* $A \equiv a$, $B \equiv b$ *etc. producta ex vtrisque erunt congrua,* ABC *etc.* $\equiv abc$ *etc.*

Ex artic. praec. $Ab \equiv ab$, et ob eandem rationem $ABC \equiv abc$; eodemque modo quotcunque alii factores accedere possunt.

Si omnes numeri A, B, C, etc. aequales assumuntur, nec non respondentes a, b, c, etc. habetur hoc theorema: *Si* $A \equiv a$ *et* k *integer positiuus, erit* $A^k \equiv a^k$.

9. *Sit X functio algebraica indeterminatae x, huius formae,* $Ax^a + Bx^b + Cx^c +$ *etc. designantibus A, B, C, etc. numeros integros quoscunque; a, b, c, etc. vero integros non negatiuos. Tum si indeterminatae x valores secundum modulum quemcunque*

congrui tribuuntur, valores functionis X inde prodeuntes congrui erunt.

Sint f, g, valores congrui ipsius x. Tum ex art. praec. $f^a \equiv g^a$ et $Af^a \equiv Ag^a$, eodemque modo $Bf^b \equiv Bg^b$ etc. Hinc $Af^a + Bf^b + Cf^c +$ etc. $\equiv Ag^a + Bg^b + Cg^c +$ etc. *Q. E. D.*

Ceterum facile intelligitur, quomodo hoc theorema ad functiones plurium indeterminatarum extendi possit.

10. Quodsi igitur pro x omnes numeri integri consecutiui substituuntur, valoresque functionis X ad residua minima reducuntur, haec seriem constituent, in qua post interuallum m terminorum (designante m modulum) iidem termini iterum recurrunt; siue haec series ex *periodo* m terminorum infinities repetita, erit formata. Sit e. g. $X = x^3 - 8x + 6$ et $m = 5$; tum pro $x = 0, 1, 2, 3$ etc., valores ipsius X haec residua minima positiua suppeditant, 1, 4, 3, 4, 3, 1, 4, etc., vbi quina priora 1, 4, 3, 4, 3 in infinitum repetuntur; atque si series retro continuatur, i. e. ipsi x valores negatiui tribuuntur, eadem periodus ordine terminorum inuerso prodit; vnde manifestum est, terminos alios quam qui hanc periodum constituant in tota serie locum habere non posse.

11. In hoc igitur exemplo X neque $\equiv 0$, neque $\equiv 2$ (mod. 5) fieri potest, multoque minus $= 0$, aut $= 2$. Vnde sequitur, aequationes $x^3 - 8x + 6 = 0$, et $x^3 - 8x + 4 = 0$ per numeros integros et proin, vti notum est, per numeros rationales solui non posse. Ge-

neraliter perspicuum est, aequationem $X = 0$, quando X functio incognitae x, huius formae, $x^n + Ax^{n-1} + Bx^{n-2} +$ etc. $+ N$; A, B, C, etc. integri, atque n integer positiuus, (ad quam formam omnes aequationes algebraicas reduci posse constat) radicem rationalem nullam habere, si congruentiae $X \equiv 0$ secundum vllum modulum satisfieri nequeat. Sed hoc criterium, quod hic sponte se nobis obtulit, in *sect. VIII* fusius pertractabitur. Poterit certe ex hoc specimine notiuncula qualiscunque de harum inuestigationum vtilitate efformari.

12. Theorematibus in hoc capite traditis complura quae in arithmeticis doceri solent innituntur, e. g. regulae ad explorandam diuisibilitatem numeri propositi per 9, 11 aut alios numeros. *Secundum modulum* 9 omnes numeri 10 potestates vnitati sunt congruae: quare si numerus propositus habet formam $a + 10\,b + 100\,c +$ etc., idem residuum minimum secundum modulum 9 dabit, quod $a + b + c +$ etc. Hinc manifestum est, si figurae singulae numeri decadice expressi sine respectu loci quem occupant addantur, summam hanc numerumque propositum eadem residua minima praebere, adeoque hunc per 9 diuidi posse, si illa per 9 sit diuisibilis, et contra. Idem etiam de diuisore 3 tenendum. Quoniam *secundum modulum* 11, $100 \equiv 1$ erit generaliter $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, et numerus formae $a + 10\,b + 100\,c +$ etc. secundum modulum 11 idem residuum minimum dabit quod $a - b + c$ etc.; vnde regula nota protinus deriuatur. Ex eo-

dem principio omnia similia praecepta facile deducuntur.

Nec minus ex praecedentibus petenda est ratio regularum, quae ad verificationem operationum arithmeticarum vulgo commendantur. Scilicet si ex numeris datis alii per additionem, subtractionem, multiplicationem aut eleuationem ad potestates sunt deducendi: substiuuntur datorum loco residua ipsorum minima secundum modulum arbitrarium (vulgo 9 aut 11, quoniam in nostro systemate decadico secundum hos, vti modo ostendimus, residua tam facile possunt inueniri). Numeri hinc oriundi illis, qui ex numeris propositis deducti fuerunt, congrui esse debent; quod nisi eueniat, vitium in calculum irrepsisse concluditur.

Sed quum haec hisque similia abunde sint nota, diutius iis immorari superfluum foret.

SECTIO SECVNDA

DE

CONGRVENTIIS PRIMI GRADVS.

13. THEOREMA. *Productum e duobus numeris positiuis numero primo dato minoribus per hunc primum diuidi nequit.*

Sit p primus, et a positiuus $< p$: tum nullus numerus positiuus b ipso p minor dabitur, ita vt sit $ab \equiv 0 \pmod{p}$.

Dem. Si quis neget, supponamus dari numeros b, c, d, etc. omnes $< p$, ita vt $ab \equiv 0$; $ac \equiv 0$; $ad \equiv 0$ etc. (mod. p). Sit omnium minimus b, ita vt omnes numeri ipso b minores hac proprietate sint destituti. Manifesto erit $b > 1$: si enim $b = 1$, foret $ab = a < p$ (*hyp.*), adeoque per p non diuisibilis. Quare p tamquam primus per b diuidi non poterit, sed inter duo ipsius b multipla proxima mb et $(m+1)b$ cadet. Sit $p - mb = b'$, eritque b' numerus positiuus et $< b$. Iam quia supposuimus, $ab \equiv 0 \pmod{p}$, habebitur quoque $mab \equiv 0$ (art. 7), et hinc, subtrahendo ab $ap \equiv 0$, erit $a(p - mb) = ab' \equiv 0$; i. e. b' inter nu-

meros b, c, d, etc. referendus, licet minimo eorum b sit minor. *Q. E. A.*

14. *Si nec a nec b per numerum primum p diuidi potest: etiam productum ab per p diuidi non poterit.*

Sint numerorum a, b, secundum modulum p residua minima positiua α, β, quorum neutrum erit o (*hyp.*). Iam si esset $ab \equiv o \pmod{p}$, foret quoque, propter $ab \equiv \alpha\beta$, $\alpha\beta \equiv o$, quod cum theoremate praec. consistere nequit.

Huius theorematis demonstratio iam ab Euclide tradita, *El. VII.* 32. Nos tamen omittere eam noluimus, tum quod recentiorum complures seu ratiocinia vaga pro demonstratione venditauerunt, seu theorema omnino praeterierunt, tum quod indoles methodi hic adhibitae, qua infra ad multo reconditiora enodanda vtemur, e casu simpliciori facilius deprehendi poterit.

15. *Si nullus numerorum a, b, c, d etc. per numerum primum p diuidi potest, etiam productum abcd etc. per p diuidi non poterit.*

Secundum artic. praec. ab per p diuidi nequit; ergo etiam abc; hinc $abcd$, etc.

16. Theorema. *Numerus compositus quicunque vnico tantum modo in factores primos resolui potest.*

Dem. Quemuis numerum compositum in factores primos resolui posse, ex elementis constat, sed pluribus modis diuersis fieri hoc non posse perperam plerumque supponitur tacite. Fingamus numerum compositum A, qui sit $= a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, alio adhuc modo in factores primos esse resolubilem. Primo manife-

stum est, in secundum hoc factorum systema alios primos quam a, b, c etc. ingredi non posse, quum quicunque alius primus numerum A ex his compositum metiri nequeat. Similiter etiam in secundo hoc factorum systemate nullus primorum a, b, c etc. deesse potest, quippe qui alias ipsum A non metiretur (art. praec.). Quare hae binae in factores resolutiones in eo tantummodo differre possunt, quod in altera aliquis primus pluries quam in altera habeatur. Sit talis primus p, qui in altera resolutione m, in altera vero n vicibus occurrat, sitque $m > n$: Iam deleatur ex utroque systemate factor p, n vicibus, quo fiet vt in altero adhuc $m - n$ vicibus remaneat, ex altero vero omnino abierit. I. e. numeri $\frac{A}{p^n}$ duae in factores resolutiones habentur, quarum altera a factore p prorsus libera, altera vero $m - n$ vicibus eum continet, contra ea quae modo demonstrauimus.

17. Si itaque numerus compositus A est productum ex B, C, D etc., patet, inter factores primos numerorum B, C, D etc. alios esse non posse, quam qui etiam sint inter factores numeri A, et quemuis horum factorum toties in B, C, D coniunctim occurrere debere, quoties in A. Hinc colligitur criterium, vtrum numerus B alium A metiatur, necne. Illud eueniet, si B neque alios factores primos, neque vllum pluries inuoluit, quam A; quarum conditionum si aliqua deficit, B ipsum A non metietur.

Facile hinc calculi combinationum auxilio deriuari potest, si $A = a^\alpha b^\beta c^\gamma$ etc. designanti-

bus vt supra a, b, c etc. numeros primos diuersos: A habere $(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. diuisores diuersos, inclusis etiam 1 et A.

18. Si igitur $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\varkappa l^\lambda m^\mu$ etc., atque primi a, b, c etc., k, l, m etc. omnes diuersi, patet A et K diuisorem communem praeter 1 non habere, siue inter se esse primos.

Pluribus numeris A, B, C etc. propositis *maxima omnibus communis mensura* ita determinatur. Resoluantur omnes in suos factores primos, atque ex his excerpantur ii, qui omnibus numeris A, B, C etc. sunt communes, (si tales non adsunt, nullus diuisor erit omnibus communis). Tum quoties quisque horum factorum primorum in singulis A, B, C etc. contineatur, siue *quot dimensiones* in singulis A, B, C quisque habeat, adnotetur. Tandem singulis factoribus primis tribuantur dimensiones omnium quas in A, B, C etc. habent minimae, componaturque productum ex iis, quod erit mensura communis quaesita.

Quando vero numerorum A, B, C etc. *minimus communis diuiduus* desideratur, ita procedendum. Colligantur omnes numeri primi, qui numerorum A, B, C etc. aliquem metiuntur, tribuatur cuiuis dimensio omnium quas in numeris A, B, C etc. habet maxima, sicque ex omnibus productum confletur, quod erit diuiduus quaesitus.

Ex. Sit $A = 504 = 2^3 3^2 7$; $B = 2880 = 2^6 3^2 5$; $C = 864 = 2^5 3^3$. Pro inueniendo diui-

sore communi maximo habentur factores primi 2, 3, quibus dimensiones 3, 2 tribuendi; vnde fiet $= 2^3 3^2 = 72$; diuiduus vero communis minimus erit $2^6 3^3 5 . 7 = 60480$.

Demonstrationes propter facilitatem omittimus. Ceterum quomodo haec problemata soluenda sint, quando numerorum *A*, *B*, *C* etc. in factores resolutio non detur, ex elementis notum.

19. *Si numeri a, b, c etc. ad alium k sunt primi, etiam productum ex illis abc etc. ad k primum est.*

Quia enim nulli numerorum *a*, *b*, *c* etc. factor primus cum *k* est communis productumque *abc* etc. alios factores primos habere nequit, quam qui sunt factores alicuius numerorum *a*, *b*, *c* etc., productum *abc* etc. etiam cum *k* factorem primum communem non habebit. Quare ex art. praec. *k* ad *abc* etc. primus.

Si numeri a, b, c etc. inter se sunt primi, aliumque k singuli metiuntur: etiam productum ex illis numerum k metietur.

Hoc aeque facile ex artt. 17, 18 deriuatur. Sit enim quicunque producti *abc* etc. diuisor primus *p*, quem contineat π vicibus, manifestumque est, aliquem numerorum *a*, *b*, *c* etc. eundem hunc diuisorem π vicibus continere debere. Quare etiam *k*, quem hic numerus metitur, π vicibus diuisorem *p* continet. Similiter de reliquis producti *abc* etc. diuisoribus.

Hinc *si duo numeri m, n secundum plures moduli inter se primos a, b, c etc. sunt congrui, etiam se-*

cundum productum ex his congrui erunt. Quum enim $m - n$ per singulos a, b, c etc. sit diuisibilis, etiam per eorum productum diuidi poterit.

Denique *si a ad b primus et ak per b diuisibilis, erit etiam k per b diuisibilis.* Namque quoniam ak tam per a quam per b diuisibilis, etiam per ab diuidi poterit, i. e $\frac{ak}{ab} = \frac{k}{b}$ erit integer.

20. *Quando $A = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, est potestas aliqua, puta $= k^n$: omnes exponentes α, β, γ etc. per n erunt diuisibiles.*

Numerus enim k alios factores primos quam a, b, c etc. non inuoluit. Contineat factorem a, α^1 vicibus, continebitque k^n siue A hunc factorem $n\alpha^1$ vicibus; quare $n\alpha^1 = \alpha$, et $\frac{\alpha}{n}$ integer. Similiter $\frac{\beta}{n}$ etc. integros esse demonstratur.

21. *Quando a, b, c etc. sunt inter se primi, et productum abc etc. potestas aliqua, puta $= k^n$: singuli numeri a, b, c etc. similes potestates erunt.*

Sit $a = l^\lambda m^\mu p^\pi$ etc., designantibus l, m, p etc. numeros primos diuersos, quorum nullus per *hyp.* est factor numerorum b, c etc. Quare productum abc etc. factorem l implicabit λ vicibus, factorem m vero μ vicibus etc.: hinc (*art. praec.*) λ, μ, π etc. per n diuisibiles adeoque $\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}}$ etc. integer. Similiter de reliquis b, c etc.

Haec de numeris primis praemittenda erant; iam ad ea quae finem nobis propositum propius attinent conuertimur.

22. *Si numeri a, b per alium k diuisibiles secundum modulum m ad k primum sunt congrui:* $\frac{a}{k}$ *et* $\frac{b}{k}$ *secundum eundem modulum congrui erunt.*

Patet enim $a - b$ per k diuisibilem fore, nec minus per m (*hyp.*); quare (*art.* 19) $\frac{a-b}{k}$ per m diuisibilis erit, i. e. erit $\frac{a}{k} \equiv \frac{b}{k}$ (mod. m.).

Si autem reliquis manentibus m et k habent diuisorem communem maximum e, erit $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$). Namque $\frac{k}{e}$ et $\frac{m}{e}$ inter se primi. At $a - b$ tam per k quam per m diuisibilis adeoque etiam $\frac{a-b}{e}$ tam per $\frac{k}{e}$ quam per $\frac{m}{e}$, hincque per $\frac{km}{ee}$ i. e. $\frac{a-b}{k}$ per $\frac{m}{e}$, siue $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$).

23. *Si a ad m primus, et e, f numeri secundum modulum m incongrui: erunt etiam ae, af incongrui secundum m.*

Hoc est tantum conuersio theor. art. praec.

Hinc vero manifestum est, si a per omnes numeros integros a 0 vsque ad $m - 1$ multiplicetur productaque secundum modulum m ad residua sua minima reducantur, haec omnia fore inaequalia. Et quum horum residuorum, quorum nullum $> m$, numerus sit m, totidemque dentur numeri a 0 usque ad $m - 1$, patet, nullum horum numerorum inter illa residua deesse posse.

24. *Expressio* $ax + b$, denotantibus a, b numeros datos, x numerum indeterminatum seu variabilem, *secundum modulum m, ad a primum, cuiuis numero dato congrua fieri potest.*

Sit numerus, cui congrua fieri debet, c, et residuum minimum positiuum ipsius $c - b$ secundum modulum m, e. Ex art. praec. necessario datur valor ipsius $x < m$, talis, vt producti ax secundum modulum m residuum minimum fiat e; esto hic valor v, eritque $av \equiv e \equiv c - b$; vnde $av + b \equiv c \pmod{m}$ *Q. E. F.*

25. Expressionem duas quantitates congruas exhibentem ad instar aequationum, *congruentiam* vocamus; quae si incognitam implicat, *resolui* dicitur, quando pro hac valor inuenitur congruentiae satisfaciens (*radix*). Hinc porro intelligitur, quid sit *congruentia resolubilis et congruentia irresolubilis*. Tandem facile perspicitur similes distinctiones locum hic habere posse vti in aequationibus. Congruentiarum *transscendentium* infra exempla occurrent; *algebraicae* vero secundum dimensionem maximam incognitae in congruentias primi, secundi altiorumque *graduum* distribuuntur. Nec minus congruentiae plures proponi possunt plures incognitas inuoluentes, de quarum *eliminatione* disquirendum.

26. Congruentia itaque primi gradus, $ax + b \equiv c$ ex art. 24 semper resolubilis, quando modulus ad a est primus. Quodsi vero v fuerit valor idoneus ipsius x, siue radix congruentiae, palam est, omnes numeros, ipsi v secundum congruentiae propositae modulum congruos, etiam radices fore (art. 9.) Neque minus facile perspicitur, omnes radices ipsi v congruos esse debere: si enim alia radix fuerit t, erit $av + b \equiv at + b$. vnde $av \equiv at$, et hinc $v \equiv t$ (art. 22). Hinc colligitur congruentiam $x + v$

(mod. m.) exhibere resolutionem completam congruentiae $ax + b \equiv c$.

Quia resolutiones congruentiae per valores ipsius x congruos per se sunt obuiae, atque, hoc respectu, numeri congrui tamquam aequiualentes considerandi, tales congruentiae resolutiones pro vna eademque habebimus. Quamobrem quum nostra congruentia $ax + b \equiv c$ alias resolutiones non admittat, pronunciabimus, vnico tantum modo eam esse resolubilem seu vnam tantum radicem habere. Ita $e.\ g.$ congruentia $6x + 5 \equiv 13$ (mod. 11) alias radices non admittit, quam quae sunt $\equiv 5$ (mod. 11). Haud perinde res se habet in congruentiis altiorum graduum, siue etiam in congruentiis primi gradus, vbi incognita per numerum est multiplicata, ad quem modulus non est primus.

27. Superest, vt de inueniendа resolutione ipsa congruentiae huiusmodi, quaedam adiiciamus. Primo obseruamus, congruentiam formae $ax + t \equiv u$, cuius modulum ad a primum supponimus, ab hac, $ax \equiv \pm 1$, pendere: si enim huic satisfacit $x \equiv r$, illi satisfaciet $x \equiv \pm (u - t)\ r$. At congruentiae $ax \equiv \pm 1$, modulo per b designato, aequiualet aequatio indeterminata $ax = by \pm 1$, quae quomodo sit soluenda hoc quidem tempore abunde est notum; quare nobis sufficiet, calculi algorithmum huc transscripsisse.

Si quantitates A, B, C, D, E etc. ita ab his α, β, γ, δ, etc. pendent, vt habeatur $A = \alpha$, $B = \beta A + 1$, $C = \gamma B + A$, $D = \delta C + B$, $E = \varepsilon D$

$+ C$ etc., breuitatis gratia ita eas designamus, $A = [\alpha]$; $B = [\alpha, \beta]$; $C = [\alpha, \beta, \gamma]$, $D = [\alpha, \beta, \gamma, \delta]$ etc. *). Iam proposita sit aequatio indeterminata $ax = by \pm 1$, vbi a, b positiui. Supponamus, id quod licet, a esse non $< b$. Tum ad instar algorithmi noti, secundum quem duorum numerorum diuisor communis maximus inuestigatur, formentur per diuisionem vulgarem aequationes,

$a = \alpha b + c$
$b = \beta c + d$
$c = \gamma d + e$ etc.

ita vt α, β, γ etc. c, d, e etc. sint integri positiui, et b, c, d, e continuo decrescentes, donec perueniatur ad
$m = \mu n + 1$, quod tandem euenire debere constat. Erit itaque $a = [n, \mu, \ldots \gamma, \beta, \alpha]$; $b = [n, \mu \ldots \gamma, \beta]$. Tum fiat $x = [\mu, \ldots \gamma, \beta]$, $y = [\nu, \ldots \gamma \beta, \alpha]$, eritque $ax = by + 1$, quando numerorum $\alpha, \beta, \gamma \ldots \mu, n$ multitudo est par, aut $ax = by - 1$, quando est impar. *Q. E. F.*

28. Resolutionem generalem huiusmodi aequationum indeterminatarum ill. Euler pri-

*) Multo generalius haecce relatio considerari potest, quod negotium alia forsan occasione suscipiemus. Hic duas tantum propositiones adiicimus, quae vsum suum in praesenti inuestigatione habent; scilicet,

1°. $[\alpha, \beta, \gamma \ldots \lambda, \mu] \cdot [\beta, \gamma \ldots \lambda] - [\alpha, \beta, \gamma \ldots \lambda] [\beta, \gamma, \ldots \lambda, \mu] = \pm 1$, vbi signum superius accipiendum quando numerorum $\alpha, \beta, \gamma \ldots \lambda, \mu$ multitudo par, inferius quando impar.

2°. Numerorum α, β, γ etc. ordo inuerti potest, $[\alpha, \beta, \gamma \ldots, \lambda, \mu] = [\mu, \lambda \ldots \gamma, \beta, \alpha]$. Demonstrationes quae non sunt difficiles hic supprimimus.

mus docuit, *Comment. Petrop. T. VII. p.* 46. Methodus qua vsus est consistit in substitutione aliarum incognitarum loco ipsarum x, y, atque hoc quidem tempore satis est nota. Ill. la Grange paullo aliter rem aggressus est: scilicet ex theoria fractionum continuarum constat si fractio $\frac{b}{a}$ in fractionem continuam

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{etc.} + \cfrac{1}{\mu + \frac{1}{n}}}}}$$

conuertatur, haecque deleta vltima sui parte $\frac{1}{n}$ in fractionem communem $\frac{x}{y}$ restituatur, fore $ax = by \pm 1$, siquidem fuerit a ad b primus. Ceterum ex vtraque methodo idem algorithmus deriuatur. Inuestigationes ill. la Grange exstant *Hist. de l' Ac. de Berlin Année* 1767 *p.* 175, et cum aliis in *Supplementis versioni gallicae Algebrae Eulerianae adiectis.*

29. Congruentia $ax + t \equiv u$ cuius modulus ad a non primus, facile ad casum praecedentem reducitur. Sit modulus m, maximusque numerorum a, m diuisor communis δ. Primo patet quemuis valorem ipsius x congruentiae secundum modulum m satisfacientem eidem etiam secundum modulum δ satisfacere (art. 5). At semper $ax \equiv 0 \pmod{\delta}$ quoniam δ ipsum a metitur. Quare, nisi $t \equiv u \pmod{\delta}$ i. e. $t - u$ per δ diuisibilis, congruentia proposita non est resolubilis.

Ponamus itaque $a = \delta e$, $m = \delta f$, $t - u = \delta k$, eritque e ad f primus. Tum vero congruentiae propositae $\delta ex + \delta k \equiv 0 \pmod{\delta f}$ aequiualebit haec $ex + k \equiv 0 \pmod{f}$, i. e. quicunque ipsius x valor huic satisfaciat, etiam illi satisfaciet et vice versa. Manifesto enim $ex + k$ per f diuidi poterit, quando $\delta ex + \delta k$ per δf diuidi potest, et vice versa. At congruentiam $ex + k \equiv 0 \pmod{f}$ supra soluere docuimus; vnde simul patet, si v sit vnus ex valoribus ipsius x, $x \equiv v \pmod{f}$ exhibere resolutionem completam congruentiae propositae.

3o. Quando modulus est compositus, nonnumquam praestat sequenti methodo vti.

Sit modulus $= mn$, atque congruentia proposita $ax \equiv b$. Soluatur primo congruentia haec secundum modulum m, ponamusque ei satisfieri, si $x \equiv v \pmod{\frac{m}{\delta}}$, designante δ diuisorem communem maximum numerorum m, a. Iam manifestum est, quemuis valorem ipsius x congruentiae $ax \equiv b$ secundum modulum mn satisfacientem eidem etiam secundum modulum m satisfacere debere: adeoque in forma $v + \frac{m}{\delta} x'$ contineri, designante x' numerum indeterminatum, quamuis non vice versa omnes numeri in forma $v + \frac{m}{\delta} x'$ contenti congruentiae secundum mod. mn satisfaciant. Quomodo autem x' determinari debeat, vt $v + \frac{m}{\delta} x'$ fiat radix congruentiae $ax \equiv b \pmod{mn}$, ex solutione congruentiae $\frac{am}{\delta} x' + av \equiv b \pmod{mn}$ deduci potest, cui aequiualet haec $\frac{a}{\delta} x' \equiv \frac{b-av}{m} \pmod{n}$. Hinc colligitur solutionem congruentiae cuiuscunque primi gradus secundum modulum mn

reduci posse ad solutionem duarum congruentiarum secundum modulum m et n. Facile autem perspicietur, si m iterum sit productum e duobus factoribus, solutionem congruentiae secundum modulum n pendere a solutione duarum congruentiarum quarum moduli sint illi factores. Generaliter solutio congruentiae secundum modulum compositum quemcumque pendet a solutione aliarum congruentiarum, quarum moduli sunt factores illius numeri; hi autem, si commodum esse videtur, ita semper accipi possunt, vt sint numeri primi.

Ex. Si congruentia $19x \equiv 1 \pmod{140}$ proponitur: soluatur primo secundum modulum 2, eritque $x \equiv 1 \pmod{2}$. Ponatur $x = 1 + 2x'$, fietque $39x' \equiv -18 \pmod{140}$ cui aequiualet $19x' \equiv -9 \pmod{70}$. Si haec iterum secundum modulum 2 soluitur, fit $x' \equiv 1 \pmod{2}$ positoque $x' = 1 + 2x''$, fit $38x'' \equiv -28 \pmod{70}$ siue $19x'' \equiv -14 \pmod{35}$. Haec secundum 5 soluta dat $x'' \equiv 4 \pmod{5}$, substitutoque $x'' = 4 + 5x'''$, fit $95x''' \equiv -90 \pmod{35}$ siue $19x''' \equiv -18 \pmod{7}$. Ex hac tandem sequitur, $x''' \equiv 2 \pmod{7}$, positoque $x''' = 2 + 7x^{IV}$ colligitur $x = 59 + 140x^{IV}$; quare $x \equiv 59 \pmod{140}$ est solutio completa congruentiae propositae.

31. Simili modo vt aequationis $ax = b$ radix per $\frac{b}{a}$ exprimitur, etiam congruentiae $ax \equiv b$ radicem quamcunque per $\frac{b}{a}$ designabimus, congruentiae modulum, distinctionis gratia, ap-

ponentes. Ita e. g. $\frac{12}{17}$ (mod. 12) denotat quemuis numerum, qui est $\equiv 11$ (mod. 12) *). Generaliter ex praecedentibus patet, $\frac{b}{a}$ (mod. c) nihil reale significare (aut si quis malit aliquid imaginarii), si a, c habeant diuisorem communem, qui ipsum b non metiatur: At hoc casu excepto, expressio $\frac{b}{a}$ (mod. c) semper valores reales habebit, et quidem infinitos: hi vero omnes secundum c erunt congrui quando a ad c primus, aut secundum $\frac{c}{\delta}$, quando δ numerorum c, a diuisor communis maximus.

Hae expressiones similem fere habent algorithmum vt fractiones vulgares. Aliquot proprietates quae facile ex praecedentibus deduci possunt hic apponimus.

1. Si secundum modulum c, $a \equiv \alpha$, $b \equiv \beta$ expressiones $\frac{a}{b}$ (mod. c) et $\frac{\alpha}{\beta}$ (mod. c) sunt aequiualentes.

2. $\frac{a}{b\delta}$ (mod. $c\delta$) et $\frac{a}{b}$ (mod. c) sunt aequiualentes.

3. $\frac{ak}{bk}$ (mod. c) et $\frac{a}{b}$ (mod. c) sunt aequiualentes quando k ad c est primus.

Multae aliae similes propositiones afferri possent: at quum nulli difficultati sint obnoxiae, neque ad sequentia adeo necessariae, ad alia properamus.

32. Problema quod magnum in sequentibus vsum habebit, *inuenire omnes numeros, qui secundum modulos quotcunque datos residua data praebent*, facile ex praecedentibus solui potest. Sint pri-

*) id quod ex analogia per $\frac{11}{1}$ (mod. 12) designari potest.

mo duo moduli, A, B, secundum quos numerus quaesitus, x, numeris a, b respectiue congruus esse debeat. Omnes itaque valores ipsius x sub forma $Ax+a$ continentur, vbi x est indeterminatus sed talis vt fiat $Ax+a \equiv b \pmod{B}$. Quodsi iam numerorum A, B diuisor communis maximus est δ, resolutio completa huius congruentiae hanc habebit formam: $x \equiv v \pmod{\frac{B}{\delta}}$ siue quod eodem redit, $x = v + \frac{kB}{\delta}$, denotante k numerum integrum arbitrarium. Hinc formula $Av + \frac{kAB}{\delta}$ omnes ipsius x valores comprehendet, i. e. $x \equiv Av \pmod{\frac{AB}{\delta}}$ erit resolutio completa problematis. Si ad modulos A, B, tertius accedit, C, secundum quem numerus quaesitus x, debet esse $\equiv c$, manifesto eodem modo procedendum, quum binae priores conditiones in vnicam iam sint conflatae. Scilicet si numerorum $\frac{AB}{\delta}$, C diuisor communis maximus $= \varepsilon$, atque congruentiae $\frac{AB}{\delta}x + Av \equiv c \pmod{C}$ resolutio: $x \equiv w \pmod{\frac{C}{\varepsilon}}$, problema per congruentiam $x \equiv \frac{ABw}{\delta} + Av \pmod{\frac{ABC}{\varepsilon}}$ complete erit resolutum. Similiter procedendum, quotcunque moduli proponantur. Obseruari conuenit $\frac{AB}{\delta}$, $\frac{ABC}{\delta\varepsilon}$ esse numerorum A, B; et A, B, C respectiue minimos communes diuiduos, facileque inde perspicitur, quotcunque habeantur moduli A, B, C etc., si eorum minimus communis diuiduus sit M, resolutionem completam hanc formam habere, $x \equiv r \pmod{M}$. Ceterum quando vlla congruentiarum auxiliarum est irresolubilis, problema impossibilitatem inuoluere concludendum est. Perspicuum vero, hoc euenire non posse, quando omnes numeri A, B, C etc. inter se sint primi.

Ex. Sint numeri A, B, C; a, b, c, 504, 35, 16; 17, — 4, 33; hic duae conditiones vt x sit $\equiv 17 \pmod{504}$ et $\equiv -4 \pmod{35}$ vnicae, vt sit $\equiv 521 \pmod{2520}$ aequiualent; ex qua cum hac: $x \equiv 33 \pmod{16}$ coniuncta, promanat $x \equiv 3041 \pmod{5040}$.

33. Quando omnes numeri A, B, C etc. inter se sunt primi, constat, productum ex ipsis esse minimum omnibus communem diuiduum. In quo casu manifestum est, omnes congruentias $x \equiv a \pmod{A}$; $x \equiv b \pmod{B}$ etc. vnicae $x \equiv r \pmod{R}$ prorsus aequiualere, denotante R numerorum A, B, C etc. productum. Hinc vero vicissim sequitur, vnicam conditionem $x \equiv r \pmod{R}$ in plures dissolui posse; scilicet si R quomodocunque in factores inter se primos A, B, C etc. resoluitur, conditiones $x \equiv r \pmod{A}$, $x \equiv r \pmod{B}$, $x \equiv r \pmod{C}$, etc. propositam exhaurient. Haec obseruatio methodum nobis aperit non modo impossibilitatem, si quam forte conditiones propositae implicent, statim detegendi, sed etiam calculum commodius atque concinnius instituendi.

34. Sint vt supra conditiones propositae, vt sit $x \equiv a \pmod{A}$ $x \equiv b \pmod{B}$, $x \equiv c \pmod{C}$. Resoluantur omnes moduli in factores inter se primos, A in $A' A'' A'''$ etc.; B in $B' B'' B'''$ etc. etc. et quidem ita vt numeri A', A'' etc. B', B'' etc. etc. sint aut primi, aut primorum potestates. Si vero aliquis numerorum A, B, C etc. iam per se est primus, aut primi potestas, nulla resolutione in factores pro hocce opus est. Tum vero ex praecedentibus pa-

tescit, pro conditionibus propositis hasce substitui posse: $x \equiv a \pmod{A'}$, $x \equiv a \pmod{A''}$, $x \equiv a \pmod{A'''}$ etc., $x \equiv b \pmod{B'}$, $x \equiv b \pmod{B''}$ etc. etc. Iam nisi omnes numeri A, B, C etc. fuerint inter se primi, ex. gr. si A ad B non primus, manifestum est, omnes diuisores primos ipsorum A, B diuersos esse non posse, sed inter factores A', A'', A''' etc. vnum aut alterum esse debere, qui inter B', B'', B''' etc. aut aequalem aut multiplum aut submultiplum habeat. Si *primo* $A' = B'$, conditiones $x \equiv a \pmod{A'}$, $x \equiv b \pmod{B'}$ identicae esse debent, siue $a \equiv b \pmod{A' \text{ vel } B'}$, quare alterutra reiici poterit. Si vero non $a \equiv b \pmod{A'}$, problema impossibilitatem implicat. Si *secundo* B' multiplum ipsius A', conditio $x \equiv a \pmod{A'}$ in hac $x \equiv b \pmod{B'}$ contenta esse debet, siue haec $x \equiv b \pmod{A'}$ quae ex posteriori deducitur cum priori identica esse debet. Vnde sequitur conditionem $x \equiv a \pmod{A'}$, nisi alteri repugnet (in quo casu problema impossibile) reiici posse. Quando omnes conditiones superfluae ita reiectae sunt, patet, omnes modulos ex his A', A'', A''' etc., B', B'', B''' etc. etc. remanentes inter se primos fore; tum igitur de problematis possibilitate certi esse et secundum praecepta ante data procedere possumus.

35. Ex. Si ut supra esse debet $x \equiv 17 \pmod{504}$; $\equiv -4 \pmod{35}$, et $\equiv 33 \pmod{16}$; hae conditiones in sequentes resolui possunt, $x \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$; $\equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$; $\equiv 33 \pmod{16}$. Ex his conditiones $x \equiv 17 \pmod{8}$, $x \equiv 17 \pmod{7}$ reiici possunt,

quum prior in conditione $x \equiv 33 \pmod{16}$ contineatur, posterior vero cum hac $x \equiv -4 \pmod{7}$ sit identica; remanent itaque

$$x \equiv \begin{cases} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{cases} \quad \text{vnde colligitur } x \equiv 3041 \pmod{5040}$$

Ceterum palam est, plerumque commodius fore, si de conditionibus remanentibus eaequae ex vna eademque conditione euolutae erant seorsim recolligantur, quum hoc nullo negotio fieri possit; *e. g.* quando ex conditionibus $x = a \pmod{A'}$ $x \equiv a \pmod{A''}$ etc. aliquae abierunt: quae ex reliquis restituitur, haec erit, $x \equiv a$ secundum modulum qui est productum omnium modulorum ex A', A'', A''' etc. remanentium. Ita in nostro exemplo ex conditionibus $x \equiv -4 \pmod{5}$ $x \equiv 4 \pmod{7}$ ea ex qua ortae erant $x \equiv -4 \pmod{35}$ sponte restituitur. Porro hinc sequitur haud prorsus perinde esse, quaenam ex conditionibus superfluis reiiciantur, quantum ad calculi breuitatem: sed haec aliaque artificia practica, quae ex vsu multo facilius quam ex praeceptis ediscuntur hic tradere non est instituti nostri.

36. Quando omnes moduli A, B, C, D etc. inter se sunt primi, sequenti methodo saepius praestat vti. Determinetur numerus α secundum A vnitati, secundum reliquorum modulorum productum vero cifrae congruus, siue sit α valor quicunque (plerumque praestat *minimum* accipere) expressionis $\frac{1}{BCD \text{ etc.}} \pmod{A}$, per BCD etc. multiplicatae (vid. art. 32); similiter sit

$\zeta \equiv 1 \pmod{B}$ et $\equiv 0 \pmod{ACD \text{ etc.}}$, $\gamma \equiv 1 \pmod{C}$ et $\equiv 0 \pmod{ABD \text{ etc.}}$, etc. Tunc si numerus x desideratur, qui secundum modulus A, B, C, D etc. numeris a, b, c, d etc. respectiue sit congruus, poni poterit $x \equiv \alpha a + \zeta b + \gamma c + \delta d$ etc. $\pmod{ABCD \text{ etc.}}$. Manifesto enim, $\alpha a \equiv a \pmod{A}$; reliqua autem membra ζb, γc etc. omnia $\equiv 0 \pmod{A}$; quare $x \equiv a \pmod{A}$. Similiter de reliquis modulis demonstratio adornatur. Haec solutio priori praeferenda, quando plura huiusmodi problemata sunt soluenda, pro quibus moduli A, B, C etc. valores suos retinent; tunc enim numeri α, ζ, γ etc. valores constantes nanciscuntur. Hoc vsu venit in problemate chronologico vbi quaeritur, quotus in periodo Juliana sit annus, cuius indictio, numerus aureus, et cyclus solaris dantur. Hic $A = 15$, $B = 19$, $C = 28$; quare, quum valor expressionis $\frac{1}{19.28} \pmod{15}$, siue $\frac{1}{532} \pmod{15}$, sit 13, erit $\alpha = 6916$. Similiter pro ζ inuenitur 4200, et pro γ 4845, quare numerus quaesitus erit residuum minimum numeri $6916\,a + 4200\,b + 4845\,c$, denotantibus a indictionem, b numerum aureum, c cyclum solarem.

37. Haec de congruentiis primi gradus vnicam incognitam continentibus sufficiant. Superest vt de congruentiis agamus, in quibus plures incognitae sunt permixtae. At quoniam hoc caput, si omni rigore singula exponere velimus, sine prolixitate absolui non potest, propositumque hoc loco nobis non est, omnia exhaurire, sed ea tantum tradere, quae atten-

tione digniora videantur: hic ad paucas obseruationes inuestigationem restringimus, vberiorem huius rei expositionem ad aliam occasionem nobis reseruantes.

1) Simili modo, vt in aequationibus, perspicitur, etiam hic totidem congruentias haberi debere, quot sint incognitae determinandae

2) Propositae sint igitur congruentiae

$ax + by + cz \ldots \equiv f \pmod{m} \ldots\ldots (A)$
$a'x + b'y + c'z \ldots \equiv f' \quad \ldots\ldots (A')$
$a''x + b''y + c''z \ldots \equiv f'' \quad \ldots\ldots (A'')$
etc.

totidem numero, quot sunt incognitae x, y, z etc.

Iam determinentur numeri ξ, ξ', ξ'' etc. ita vt sit

$b\xi + b'\xi' + b''\xi'' + \text{etc.} = 0.$
$c\xi + c'\xi' + c''\xi'' + \text{etc.} = 0.$
etc.

et quidem ita vt omnes sint integri nullumque factorem communem habeant, quod fieri posse ex theoria aequationum linearium constat. Simili modo determinentur υ, υ', υ'' etc., ζ, ζ', ζ'' etc. etc. ita vt sit

$a\upsilon + a'\upsilon' + a''\upsilon'' + \text{etc.} = 0.$
$c\upsilon + c'\upsilon' + c''\upsilon'' + \text{etc.} = 0.$
etc.
$a\zeta + a'\zeta' + a''\zeta'' + \text{etc.} = 0.$
$b\zeta + b'\zeta' + b''\zeta'' + \text{etc.} = 0.$
etc. etc.

3) Manifestum est si congruentiae A, A', A'' etc. per ξ, ξ', ξ'' etc.; tum per υ, υ', υ'', etc. etc. multiplicentur, tuncque addantur, has congruentias prouenturas esse:

$(a\xi + a'\xi' + a''\xi'' + \text{etc.})\, x \equiv f\xi + f'\xi' + f''\xi'' + \text{etc.}$
$(b\upsilon + b'\upsilon' + b''\upsilon'' + \text{etc.})\, y \equiv f\upsilon + f'\upsilon' + f''\upsilon'' + \text{etc.}$
$(c\zeta + c'\zeta' + c''\zeta'' + \text{etc.})\, z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{etc.}$
etc.

quas breuitatis gratia ita exhibemus:

$\Sigma\,(a\xi)\, x \equiv \Sigma\,(f\xi)$
$\Sigma\,(b\upsilon)\, y \equiv \Sigma\,(f\upsilon)$
$\Sigma\,(c\zeta)\, z \equiv \Sigma\,(f\zeta)$ etc.

4) Iam plures casus sunt distinguendi. *Primo* quando omnes incognitarum coefficientes, $\Sigma\,(a\xi)$, $\Sigma\,(a\upsilon)$ etc. ad congruentiarum modulum m sunt primi, hae congruentiae secundum praecepta ante tradita solui possunt, problematisque solutio completa per congruentias formae $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$ etc. exhibebitur *). E. g. Si proponuntur congruentiae $x + 3y + z \equiv 1$; $4x + y + 5z \equiv 7$; $2x + 2y + z \equiv 3 \pmod{8}$, inuenietur $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, vnde fit $-15x \equiv -26$; quare $x \equiv 6 \pmod{8}$; eodem modo inuenitur $15y \equiv -4$, $15z \equiv 1$, et hinc $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5) *Secundo* quando non omnes coefficientes, $\Sigma\,(a\xi)$, $\Sigma\,(b\upsilon)$ etc. ad modulum sunt primi,

*) Obseruare conuenit hancce conclusionem demonstratione egere, quam autem hic supprimimus. Proprie enim nihil aliud ex analysi nostra sequitur, quam quod congruentiae propositae per alios incognitarum x, y etc. valores solui nequeant: hos vero satisfacere non sequitur. Fieri enim posset vt nulla omnino solutio daretur. Similis paralogismus etiam in aequationum linearium explicatione plerumque committitur.

sint α, $\mathfrak{G}$, γ etc. diuisores communes maximi ipsius m cum $\Sigma(a\xi)$, $\Sigma(b\upsilon)$, $\Sigma(c\zeta)$ etc. resp., patetque problema impossibile esse, nisi illi numeros $\Sigma(f\xi)$, $\Sigma(f\upsilon)$, $\Sigma(f\zeta)$ etc. resp. metiantur. Quando vero hae conditiones locum habent, congruentiae in (3) complete resoluentur per tales $x \equiv p (\mathrm{mod.}\ \frac{m}{\alpha})$, $y \equiv q (\mathrm{mod.}\ \frac{m}{\mathfrak{G}})$, $z \equiv r (\mathrm{mod.}\ \frac{m}{\gamma})$ etc., aut si mauis dabuntur α valores diuersi ipsius x (i. e. secundum m incongrui puta p, $p + \frac{m}{\alpha} \ldots p + \frac{(\alpha - 1)m}{\alpha}$), $\mathfrak{G}$ valores diuersi ipsius y etc., illis congruentiis satisfacientes: manifestoque omnes solutiones congruentiarum propositarum (si quae omnino dantur) inter illas reperientur. Attamen hanc conclusionem conuertere non licet; nam plerumque non omnes combinationes omnium α valorum ipsius x cum omnibus ipsius y cum omnibus ipsius z etc. problemati satisfaciunt, sed quaedam tantum, quarum nexum per vnam pluresue congruentias conditionales exhibere licet. At quum completa huius problematis resolutio ad sequentia non sit necessaria, hoc argumentum fusius hoc loco non exsequimur, exemploque ideam qualemcunque de eo dedisse sat habemus.

Propositae sint congruentiae $3^x + 5^y + z \equiv 4$, $2^x + 3^y + 2z \equiv 7$, $5^x + y + 3z \equiv 6 (\mathrm{mod.}\ 12)$. Hic fiunt ξ, ξ', ξ''; υ, υ', υ''; ζ, ζ', ζ'' resp. $= 1, -2, 1$; $1, 1, -1$; $-13, 22, -1$, vnde $4^x \equiv -4$, $7^y \equiv 5$, $28z \equiv 96$. Hinc prodeunt quatuor valores ipsius x puta $\equiv 2, 5, 8, 11$; vnus valor ipsius y puta $\equiv 11$; quatuor valores ipsius z puta $\equiv 0, 3, 6, 9$ (mod. 12). Iam vt sciamus, quasnam combina-

tiones valorum ipsius x cum valoribus ipsius z adhibere liceat, substituimus in congruentiis propp. pro x, y, z resp. $2 + 3t$, 11, $3u$, vnde transeunt in has $57 + 9t + 3u \equiv 0$, $30 + 6t + 6u \equiv 0$, $15 + 15t + 9u \equiv 0 \pmod{12}$, quibus facile intelligitur aequiualere has $19 + 3t + u \equiv 0$, $10 + 2t + 2u \equiv 0$, $5 + 5t + 3u \equiv 0 \pmod{4}$. Prima manifesto requirit vt sit $u \equiv t + 1 \pmod{4}$, quo valore in reliquis substituto etiam his satisfieri inuenitur. Hinc colligitur, valores ipsius x hos $2, 5, 8, 11$ (qui prodeunt statuendo $t \equiv 0, 1, 2, 3$) necessario combinandos esse cum valoribus ipsius z his $z \equiv 3, 6, 9, 0$ resp., ita vt omnino quatuor solutiones habeantur

$$\left.\begin{array}{l} x \equiv 2, 5, 8, 11 \\ y \equiv 11, 11, 11, 11 \\ z \equiv 3, 6, 9, 0 \end{array}\right\} \pmod{12}$$

* * *

His disquisitionibus, per quas sectionis propositum iam absolutum est, adhac quasdam propositiones similibus principiis innixas adiungimus, quibus in sequentibus frequenter opus erit.

38. Problema. *Inuenire, quot numeri positiui dentur numero positiuo dato A minores simulque ad ipsum primi.*

Designemus breuitatis gratia multitudinem numerorum positiuorum ad numerum datum primorum ipsoque minorum per praefixum characterem φ. Quaeritur itaque φA.

I. Quando A est primus, manifestum est omnes numeros ab 1 vsque ad $A - 1$ ad A primos esse; quare in hoc casu erit $\varphi A = A - 1$.

II. Quando A est numeri primi potestas puta $= p^m$, omnes numeri per p diuisibiles ad A non erunt primi, reliqui erunt. Quamobrem de $p^m - 1$ numeris hi sunt reiiciendi: p, $2p$, $3p$ .... $(p^{m-1} - 1)\, p$; remanent igitur $p^m - 1 - (p^{m-1} - 1)$ siue $p^{m-1}\,(p - 1)$. Hinc $\varphi\, p^m = p^{m-1}\,(p - 1)$.

III. Reliqui casus facile ad hos reducuntur ope sequentis propositionis: *Si A in factores M, N, P etc. inter se primos est resolutus, erit $\varphi A = \varphi M . \varphi N . \varphi P$ etc.*, quae ita demonstratur. Sint numeri ad M primi ipsoque M minores, m, m', m'' etc. quorum itaque multitudo $= \varphi M$. Similiter sint numeri ad N, P etc. respectiue primi ipsisque minores, n, n', n'' etc.; p, p', p'' etc. etc., quorum multitudo $\varphi N\, \varphi P$ etc. Iam constat omnes numeros ad productum A primos etiam ad factores singulos M, N, P etc. primos fore et vice versa (art. 19); porro omnes numeros qui horum m, m', m'' etc. alicui sint congrui secundum modulum M ad M primos fore et vice versa, similiterque de N, P etc. Quaestio itaque huc reducta est: determinare quot dentur numeri infra A, qui secundum modulum M, alicui numerorum m, m', m'' etc. secundum modulum N, alicui ex his n, n', n'' etc. etc. sint congrui. Sed ex art. 32 sequitur, omnes numeros, secundum singulos modulos M, N, P etc. residua determinata dantes, congruos secun-

dum eorum productum A fore, adeoque infra A vnicum tantum dari, secundum singulos M, N, P etc. residuis datis congruum. Quare numerus quaesitus aequalis erit numero combinationum singulorum numerorum m, m', m'' cum singulis n, n', n'' atque p, p', p'' etc. etc. Hunc vero esse $= \varphi M . \varphi N . \varphi P$ etc. ex theoria combinationum constat. *Q. E. D.*

IV. Iam quomodo hoc ad casum de quo agimus applicandum sit facile intelligitur. Resoluatur A in factores suos primos siue reducatur ad formam $a^\alpha b^\beta c^\gamma$ etc. designantibus a, b, c etc. numeros primos diuersos. Tum erit $\varphi A = \varphi a^\alpha . \varphi b^\beta . \varphi c^\gamma$ etc. $= a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1)\, c^{\gamma-1}(c-1)$ etc. seu concinnius $\varphi A = A \frac{a-1}{a} . \frac{b-1}{b} . \frac{c-1}{c}$ etc.

Exempl. Sit $A = 60 = 2^2 . 3 . 5$, adeoque $\varphi A = \frac{1}{2} . \frac{2}{3} . \frac{4}{5} . 60 = 16$. Numeri hi ad 60 primi sunt 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

Solutio prima huius problematis exstat in commentatione ill. Euleri, *theoremata arithmetica noua methodo demonstrata*, Comm. nou. Ac. Petrop. VIII. p. 74. Demonstratio postea repetita est in alia diss. *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII p. 17.

39. Si characteris φ significatio ita determinatur, vt φA exprimat multitudinem numerorum ad A primorum ipsoque A *non maiorum* perspicuum est φ 1 fore non amplius $= 0$, sed $= 1$; in omnibus reliquis casibus nihil hinc immutari. Hancce definitionem adoptantes sequens habebimus theorema.

Si a, a', a'' etc. sunt omnes diuisores ipsius A, (vnitate et ipso A non exclusis) erit $\varphi a + \varphi a' + \varphi a'' + \text{etc.} = A$.

Ex. sit $A = 30$; tum erit $\varphi 1 + \varphi 2 + 3\varphi + \varphi 5 + \varphi 6 + \varphi 10 + \varphi 15 + \varphi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Demonstr. Multiplicentur omnes numeri ad a primi ipsoque a non maiores per $\frac{A}{a}$, similiter omnes ad a' primi per $\frac{A}{a'}$ etc., habebunturque $\varphi a + \varphi a' + \varphi a'' +$ etc. numeri, omnes ipso A non maiores. At

1) omnes hi numeri erunt inaequales. Omnes enim eos qui ex *eodem* ipsius A diuisore sint generati, inaequales fore, per se clarum. Si vero e diuisoribus diuersis M, N numerisque μ, ν ad istos respectiue primis aequales prodiissent, *i. e.* si esset $\frac{A}{M}\mu = \frac{A}{N}\nu$, sequeretur $\mu N = \nu M$. Ponatur $M > N$ (id quod licet). Quoniam M ad μ est primus, atque numerum μN metitur, etiam ipsum N metietur, maior minorem. *Q. E. A.*

2) inter hos numeros, omnes hi 1, 2, 3 .... A inuenientur. Sit numerus quicunque ipsum A non superans t, maxima numerorum A, t communis mensura δ eritque $\frac{A}{\delta}$ diuisor ipsius A ad quem $\frac{t}{\delta}$ primus. Manifesto hinc numerus t inter eos inuenietur qui ex diuisore $\frac{A}{\delta}$ prodierunt.
3) Hinc colligitur horum numerorum multitudinem esse A, quare $\varphi a + \varphi a' + \varphi a'' + \text{etc.} = A$. *Q. E. D.*

40. *Si maximus numerorum A, B, C, D etc. diuisor communis* $= \mu$: *numeri a, b, c, d etc. ita determinari possunt, vt sit* $aA + bB + cC + \text{etc.} = \mu$.

Dem. Consideremus primo duos tantum numeros A, B, sitque horum diuisor maximus communis $= \lambda$. Tum congruentia $Ax \equiv \lambda \pmod{B}$ erit resolubilis (art. 30). Sit radix $\equiv \alpha$, ponaturque $\frac{\lambda - A\alpha}{B} = \zeta$. Tum erit $\alpha A + \zeta B = \lambda$, vti desiderabatur.

Accedente numero tertio C, sit maximus diuisor communis numerorum λ, C, $= \lambda'$, eritque hic simul maximus diuisor communis numerorum A, B, C *). Determinentur numeri k, γ ita vt sit $k\lambda + \gamma C = \lambda'$, eritque $k\alpha A + k\zeta B + \gamma C = \lambda'$.

Accedente numero quarto D, ponatur maximus diuisor communis numerorum λ', D (quem simul esse maximum diuisorem communem numerorum A, B, C, D facile perspicitur) $= \lambda''$, fiatque $k'\lambda' + \delta D = \lambda''$. Tum erit $kk'\alpha A + kk'\zeta B + k'\gamma C + \delta D = \lambda''$.

Simili modo proced ipotest, quotcunque alii numeri accedant.

Si itaque numeri A, B, C, D etc. diuisorem communem non habent, patet fieri posse $aA + bB + cC + \text{etc.} = 1$.

41. *Si p est numerus primus atque habentur p res, inter quas quotcunque aequales esse possunt, modo non omnes sint aequales: numerus permutationum harum rerum per p erit diuisibilis.*

*) Metietur enim manifesto λ' omnes A, B, C. Si vero non esset diuisor communis *maximus*: maximus foret maior quam λ' Iam quoniam hic diuisor maximus metitur ipsos A B; metietur etiam ipsum $\alpha A + \zeta B$ i. e. ipsum λ', maior minorem Q. E. A. — Facilius adhuc hoc ex art. 18 deduci potest.

Exempl. Quinque res A, A, A, B, B, decem modis diuersis possunt transponi.

Demonstratio huius theorematis facile quidem ex nota permutationum theoria peti potest. Si enim inter has res sunt primo a aequales nempe $= A$, tum b aequales nempe $= B$, tum c aequales nempe $= C$ etc. (vbi numeri a, b, c etc. etiam unitatem designare possunt), ita vt habeatur $a + b + c + \text{etc.} = p$, numerus permutationum erit $= \frac{1 \cdot 2 \cdot 3 \ldots p}{1 \cdot 2 \cdot 3 \ldots a \cdot 1 \cdot 2 \ldots b \cdot 1 \cdot 2 \ldots c \text{ etc.}}$. Iam per se clarum est, huius fractionis numeratorem per denominatorem diuisibilem esse, quoniam numerus permutationum debet esse integer: at numerator per p diuisibilis est, denominator vero, qui ex factoribus ipso p minoribus est compositus, per p non diuisibilis (art. 15). Quare numerus permutationum per p erit diuisibilis (art. 19).

Speramus tamen fore quibus etiam sequens demonstratio haud ingrata sit futura.

Quando in duabus permutationibus rerum e quibus compositae sunt ordo in eo tantum discrepat, vt ea res quae in altera primum locum occupat, aliam sedem in altera teneat, reliquae autem eodem in vtraque ordine progrediuntur, eamque quae in altera vltima est, ea quae est prima, in altera excipit; *permutationes similes* vocemus *). Ita in ex. nostro permutationes $ABAAB$ et $ABABA$ similes erunt,

*) Si permutationes similes in circulum scriptae esse concipiuntur ita vt vltima res primae fiat contigua, nulla omnino erit discrepantia, quoniam nullus locus primus aut vltimus vocari poterit,

quoniam res quae in priori primum secundum etc. locum occupant, in posteriori loco tertio quarto etc. eodem ordine sunt collocatae.

Iam quoniam quaeque permutatio ex p rebus constat, patet cuiuis $p-1$ similes adinueniri posse, si ea res quae prima fuerat, ad secundum, tertium etc. locum promoueatur. Quarum si nullae identicae esse possunt manifestum est, omnium permutationum numerum per p diuisibilem euadere, quippe qui p vicibus maior sit quam numerus omnium permutationum dissimilium. Supponamus igitur duas permutationes $PQ \ldots TV \ldots YZ$; $V \ldots YZPQ \ldots T$, quarum altera ex altera per terminorum promotionem orta sit, identicas esse siue $P = V$ etc. Sit terminus P qui in priori est primus, $n+1$ *tus* in posteriori. Erit igitur in serie posteriori terminus $n+1$ *tus* aequalis primo, $n+2$ *tus* secundo etc. vnde $2n+1$ *tus* rursus primo aequalis euadet, eademque ratione $3n+1$ *tus* etc.; generaliterque terminus $kn+m$ *tus m to* (vbi quando $kn+m$ ipsum p superat, aut series $V \ldots YZPQ \ldots T$ semper ab initio repeti concipienda est, aut a $kn+m$ multiplum ipsius p proxime minus rescindendum). Quamobrem si k ita determinatur, vt fiat $kn \equiv 1 \pmod{p}$, quod fieri potest quia p primus, sequitur generaliter terminum *m tum* $m+1$ *to* aequalem esse, siue quemuis terminum sequenti, i. e. omnes terminos aequales esse contra hypothesin.

42. *Si coefficientes* $A, B, C \ldots N$; $a, b, c \ldots$ *n duarum functionum formae*

$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots\ldots + N \ldots\ldots (P)$
$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \ldots\ldots + n \ldots\ldots (Q)$
omnes sunt rationales, neque vero omnes integri, productumque ex (P) *et* $(Q) =$
$x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$:
omnes coefficientes $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{Z}$ *integri esse nequeunt.*

Demonstr. Exprimantur omnes fractiones in coefficientibus A, B etc. a, b etc. per numeros quam minimos, eligaturque ad libitum numerus primus p, qui aliquem aut plures ex denominatoribus harum fractionum metiatur. Ponamus, id quod licet, p metiri denominatorem alicuius coefficientis fracti in (P), patetque si (Q) per p diuidatur, etiam in $\frac{(Q)}{p}$ dari ad minimum vnum coefficientem fractum cuius denominator implicet factorem p (puta coefficientem primum $\frac{1}{p}$). Iam facile perspicitur, in (P) datum iri terminum vnum, fractum, cuius denominator inuoluat *plures* dimensiones ipsius p quam denominatores omnium similium praecedentium, et *non pauciores* quam denominatores omnium sequentium; sit hic terminus $= Gx^g$, et multitudo dimensionum ipsius p in denominatore ipsius G, $= t$. Similis terminus dabitur in $\frac{(Q)}{p^\mu}$, qui sit $= \Gamma x^\gamma$ et multitudo dimensionum ipsius p in denominatore ipsius Γ, $= \tau$. Manifesto hic erit $t + \tau$ ad minimum $= 2$. His ita praeparatis, terminus $x^{g+\gamma}$ producti ex (P) et (Q) coefficientem habebit fractum, cuius denominator $t + \tau - 1$ dimensiones ipsius p inuoluet, id quod ita demonstratur.

Sint termini qui in (P) terminum Gx^g praecedunt, $'Gx^{g+1}$, $''Gx^{g+2}$, etc. sequentes vero $G'x^{g-1}$, $G''x^{g-2}$ etc.; similiterque in $(\frac{Q}{p})$

praecedant terminum Γx^{γ} termini $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$ etc. sequantur autem termini $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$ etc. Tum constat in producto ex (P), $\frac{(Q)}{p}$ coefficientem termini $x^{g+\gamma}$ fore $= G\Gamma$
$+ 'G\Gamma' + ''G\Gamma'' +$ etc.
$+ '\Gamma G' + ''\Gamma G'' +$ etc.
Pars $G\Gamma$ erit fractio quae si per numeros quam minimos exprimitur in denominatore $t+\tau$ dimensiones ipsius p inuoluit, reliquae autem partes si sunt fractae, in dominatore pauciores dimensiones numeri p implicabunt, quoniam omnes sunt producta e binis factoribus quorum alter non plures quam t, alter vero pauciores quam τ dimensiones ipsius p implicat; vel alter non plures quam τ, alterque pauciores quam t. Hinc $G\Gamma$ erit formae $\frac{e}{fp^{t+\tau}}$, reliquarum vero summa formae $\frac{e'}{f'p^{t+\tau-\delta}}$, vbi δ positiuus et e, f, f' a factore p liberi: quare omnium summa erit $= \frac{ef'+e'fp^{\delta}}{ff'p^{t+\tau}}$, cuius numerator per p non diuisibilis, adeoque denominator per nullam reductionem pauciores dimensiones quam $t+\tau$ obtinere potest. Hinc coefficiens termini $x^{g+\gamma}$ in producto ex (P), (Q) erit $= \frac{ef'+e'fp^{\delta}}{ff'p^{t+\tau-1}}$, i. e *fractio* cuius denominator $t+\tau-1$ dimensiones ipsius p implicat. *Q. E. D.*

43. *Congruentia* m^{ti} *gradus*, $Ax^m + Bx^{m-1} + Cx^{m-2} +$ *etc.* $+ Mx + N \equiv o$, *cuius modulus est numerus primus* p, *ipsum* A *non metiens, pluribus quam* m *modis diuersis solui non potest, siue plures quam* m *radices secundum* p *incongruos non habet* (Vid. artt. 25, 26)

Si quis neget, ponamus dari congruentias diuersorum graduum m, n, etc. quae plures quam m, n etc. radices habeant, sitque minimus gradus, m, ita vt omnes similes congruentiae inferiorum graduum theoremati nostro sint consentaneae. Quod quum de primo grado iam supra sit demonstratum (art. 26), manifestum est, m fore aut $= 2$ aut maiorem. Admittet itaque congruentia $Ax^m + Bx^{m-1} +$ etc. $+ Mx + N \equiv 0$ saltem $m+1$ radices, quae sint $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma$ etc., ponamusque id quod licet omnes numeros α, β, γ etc. esse positiuos et minores quam p, omniumque minimum α. Iam in congruentia proposita substituatur pro x, $y + \alpha$, transeatque inde in hanc $A' y^m + B' y^{m-1} + C' y^{m-2} \ldots + M' y + N' \equiv 0$. Tum manifestum est, huic congruentiae satisfieri deberi, si ponatur $y \equiv 0$, aut $\equiv \beta - \alpha$, aut $\equiv \gamma - \alpha$ etc., quae radices omnes erunt diuersae, numerusque earum $= m + 1$. At ex eo quod $y \equiv 0$ est radix, sequitur, N' per p diuisibilem fore. Quare etiam haec expressio, $y (A' y^{m-1} + B' y^{m-2} +$ etc. $+ M')$ fiet $\equiv 0$ (mod. p), si ipsi y vnus ex m valoribus, $\beta - \alpha$, $\gamma - \alpha$, etc. tribuitur, qui omnes sunt > 0 et $< p$, adeoque in omnibus hisce casibus etiam $A' y^{m-1} + B' y^{m-2} +$ etc. $+ M'$ fiet $\equiv 0$ art. 22; i. e. congruentia $A' y^{m-1} + B' y^{m-2} +$ etc. $+ M' \equiv 0$, quae est gradus $m - 1^{ti}$, m radices habet et proin theoremati nostro aduersatur (patet enim facile, A' fore $= A$, adeoque per p non diuisibilem, vti requiritur) licet supposuerimus, omnes congruentias inferioris gradus quam m^{ti}, theoremati consentire. *Q. E. A.*

44. Quamuis hic supposuerimus, modulum p non metiri coefficientem termini summi, tamen theorema ad hunc casum non restringitur. Si enim primus coefficiens siue etiam aliqui sequentium per p diuisibiles essent, hi termini tuto reiici possent, congruentiaque tandem ad inferiorem gradum deprimeretur, vbi coefficiens primus per p non amplius foret diuisibilis, siquidem non omnes coefficientes per p diuidi possunt; in quo casu, congruentia foret, identica atque incognita prorsus indeterminata.

Theorema hoc primum ab ill. La Grange propositum atque demonstratum est (*Mem. de l'Ac. de Berlin, Année* 1768 *p.* 192.). Exstat etiam in dissert. ill. Le Gendre, *Recherches d'Analyse indeterminée, Hist. de l'Acad. de Paris* 1785. *p.* 466. Ill. Euler in *Nou. Comm. Ac. Petr. XVIII. p.* 93 demonstrauit congruentiam $x^n - 1 \equiv 0$ plures quam n radices diuersas habere non posse. Quae quamuis sit particularis, tamen methodus qua vir summus vsus est omnibus congruentiis facile adaptari potest. Casum adhuc magis limitatum iam antea absoluerat, Comm. Ac. Petr. V. p. 6, sed haec methodus generaliter adhiberi nequit. Infra Sect. VIII, alio adhuc modo theorema demonstrabimus; at quantumuis diuersae primo aspectu omnes hae methodi videri possint, periti qui comparare eas voluerint facile certiores fient omnes eidem principio superstructas esse. Ceterum quum hoc theorema hic tantum tamquam lemma sit considerandum, neque completa expositio huc pertineat: de modulis compositis seorsim agere supersedemus.

Sectio Tertia

de

RESIDVIS POTESTATVM.

45. Theorema. *In omni progressione geometrica*, 1, a, aa, a^3 *etc. praeter primum* 1, *alius adhuc datur terminus*, a^t, *secundum modulum* p *ad* a *primum vnitati congruus, cuius exponens* $t < p$.

Demonstr. Quoniam modulus p ad a, adeoque ad quamuis ipsius a potestatem est primus, nullus progressionis terminus erit $\equiv 0 \pmod{p}$, sed quiuis alicui ex his numeris $1, 2, 3 \ldots p-1$ congruus. Quorum multitudo quum sit $p-1$, manifestum est, si plures quam $p-1$ progressionis termini considerentur, omnes residua minima diuersa habere non posse. Quocirca inter terminos 1, a, aa, $a^3 \ldots a^{p-1}$ bini ad minimum congrui inuenientur. Sit itaque $a^m \equiv a^n$ et $m > n$, fietque diuidendo per a^n, $a^{m-n} \equiv 1$ (art. 22) vbi $m-n < p$, et > 0. *Q. E. D.*

Ex. In progressione 1, 2, 4, 8 etc. terminus primus qui secundum modulum 13 vnitati

est congruus, inuenitur $2^{12} = 4096$. At secundum modulum 23 in eadem progressione fit $2^{11} = 2048 \equiv 1$. Similiter numeri 5 potestas sexta, 15625, vnitati congrua secundum modulum 7, quinta vero, 3125, secundum 11. In aliis igitur casibus potestas exponentis minoris quam $p - 1$ vnitati congrua euadit, in aliis contra vsque ad potestatem $p - 1$ tam ascendere necesse est.

46. Quando progressio vltra terminum qui vnitati est congruus continuatur, eadem quae ab initio habebantur residua prodeunt iterum. Scilicet si $a^t \equiv 1$, erit $a^{t+1} \equiv a$, $a^{t+2} \equiv aa$ etc. donec ad terminum a^{2t} perueniatur, cuius residuum minimum iterum erit $\equiv 1$, atque residuorum *periodum* denuo inchoat. Habetur itaque periodus t residua comprehendens, quae simulac finita est ab initio semper repetitur; neque alia residua quam quae in hac periodo continentur in tota progressione occurrere possunt. Generaliter erit $a^{mt} \equiv 1$, et $a^{mt+n} \equiv a^n$, id quod per designationem nostram ita exhibetur:

Si $r \equiv s \pmod{t}$ *erit*

$a^r \equiv a^s \pmod{p}$

47. Petitur ex hoc theoremate compendium potestatum quantumuis magno exponente affectarum residua expedite inueniendi, simulac potestas vnitati congrua innotescat. Si ex. gr. residuum e diuisione potestatis 3^{1000} per 13 oriundum quaeritur, erit propter $3^3 \equiv 1 \pmod{13}$, $t \equiv 3$; quare quum sit $1000 \equiv 1 \pmod{3}$, erit $3^{1000} \equiv 3 \pmod{13}$.

48. Quando a^t est *infima* potestas vnitati congrua (praeter $a^0 = 1$, ad quem casum hic

non respicimus), illi t termini, residuorum periodum constituentes omnes erunt diuersi, vti ex demonstratione art. 45 nullo negotio perspicitur. Tum autem propositio art. 46 conuerti potest; scilicet si $a^m \equiv a^n \pmod{p}$ erit $m \equiv n \pmod{t}$. Si enim m, n secundum modulum t incongrui essent, residua eorum minima, μ, ν diuersa forent. At $a^\mu \equiv a^m$, $a^\nu \equiv a^n$, quare $a^\mu \equiv a^\nu$ i. e. non omnes potestates infra a^t incongrui forent contra hypoth.

Si itaque $a^k \equiv 1 \pmod{p}$, erit $k \equiv 0 \pmod{t}$ *i. e.* k per t diuisibilis.

Hactenus de modulis quibuscunque si modo ad a sint primi diximus. Iam modulos qui sunt numeri absolute primi seorsim considerabimus atque huic fundamento inuestigationem generaliorem postea superstruamus.

49. Theorema. *Si p est numerus primus ipsum a non metiens, atque a^t infima ipsius a potestas secundum modulum p vnitati congrua, exponens t aut erit $= p - 1$ aut pars aliquota huius numeri.*

Conferantur exempla art. praec.

Demonstr. Quum iam ostensum sit, t esse aut $= p - 1$, aut $< p - 1$, superest, vt in posteriori casu t semper ipsius $p - 1$ partem aliquotam esse euincatur.

I. Colligantur residua minima positiua omnium horum terminorum, $1, a, aa \ldots a^{t-1}$, quae per $\alpha, \alpha', \alpha''$ etc. designentur, ita vt sit $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv aa$ etc. Perspicuum est, haec omnia fore diuersa, si enim duo termini a^m, a^n

eadem praeberent, foret (supponendo $m > n$), $a^{m-n} \equiv 1$ atque $m - n < t$, *Q. E. A.* quum nulla inferior potestas quam a^t vnitati sit congrua, *hyp.* Porro omnes $\alpha, \alpha', \alpha''$ etc. in serie numerorum 1, 2, 3 ... $p-1$ continentur, quam tamen non exhaurient, quum $t < p-1$. Complexum omnium $\alpha, \alpha', \alpha''$ etc. per (A) designabimus. Comprehendet igitur (A) terminos t.

II. Accipiatur numerus quicunque ζ ex his 1, 2, 3 ... $p-1$, qui in (A) desit. Multiplicetur ζ per omnes $\alpha, \alpha', \alpha''$ etc., sintque residua minima inde oriunda ζ, ζ', ζ'' etc., quorum numerus etiam erit t. At haec residua tum inter se quam ab omnibus $\alpha, \alpha', \alpha''$ etc. erunt diuersa. Si enim *prior* assertio falsa esset, haberetur $\zeta a^m \equiv \zeta a^n$ adeoque diuidendo per ζ, $a^m \equiv a^n$, contra ea quae modo demonstrauimus; si vero *posterior*, haberetur $\zeta a^m \equiv a^n$, vnde, quando $m < n$, $\zeta \equiv a^{n-m}$ i. e. ζ alicui ex his $\alpha, \alpha', \alpha''$ etc. congruus contra hyp.; quando vero $m > n$, sequitur multiplicando per a^{t-m}, $\zeta a^t \equiv a^{t+n-m}$, siue propter $a^t \equiv 1$, $\zeta \equiv a^{t+n-m}$, quae est eadem absurditas. Designetur complexus omnium ζ, ζ', ζ'' etc. quorum multitudo $= t$, per (B), habebunturque iam $2t$ numeri ex his 1, 2, 3 ... $p-1$. Quodsi igitur (A) et (B) omnes hos numeros complectuntur, fit $\frac{p-1}{2} = t$ adeoque theorema demonstratum.

III. Si vero aliqui adhuc deficiunt, sit horum aliquis γ. Per hunc multiplicentur omnes $\alpha, \alpha', \alpha''$ etc., productorumque residua minima sint $\gamma, \gamma', \gamma''$ etc.; omnium complexus per (C) designetur. (C) igitur comprehendet t numeros

ex his 1, 2, 3 ... $p-1$, quae omnes tum inter se quam a numeris in (*A*) et (*B*) contentis erunt diuersi. Assertiones priores eodem modo demonstrantur vt in II, tertia ita. Si esset $\gamma a^m \equiv \epsilon a^n$, fieret $\gamma \equiv \epsilon a^{n-m}$, aut $\equiv \epsilon a^{t+n-m}$ prout $m < n$, aut $> n$, in vtroque casu γ alicui ex (*B*) congrua contra hyp. Habentur igitur $3t$ numeri ex his 1, 2, 3 ... $p-1$, atque si nulli amplius desunt, fiet $t = \frac{p-1}{3}$ adeoque theorema erit demonstratum.

IV. Si vero etiamnum aliqui desunt eodem modo ad quartum numerorum complexum, (*D*), progrediendum erit etc. Patet vero quoniam numerorum 1, 2, 3 .... $p-1$ multitudo est finita, tandem eam exhaustum iri, adeoque multiplum ipsius t fore: quare t erit pars aliquota numeri $p-1$. *Q. E. D.*

5o. Quum igitur $\frac{p-1}{t}$ sit integer, sequitur euehendo vtramque partem congruentiae $a^t \equiv 1$ ad potestatem exponentis $\frac{p-1}{t}$, $a^{p-1} \equiv 1$, *siue* $a^{p-1} - 1$ *semper per* p *diuisibilis est, quando* p *est primus ipsum* a *non metiens.*

Theorema hoc quod tum propter elegantiam tum propter eximiam vtilitatem omni attentione dignum, ab inuentore *theorema Fermatianum* appellari solet. Vid. *Fermatii Opera Mathem. Tolosae* 1679 *fol. p.* 163. Demonstrationem inuentor non adiecit, quam tamen in potestate sua esse professus est. Ill. Euler primus demonstrationem publici iuris fecit, in diss. cui titulus *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop.* T.

VIII *). Innititur ista euolutioni potestatis $(a+1)^p$, vbi ex coefficientium forma facillime deducitur $(a+1)^p - a^p - 1$ semper per p fore diuisibilem, adeoque $(a+1)^p - (a+1)$ per p diuisibilem fore, quando $a^p - a$ per p sit diuisibilis. Iam quia $1^p - 1$ semper per p diuisibilis est, etiam $2^p - 2$ semper erit; hinc etiam $3^p - 3$ etc. generaliterque $a^p - a$. Quodsi itaque p ipsum a non metitur, etiam $a^{p-1} - 1$ per p diuisibilis erit. Haec sufficient ad methodi indolem declarandam. Clar. Lambert similem demonstrationem tradidit in *Actis Erudit.* 1769. *p.* 109. Quia vero euolutio potestatis binomii a theoria numerorum satis aliena esse videbatur, aliam demonstrationem ill. Euler inuestigauit quae exstat *Comment. nou. Petr. T. VII. p.* 70, atque cum ea quam nos art. praec. exposuimus prorsus conuenit. In sequentibus adhuc aliae quaedam se nobis offerent. Hoc loco vnam superaddere liceat, quae similibus principiis innititur, vti prima ill. Euleri. Propositio sequens, cuius casus tantum particularis est theorema nostrum, etiam ad alias inuestigationes infra adhibebitur.

Polynomii $a+b+c+$ *etc. potestas* p *ta secundum modulum* p *est* $\equiv a^p + b^p + c^p +$ *etc., siquidem* p *est numerus primus.*

*) In comment. anteriore vir summus ad scopum nondum peruenerat. *Com. Petr.* T. VI. p. 106. — In controuersia famosa inter Maupertuis et König, a principio actionis minimae orta, sed mox ad res heterogeneas egressa, König in manibus se habere dixit autographum Leibnitianum, in quo demonstratio huius theorematis cum Euleriana prorsus conspirans contineatur. *Appel au public.* p. 106. Licet vero fidem huic testimonio denegare nolimus, certe Leibnitius inuentum suum numquam publicauit. Conf. *Hist. de l'Ac. de Prusse. A.* 1750. *p.* 530.

Demonstr. Constat potestatem p^{tam} polynomii $a + b + c +$ etc. esse compositam e partibus formae $\varkappa a^{\alpha} b^{\beta} c^{\gamma}$ etc. vbi $\alpha + \beta + \gamma$ etc. $= p$, et $\varkappa$ designat, quot modis p res, quarum α, β, γ etc. respectiue sunt $= a$, b, c etc. permutari possint. At supra art. 41 ostendimus, hunc numerum semper esse per p diuisibilem, nisi omnes res sint aequales, i. e. nisi aliquis numerorum α, β, γ etc. sit $= p$ reliqui vero $= 0$. Vnde sequitur omnes ipsius $(a + b + c +$ etc.$)^p$ partes, praeter has a^p, b^p, c^p etc., per p diuisibiles esse; quae igitur quando de congruentia secundum modulum p agitur, tuto omitti poterunt, fietque $(a + b + c +$ etc.$)^p \equiv a^p + b^p + c^p +$ etc. *Q. E. D.*

Quodsi iam omnes quantitates a, b, c etc. $= 1$ ponuntur, numerusque earum $= k$, fiet $k^p \equiv k$ vti in art. praec.

52. Quoniam igitur alii numeri quam qui sunt diuisores ipsius $p - 1$ nequeunt esse exponentes potestatum infimarum ad quas euecti numeri aliqui vnitati congrui fiunt, quaestio sese offert, num omnes ipsius $p - 1$ diuisores ad hoc sint idonei, atque, quando omnes numeri per p non diuisibiles secundum exponentem infimae suae potestatis vnitati congruae classificentur, quot ad singulos exponentes sint peruenturi. Vbi statim observare conuenit, sufficere, si omnes numeri positiui ab 1 vsque ad $p - 1$ considerentur; manifestum enim est, numeros congruos ad eandem potestatem eleuari debere, quo vnitati fiant congruae, adeoque numerum quemcunque ad eundem exponentem esse referendum ad quem residuum suum mi-

nimum positiuum. Quocira in id nobis erit incumbendum, vt quomodo hoc respectu numari 1, 2, 3 .... $p-1$ inter singulos $p-1$ factores distribuendi sint eruamus. Breuitatis gratia, si d est vnus e diuisoribus numeri $p-1$ (ad quos etiam 1 et $p-1$ referendi), per ψd designabimus multitudinem numerorum positiuorum ipso p minorum quorum potestas d^{te} est infima vnitati congrua.

53. Quo facilius haec disquisitio intelligi possit, exemplum apponimus. Pro $p=19$ distribuentur numeri 1, 2, 3 .... 18 inter diuisores numeri 18 hoc modo:

1	1.
2	18.
3	7, 11.
6	8, 12.
9	4, 5, 6, 9, 16, 17.
18	2, 3, 10, 13, 14, 15.

In hoc igitur casu fit $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. Vbi exigua attentio docet, totidem ad quemuis exponentem pertinere, quot dentur numeri hoc non maiores ad ipsumque primi, siue esse in hoc certe casu, retento signo art. 40, $\psi d = \varphi d$. Hanc autem obseruationem generaliter veram esse ita demonstramus.

I. Si numerus aliquis habetur, a, ad exponentem d *pertinens* (*i. e.* cuius potestas d^{ta} vnitati congrua, omnes inferiores incongruae), omnes huius potestates, aa, a^3, a^4 .... a^d siue ipsarum residua minima proprietatem priorem etiam possidebunt (vt potestas ipsarum d^{ta} vnitati sit congrua) et quum hoc ita etiam expri-

mi possit, residua minima numerorum a, aa, a^3 .... a^d (quae omnia sunt diuersa) esse radices congruentiae $x^d \equiv 1$, haec autem plures quam d radices diuersas habere nequeat, manifestum est, praeter numerorum a, aa, a^3 .... a^d residua minima alios numeros inter 1 et $p-1$ incl. non dari quorum potestates exponentis d congruae sint vnitati. Hinc patet omnes numeros ad exponentem d pertinentes inter residua minima numerorum a, aa, a^3 .... a^d reperiri. Quales vero sint, quantaque eorum multitudo ita definitur. Si k est numerus ad d primus, omnes potestates ipsius a^k, quarum exponentes $< d$, vnitati non erunt congrui: esto enim $\frac{1}{k}$ (mod. d) $\equiv m$ (vid. art. 31) eritque $a^{km} \equiv a$; quare si potestas e^{ta} ipsius a^k vnitati esset congrua atque $e < d$, foret etiam $a^{kme} \equiv 1$ et hinc $a^e \equiv 1$ contra hyp. Hinc manifestum est, residuum minimum ipsius a^k ad exponentem d pertinere. Si vero k diuisorem aliquem, δ, cum d communem habet, ipsius a^k residuum minimum ad exponentem d non pertinet; quoniam tum potestas $\frac{d}{\delta}^{ta}$ iam vnitati fit congrua (erit enim $\frac{kd}{\delta}$ per d diuisibilis, siue $\equiv 0$ (mod. d) adeoque $a^{\frac{kd}{\delta}} \equiv 1$). Hinc colligitur, totidem numeros ad exponentem d pertinere quot numerorum 1, 2, 3 .... d ad d sint primi. At memorem esse oportet, hanc conclusionem innixam esse suppositioni, vnum numerum a iam haberi ad exponentem d pertinentem. Quamobrem dubium remanet, fierine possit vt ad aliquem exponentem nullus omnino numerus pertineat; conclusioque eo limitatur vt ψd sit vel $= 0$ vel $= \varphi d$.

54. II. Iam sint omnes diuisores numeri $p-1$ hi: d, d', d'', etc. eritque, quia omnes numeri $1, 2, 3 \ldots p-1$ inter hos sunt distributi, $\psi d + \psi d' + \psi d'' + \text{etc.} = p-1$. At in art. 40 demonstrauimus esse $\varphi d + \varphi d' + \varphi d'' + \text{etc.} = p-1$, atque ex art. praec. sequitur ψd ipsi φd aut aequalem aut ipso minorem esse, maiorem esse non posse, similiterque de $\psi d'$ et $\varphi d'$, etc. Si itaque aliquis terminus ex his $\psi d, \psi d', \psi d''$ etc. termino respondente ex his $\varphi d, \varphi d', \varphi d''$, esset minor (siue etiam plures) illorum summa summae horum aequalis esse non posset. Vnde tandem concludimus ψd *ipsi* φd *semper esse aequalem*, adeoque a magnitudine ipsius $p-1$ non pendere.

55. Maximam autem attentionem meretur casus particularis propositionis praecedentis scilicet *semper dari numeros quorum nulla potestas inferior quam* $p-1^{ta}$ *vnitati congrua*, et quidem totidem inter 1 et $p-1$ quot infra $p-1$ sint numeri ad $p-1$ primi. Cuius theorematis demonstratio quum minime tam obuia sit quam primo aspectu videri possit, propter theorematis dignitatem liceat aliam adhuc adiicere a praecedente aliquantum diuersam, quandoquidem methodorum diuersitas ad res obscuriores illustrandas plurimum conferre solet. Resoluatur $p-1$ in factores suos primos fiatque $p-1 = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales. Tum theorematis demonstrationem per sequentia absoluemus:

I. Semper inueniri posse numerum A, (aut plures), ad exponentem a^α pertinentem,

similiterque numeros B, C etc. ad exponentes b^{β}, c^{γ} etc. respectiue pertinentes.

II. Productum ex omnibus numeris A, B, C etc. (siue huius producti residuum minimum) ad exponentem $p-1$ pertinere. Haec autem ita demonstramus.

I. Sit g numerus aliquis ex his $1, 2, 3 \ldots p-1$, congruentiae $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$ *non* satisfaciens, omnes enim hi numeri congruentiae huic, cuius gradus $< p-1$, satisfacere nequeunt. Tum dico si potestas $\frac{p-1}{a^{\alpha}}$ ta ipsius g ponatur $\equiv h$, hunc numerum, siue eius residuum minimum ad exponentem a^{α} pertinere.

Namque patet potestatem a^{α} tam ipsius h congruam fore potestati $p-1$ tae ipsius g *i. e.* vnitati, potestas vero $a^{\alpha-1}$ ta ipsius h congrua erit potestati $\frac{p-1}{a}$ tae ipsius g, *i. e.* vnitati erit incongrua, multoque minus potestates $a^{\alpha-2}$, $a^{\alpha-3}$ tae etc. ipsius h vnitati congruae esse possunt. At exponens infimae potestatis ipsius h, vnitati congruae, siue exponens ad quem pertinet h, numerum a^{α} metiri debet (art. 48). Quare quum a^{α} per alios numeros diuisibilis non sit quam per se ipsum, atque per inferiores ipsius a potestates, necessario a^{α} erit exponens ad quem h pertinet. *Q. E. D.* Per similem methodum demonstratur, dari numeros ad exponentes b^{β}, c^{γ} etc. pertinentes.

II. Si supponimus, productum ex omnibus A, B, C etc. non ad exponentem $p-1$, sed ad minorem t pertinere, t ipsum $p-1$ metietur (art. 48), siue erit $\frac{p-1}{t}$ integer vnitate maior. Facile autem perspicitur, hunc quotientem vel

esse vnum e numeris primis a, b, c etc. vel saltem per aliquem eorum diuisibilem (art. 17), ex. gr. per a, de reliquis enim simile est ratiocinium. Metietur itaque t ipsum $\frac{p-1}{a}$; quare productum ABC etc. etiam ad potestatem $\frac{p-1}{a}$ tam eleuatum vnitati erit congruum (art. 46). Sed perspicuum est singulos B, C, etc. (exemto ipso A) ad potestatem $\frac{p-1}{a}$ tam eleuatos vnitati congruos fieri, quum exponentes b^α, c^γ, etc. ad quos singuli pertinent ipsum $\frac{p-1}{a}$ metiantur. Hinc erit $A^{\frac{p-1}{a}}\ B^{\frac{p-1}{a}}\ C^{\frac{p-1}{a}}$ etc. $\equiv A^{\frac{p-1}{a}} \equiv 1$. Vnde sequitur exponentem ad quem A pertinet ipsum $\frac{p-1}{a}$ metiri debere (art. 48), i. e. $\frac{p-1}{a^{\alpha+1}}$ esse integrum; at $\frac{p-1}{a^{\alpha+1}} \equiv \frac{b^\alpha c^\gamma \text{ etc.}}{a}$ integer esse nequit (art. 15). Vnde tandem concludere oportet, suppositionem nostram consistere non posse, i. e. productum ABC etc. reuera ad exponentem $p-1$ pertinere. *Q. E. D.*

Demonstratio posterior priori aliquantulum prolixior esse videtur, prior contra posteriori minus directa.

56. Hoc theorema insigne exemplum suppeditat, quanta circumspectione in theoria numerorum saepenumero opus sit, ne, quae non sunt, pro certis assumamus. Celeb. Lambert in diss. iam supra laudata *Acta Erudit.* 1769 p. 127 huius propositionis mentionem facit seddemonstrationis ne necessitatem quidem attigit. Nemo vero demonstrationem tentauit praeter summum Eulerum *Comment. nou. Ac. Petrop. T. XVIII* ad annum

1773 *Demonstrationes circa residua ex diuisione potestatum per numeros primos resultantia* p. 85 seqq. vid. imprimis art. 37 vbi de demonstrationis necessitate fusius locutus est. At demonstratio quam Vir sagacissimus exhibuit duos defectus habet. Alterum quod art. 31 et sqq. tacite supponit, congruentiam $x^n \equiv 1$ (translatis ratiociniis illic adhibitis in nostra signa) reuera n radices diuersas habere, quamquam ante nihil aliud fuerit demonstratum quam quod *plures* habere nequeat; alterum, quod formulam art. 34 per inductionem tantummodo deduxit.

57. Numeros ad exponentem $p-1$ pertinentes *radices primitiuas* cum ill. Eulero vocabimus. Si igitur a est radix primitiua, potestatum a, aa, a^3 ... a^{p-1} residua minima omnia erunt diuersa; vnde facile deducitur, inter haec omnes numeros 1, 2, 3, ... $p-1$, qui totidem sunt multitudine quot illa residua minima, reperiri debere, *i. e.* quemuis numerum per p non diuisibilem potestati alicui ipsius a congruum esse. Insignis haec proprietas permagnae est vtilitatis, operationesque arithmeticas, ad congruentias pertinentes, haud parum subleuare potest, simili fere modo, vt logarithmorum introductio operationes arithmeticae vulgaris. Radicem aliquam primitiuam, a, ad lubitum pro *basi* adoptabimus, ad quam omnes numeros per p non diuisibiles referemus, et si fuerit $a^e \equiv b \pmod p$, e ipsius b *indicem* vocabimus. Ex. gr. si pro modulo 19, radix primitiua 2 pro basi assumatur respondebunt

numeris 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18.
indices 0. 1. 13. 2. 16. 14. 6. 3. 8. 17. 12. 15. 5. 7. 11. 4. 10. 9.

Ceterum patet, manente basi, cuique numero plures indices conuenire, sed hos omnes secundum modulum $p-1$ fore congruos; quamobrem quoties de indicibus sermo erit, qui secundum modulum $p-1$ sunt congrui pro aequiualentibus habebuntur, simili modo vti numeri ipsi, quando secundum modulum p sunt congrui, tamquam aequiualentes spectantur.

58. Theoremata ad indices pertinentia prorsus analoga sunt iis quae ad logarithmos spectant.

Index producti e quotcunque factoribus conflati congruus est summae indicum singulorum factorum secundum modulum $p-1$.

Index potestatis numeri alicuius congruus est producto ex indice numeri dati in exponentem potestatis, secundum mod. $p-1$.

Demonstrationes propter facilitatem omittimus.

Hinc perspicitur si tabulam construere velimus ex qua omnium numerorum indices pro modulis diuersis desumi possint, ex hac tum omnes numeros modulo maiores, tum omnes compositos omitti posse. Specimen huius modi tabulae ad calcem operis huius adiectum est, *Tab. I*, vbi in prima columna verticali positi sunt numeri primi primorumque potestates a 3 vsque ad 97, qui tamquam moduli sunt spectandi, iuxta hos singulos numeri pro basi as-

sumti; tum sequuntur indices numerorum primorum successiuorum, quorum quini semper per paruulum interuallum sunt disiuncti, eodemque ordine supra dispositi sunt numeri primi; ita vt quis index numero primo dato secundum modulum datum respondeat, facile tutoque inueniri possit.

Ita ex. gr. si $p = 67$ index numeri 60, assumto 12 pro basi erit $\equiv 2$ Ind. $2 +$ Ind. $3 -$ Ind. 5 (mod. 66) $\equiv 58 + 9 + 39 \equiv 40$.

59. *Index valoris cuiuscunque expressionis* $\frac{a}{b}$ *(mod. p.), (art. 31) congruus est secundum modulum* $p - 1$ *differentiae indicum numeratoris a et denominatoris b, siquidem numeri a, b per p non sunt diuisibiles.*

Sit enim valor quicunque c; eritque $bc \equiv a$ (mod. p); hinc Ind. $b +$ Ind. $c \equiv$ Ind. a (mod. $p - 1$) adeoque
Ind. $c \equiv$ Ind. $a -$ Ind. b.

Si itaque tabula habetur, ex qua index cuique numero respondens pro quouis modulo primo, aliaque ex qua numerus ad indicem datum pertinens deriuari possit, omnes congruentiae primi gradus facillimo negotio solui poterunt, quoniam omnes reduci possunt ad tales, quarum modulus est numerus primus (art. 30). *E. g.* proposita congruentia $29x + 7 \equiv 0$ (mod. 47) erit $x \equiv \frac{-7}{29}$ (mod. 47).
Hinc *Ind.* $x \equiv$ Ind. $- 7 -$ Ind. $29 \equiv$ Ind. $40 -$ Ind. $29 \equiv 15 - 43 \equiv 18$ (mod. 46). At numerus cuius index 18 inuenitur 3. Quare

$x \equiv 3 \pmod{47}$. — Tabulam secundam quidem non adiecimus: at huius vice alia defungi poterit vti Sect. VI ostendemus.

60. Simili modo vt art. 31 radices congruentiarum primi gradus designauimus, in sequentibus etiam congruentiarum purarum altiorum graduum radices per signum exhibebimus. Vti scilicet $\sqrt[n]{A}$ nihil aliud significat quam radicem aequationis $x^n = A$; ita apposito modulo per $\sqrt[n]{A} \pmod{p}$ denotabitur radix quaecunque congruentiae $x^n \equiv A \pmod{p}$. Hanc expressionem $\sqrt[n]{A} \pmod{p}$ tot valores habere dicemus, quot habet secundum p incongruos, omnes enim qui secundum p sunt congrui tamquam aequiualentes spectandi (art. 26). Ceterum patet, si A, B secundum p fuerint congrui, expressiones $\sqrt[n]{A}$, $\sqrt[n]{B} \pmod{p}$ aequiualentes fore.

Iam si ponitur $\sqrt[n]{A} \equiv x \pmod{p}$, erit n Ind. $x \equiv$ Ind. $A \pmod{p-1}$. Ex hac congruentia deducuntur ad praecepta sectionis praec. valores ipsius Ind. x atque ex his valores respondentes ipsius x. Facile vero perspicitur x habere totidem valores, quot radices congruentia n Ind. $x \equiv A \pmod{p-1}$. Manifesto igitur $\sqrt[n]{A}$ vnum tantummodo valorem habebit quando n ad $p-1$ est primus; quando vero numeri n, $p-1$ diuisorem communem habent δ, atque hic est maximus, Ind. x habebit δ valores incongruos secundum $p-1$, adeoque $\sqrt[n]{A}$ totidem valores incongruos secundum p, siquidem Ind. A per δ est diuisibilis. Qua con-

ditione deficiente $\sqrt[n]{A}$ nullum valorem realem habebit.

Exemplum. Quaeruntur valores expressionis $\sqrt[15]{11}$ (mod. 19). Solui itaque debet congruentia 15 Ind. $x \equiv$ Ind. $11 \equiv 6$ (mod. 18), inuenienturque tres valores ipsius Ind. $x \equiv 4$, 10, 16 (mod. 18). His vero respondent valores ipsius x, 6, 9, 4.

61. Quantumuis expedita sit methodus haec quando tabulae necessariae adsunt, debemus tamen non obliuisci, indirectam eam esse. Operae igitur pretium erit inquirere quantum methodi directae polleant: trademusque hic ea quae ex praecedentibus hauriri possunt: alia, quae considerationes reconditiores postulant, ad sectionem VIII reseruantes. Initium facimus a casu simplicissimo, vbi $A = 1$, siue vbi radices congruentiae $x^n \equiv 1$ (mod. p) quaeruntur. Hic itaque, assumta radice quacunque primitiua pro basi, debet esse n Ind. $x \equiv 0$ (mod. $p-1$). Quae congruentia, quando n ad $p-1$ est primus, vnam tantummodo radicem habebit, scilicet Ind. $x \equiv 0$ (mod. $p-1$): quare *in hocce casu* $\sqrt[n]{1}$ (mod p) vnicum valorem habet, scilicet $\equiv 1$. Quando autem numeri n, $p-1$ habent diuisorem communem (maximum) δ, congruentiae n Ind. $x \equiv 0$ (mod. $p-1$) solutio completa erit Ind. $x \equiv 0$ (mod. $\frac{p-1}{\delta}$) V. art. 30., *i. e.* Ind. x secundum modulum $p-1$ alicui ex his numeris, $0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \frac{3(p-1)}{\delta}, \ldots \frac{(\delta-1)(p-1)}{\delta}$ congruus esse debebit, siue δ valores secundum modu-

lum $p-1$ incongruos habebit; quare etiam x in hocce casu δ valores diuersos (secundum modulum p incongruos) habebit. Hinc perspicitur, expressionem $\sqrt[\delta]{1}$ etiam δ valores diuersos habere, quorum indices cum ante allatis prorsus conueniant. Quocirca expressio $\sqrt[\delta]{1}$ (mod. p) huic $\sqrt[n]{1}$ (mod. p) omnino aequiualet, i. e. congruentia $x^\delta \equiv 1$ (mod. p) easdem radices habet quas haec, $x^n \equiv 1$ (mod. p). Prior autem inferioris erit gradus siquidem δ et n sunt inaequales.

Ex. $\sqrt[15]{1}$ (mod. 19) tres habet valores, quia 3 maxima numerorum 15, 18 mensura communis, hique simul erunt valores expressionis $\sqrt[3]{1}$ (mod. 19). Sunt autem hi, 1, 7, 11.

62. Per hanc igitur reductionem id lucramur vt alias congruentias formae $x^n \equiv 1$ soluere non sit opus, quam vbi n moduli est diuisor. Infra vero ostendemus, congruentias huius formae semper vlterius adhuc deprimi posse, licet praecedentia ad hoc non sufficiant. Vnum tamen casum iam hic absoluere possumus scilicet vbi $n = 2$. Manifesto enim valores expressionis $\sqrt[2]{1}$ erunt $+1$ et -1 quia plures quam duos habere nequit, hique $+1$ et -1 semper sunt incongrui nisi modulus sit $= 2$, in quo casu $\sqrt[2]{1}$ vnam tantum valorem habere posse, per se clarum. Hinc sequitur, $+1$ et -1 etiam fore valores expressionis $\sqrt[2m]{1}$ quando m ad $\frac{p-1}{2}$ sit primus. Hoc semper eueniet, quoties modulus est eius indolis vt $\frac{p-1}{2}$ fiat numerus absolute primus (nisi forte $p-1 = 2m$ in

quo casu omnes numeri 1, 2, 3 .... $p-1$ sunt radices) ex. gr. quando $p=3, 5, 7, 11, 23, 47, 59, 83, 107$ etc. - Tamquam corollarium hic annotetur, indicem ipsius -1 semper esse $\equiv \frac{p-1}{2} \pmod{p-1}$, quaecunque radix primitiua pro basi accipiatur. Namque 2 Ind. $(-1) \equiv 0 \pmod{p-1}$. Quare Ind. (-1) erit vel $\equiv 0$, vel $\equiv \frac{p-1}{2} \pmod{p-1}$: 0 vero semper index ipsius $+1$, atque $+1$, et -1 semper indices diuersos habere debent (praeter casum $p=2$ ad quem hic respicere operae non est pretium).

63. Ostendimus art. 60 expressionem $\sqrt[n]{A} \pmod{p}$ habere δ valores diuersos, aut omnino nullum, si fuerit δ diuisor communis maximus numerorum n, $p-1$. Iam vti modo docuimus $\sqrt[n]{A}$ et $\sqrt{A}$ aequiualentes esse, si fuerit $A \equiv 1$, generalius probabimus, expressionem $\sqrt[n]{A}$ semper ad aliam $\sqrt[\delta]{B}$ reduci posse cui aequiualeat. Illius enim valore quocunque denotato per x erit $x^n \equiv A$; iam sit t valor quicunque expressionis $\frac{\delta}{n} \pmod{p-1}$, quam valores reales habere ex art. 31 perspicuum; eritque $x^{tn} \equiv A^t$ at $x^{tn} \equiv x^\delta$ propter $tn \equiv \delta \bmod. (p-1)$. Quare $x \equiv A^t$ adeoque quicunque ipsius $\sqrt[n]{A}$ valor erit etiam valor ipsius $\sqrt[\delta]{A^t}$. Quoties igitur $\sqrt[n]{A}$ valores reales habet, expressioni $\sqrt[\delta]{A^t}$ prorsus aequiualens erit, quoniam illa neque alios habet quam haec neque pauciores, licet quando $\sqrt[n]{A}$ nullum valorem realem habet, fieri tamen possit vt $\sqrt[\delta]{A^t}$ valores reales habeat.

Ex. Si valores expressionis $\sqrt[21]{2} \pmod{31}$ quaeruntur, erit numerorum 21 et 30 diuisor

communis maximus 3, expressionisque $\frac{3}{21}$ (mod. 30) valor aliquis 3, quare si $\sqrt[21]{2}$ valores reales habet, huic expressioni $\sqrt[3]{2^3}$ siue $\sqrt[3]{8}$ aequiualebit, inuenieturque reuera, posteriores expressionis valores qui sunt 2, 10, 19 etiam priori satisfacere.

64. Ne autem hanc operationem incassum suscepisse periclitemur, regulam inuestigare oportet, per quam statim diiudicari possit vtrum $\sqrt[n]{A}$ valores reales admittat necne. Quodsi tabula indicum habetur, res in promtu est; namque ex art. 60 manifestum est, valores reales dari, si ipsius A index, radice quacunque primitiua pro basi accepta, per δ sit diuisibilis, sin vero minus, non dari. Attamen hoc etiam absque tali tabula inueniri potest. Posito enim indice ipsius $A = k$, si hic fuerit per δ diuisibilis, erit $\frac{k(p-1)}{\delta}$ per $p-1$ diuisibilis et vice versa. Atqui numeri $A^{\frac{p-1}{\delta}}$ index erit $\frac{k(p-1)}{\delta}$. Quare si $\sqrt[n]{A}$ (mod. p) habet valores reales, $A^{\frac{p-1}{\delta}}$ vnitati congruus erit, sin minus, incongruus. Ita in exemplo art. praec. habetur $2^{10} = 1024 \equiv 1$ (mod. 31), vnde concluditur $\sqrt[21]{2}$ (mod. 31) valores reales habere. Similiter certiores hinc fimus, $\sqrt[2]{-1}$ (mod. p) semper valores binos reales habere, quando p sit formae $4m+1$, nullum vero, quando p sit formae $4m+3$; propter $(-1)^{2m} = 1$ et $(-1)^{2m+1} = -1$. Elegans hoc theorema, quod vulgo ita profertur: *Si p est numerus primus formae $4m+1$, inueniri potest quadratum aa, ita vt $aa+1$ per p fiat diuisibilis; si vero p est formae*

$4m - 1$, *tale quadratum non datur*, hoc modo demonstratum est ab ill. Eulero, *Comm. nou. Acad. Petrop.* T. XVIII. p. 112 ad annum 1773. Demonstrationem aliam iam multo ante dederat, *Comm. nou.* T. V. p. 5 qui prodiit a. 1760. In dissert. priori, Comm. nou. T. IV, p. 25, rem nondum perfecerat. Postea etiam ill. La Grange theorematis demonstrationem tradidit, Nouveaux Mem. de l'Ac. de Berlin A. 1775 p. 342. Aliam adhuc demonstrationem in sectione sequenti vbi proprie de hoc argumento agendum erit, dabimus.

65. Postquam omnes expressiones $\sqrt[n]{A}$ (mod. p) ad tales reducere docuimus, vbi n diuisor numeri $p-1$, criteriumque nacti sumus vtrum valores reales admittat, necne, tales expressiones $\sqrt[n]{A}$ (mod. p) vbi n ipsius $p-1$ est diuisor accuratius considerabimus. Primo ostendemus, quam relationem valores singuli expressionis inter se habeant, tum artificia quaedam trademus, quorum auxilio vnus valor expressionis saepenumero inueniri possit.

Primo, quando $A \equiv 1$, atque r aliquis ex n valoribus expressionis $\sqrt[n]{1}$ (mod. p), siue $r^n \equiv 1$ (mod. p), omnes etiam ipsius r potestates erunt valores istius expressionis; horum autem totidem erunt diuersi quot vnitates habet exponens ad quem r pertinet (art. 48). Quodsi igitur r est valor ad exponentem n pertinens, potestates ipsius r hae $r, r^2, r^3 \ldots r^n$ (vbi loco vltimae *vnitas* substitui potest) omnes expressionis $\sqrt[n]{1}$ (mod. p) valores inuoluent. Qualia

autem subsidia exstent ad tales valores inueniendos qui ad exponentem n pertineant, in sect. VIII fusius explicabimus.

Secundo. Quando A vnitati est incongruus, vnusque expressionis $\sqrt[n]{A}$ (mod. p) notus, qui sit x, reliqui hoc modo inde deducuntur. Sint valores expressionis $\sqrt[n]{1}$, r, $r^2 \ldots r^{n-1}$ (vti modo ostendimus), eruntque omnes expr. $\sqrt[n]{A}$ valores hi: x, xr, $xr^2 \ldots xr^{n-1}$; namque omnes hos congruentiae $x^n \equiv A$ satisfacere inde manifestum quod, posito quocunque eorum $\equiv xr^k$ potestas ipsius n^{ta}, $x^n r^{nk}$, propter $r^n \equiv 1$ et $x^n \equiv A$, vnitati fit congrua: omnes diuersos esse ex art. 23 facile intelligitur; plures autem valores quam hos quorum numerus est n, expressio $\sqrt[n]{A}$ habere nequit. Ita ex. gr. si alter expressionis $\sqrt[2]{A}$ valor est x, alter erit $-x$. Denique hinc concludendum omnes valores expr. $\sqrt[n]{A}$ inuenire non posse, nisi simul omnes valores expr. $\sqrt[n]{1}$ constent.

66. Secundum quod nobis proposueramus fuit, docere, in quo casu vnus expressionis $\sqrt[n]{A}$ (mod. p) valor (vbi n supponitur esse diuisor ipsius $p-1$) directe inueniri possit. Hoc euenit quando aliquis valor potestati alicui ipsius A congruus euadit, qui casus quum haud raro occurrat, aliquantum huic rei immorari non superfluum erit. Sit talis valor, *si quis datur* x, siue $x \equiv A^k$ et $A \equiv x^n$ (mod. p). Hinc colligitur $A \equiv A^{kn}$; quare si numerus k habetur, ita vt sit $A \equiv A^{kn}$, A^k erit valor quaesitus. At huic conditioni aequiualet ista, vt sit $1 \equiv kn$ (mod. t),

designante t exponentem ad quem pertinet A (art. 46, 48). Vt vero haec congruentia possibilis sit, requiritur, vt sit n ad t primus. Hoc in casu erit $k \equiv \frac{1}{n} \pmod{t}$; si vero t et n diuisorem communem habent, nullus valor x potestati ipsius A congruus esse potest.

67. Quum autem ad hanc solutionem ipsum t nouisse oporteat, videamus quomodo procedere possimus, si hunc numerum ignoremus. Primo facile intelligitur, t ipsum $\frac{p-1}{n}$ metiri debere, siquidem $\sqrt[n]{A} \pmod{p}$ valores reales habeat, vti hic semper supponimus. Sit enim quicunque valor y, eritque tum $y^{p-1} \equiv 1$, tum $y^n \equiv A \pmod{p}$; quare eleuando partes posterioris congruentiae ad potestatem $\frac{p-1}{n}$ tam, fiet $A^{\frac{p-1}{n}} \equiv 1$; adeoque $\frac{p-1}{n}$ per t diuisibilis (art 48). Iam si $\frac{p-1}{n}$ ad n est primus, congruentia art. praec. $kn \equiv 1$ etiam secundum modulum $\frac{p-1}{n}$ solui poterit, manifestoque valor ipsius k congruentiae secundum modulum hunc satisfaciens eidem etiam secundum modulum t, qui ipsum $\frac{p-1}{n}$ metitur, satisfaciet, (art. 5). Tum igitur quod quaerebatur inuentum. Si vero $\frac{p-1}{n}$ ad n non est primus, omnes ipsius $\frac{p-1}{n}$ factores primi qui simul ipsum n metiuntur ex $\frac{p-1}{n}$ eiiciantur. Hinc nanciscemur numerum $\frac{p-1}{nq}$, ad n primum, designante q productum ex omnibus illis factoribus primis, quos eiecimus. Quodsi iam conditio ad quam in artic. praec. peruenimus vt t ad n sit primus locum habet, t etiam ad q erit primus adeoque etiam ipsum $\frac{p-1}{nq}$ metietur. Quare si congruen-

entia $kn \equiv 1 \pmod{\frac{p-1}{nq}}$ soluitur (quod fieri potest quia n ad $\frac{p-1}{nq}$ primus), valor ipsius k etiam secundum modulum t congruentiae satisfaciet, id quod quaerebatur. Totum hoc artificium in eo versatur, vt numerus eruatur qui ipsius t, quem ignoramus, vice fungi possit. Attamen probe meminisse oportet, nos quando $\frac{p-1}{n}$ ad n non est primus, supposuisse conditionem art. praec. locum habere, quae si deficit omnes conclusiones erroneae erunt; atque si regulas datas temere sequendo pro x valor inuenitur, cuius potestas n^{ta} ipsi A non sit congrua, indicio hoc est, conditionem deficere adeoque methodum hanc omnino adhiberi non posse.

67. Sed in hocce etiam casu saepe prodesse potest, hunc laborem suscepisse; operaeque pretium est, quomodo hic valor falsus ad veros sese habeat inuestigare. Supponamus itaque numeros k, z rite esse determinatos sed z^n non esse $\equiv A \pmod{p}$. Tum si modo valores expressionis $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$ determinari possint, hos singulos per z multiplicando valores ipsius $\sqrt[n]{A}$ obtinebimus. Si enim v est valor aliquis ipsius $\sqrt[n]{\frac{A}{z^n}}$: erit $(vz)^n \equiv A$. Sed expressio $\sqrt[n]{\frac{A}{z^n}}$ eatenus hac $\sqrt[n]{A}$ simplicior, quod $\frac{A}{z^n} \pmod{p}$ ad exponentem minorem plerumque pertinet quam A. Scilicet si numerorum t, q diuisor communis maximus est d, $\frac{A}{z^n} \pmod{p}$ ad exponentem d pertinebit, id quod ita demonstratur. Substituto pro z valore, fit $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \pmod{p}$. At $kn - 1$ per $\frac{p-1}{nq}$ diuisibilis (art. praec.), $\frac{p-1}{n}$ vero per t (ibid.) siue

siue $\frac{p-}{nd}$ per $\frac{t}{d}$. Atqui $\frac{t}{d}$ ad $\frac{q}{d}$ est primus (hyp.), quare etiam $\frac{p-1}{nd}$ per $\frac{tq}{dd}$ siue $\frac{p-1}{nq}$ per $\frac{t}{d}$, adeoque etiam $kn-1$ per $\frac{t}{d}$ et $(kn-1)\,d$ per t erit diuisibilis. Hinc $A^{(kn-1)d} \equiv 1 \pmod{p}$. Vnde facile deducitur, $\frac{A}{z^n}$ ad potestatem d^{tam} euectum vnitati congruum fieri. Quod vero $\frac{A}{z^n}$ ad exponentem minorem quam d pertinere non possit facile quidem demonstrari potest, sed quoniam ad finem nostrum non requiritur, huic rei non immoramur. Certi igitur esse possumus, $\frac{A}{z^n} \pmod{p}$ semper ad minorem exponentem pertinere, quam A, vnico excepto casu, scilicet quando t ipsum q metitur, adeoque $d = t$.

Sed quid iuuat, quod $\frac{A}{z^n}$ ad minorem exponentem pertinet, quam A? Plures numeri dantur qui possunt esse A quam qui possunt esse $\frac{A}{z^n}$, et quando secundum eundem modulum plures huiusmodi expressiones $\sqrt[n]{A}$ euoluere occasio est, id lucramur vt plures ex eodem fonte haurire possimus. Ita ex. gr. semper vnicum saltem valorem expressionis $\sqrt[2]{A}$ (mod. 29) determinare in potestate erit, si modo expressionis $\sqrt[2]{-1}$ (mod. 29) valores (qui sunt ± 12) innotuerint. Facile enim ex art. praec. perspicitur, huiusmodi expressionum vnum valorem semper directe determinari posse, quando t impar, et d fieri $= 2$ quando t par; praeter -1 autem nullus numerus ad exponentem 2 pertinet.

68. *Exempla.*
Quaeritur $\sqrt[3]{31}$ (mod. 37). Hic $p-1=36$, $n=3$, $\frac{p-1}{3}=12$, adeoque $q=3$: debet igitur esse $3k\equiv 1$ (mod. 4) quod obtinetur ponendo $k=3$. Hinc $x\equiv 31^3$ (mod. 37) $\equiv 6$, inueniturque reuera $6^3\equiv 31$ (mod. 37). Si valores expressionis $\sqrt[3]{1}$ (mod. 37) sunt notae, etiam reliqui expr. $\sqrt[3]{6}$ valores determinari possunt. Sunt vero illi 1, 10, 26, per quos multiplicando ipsum 6, prodeunt reliqui $\equiv 23$ et 8.

Si autem quaeritur valor expr. $\sqrt[2]{3}$ (mod. 37), erit $n=2$, $\frac{p-1}{n}=18$; adeoque $q=2$. Hinc debet esse $2k\equiv 1$ (mod. 9), vnde fit $k\equiv 5$ (mod. 9). Quare $x\equiv 3^5\equiv 21$ (mod. 37); at 21^2 non $\equiv 3$, sed $\equiv 34$; est autem $\frac{3}{34}$ (mod. 37) $\equiv -1$, atque $\sqrt[2]{-1}$ (mod. 37) $\equiv \pm 6$; vnde obtinentur valores veri $\pm 6.\ 21\equiv \pm 15$.

Haec fere sunt, quae hic de talium expressionum euolutione tradere licuit. Palam est methodos directas satis prolixas saepe euasuras: at hoc incommodum tantum non omnibus methodis directis in numerorum theoria incumbit; neque ideo negligendum censuimus, quantum hic praestare valeant ostendere. Etiam hic obseruare conuenit, artificia particularia quae exercitato haud raro se offerunt sigillatim explicare, non esse instituti nostri.

69. Reuertimur nunc ad radices quas diximus primitiuas. Ostendimus, radice primitiua quacunque pro basi assumta omnes numeros, quorum indices ad $p-1$ primi, etiam fo-

re radices primitiuas, nullosque praeter hos; vnde simul radicum primitiuarum multitudo sponte innotescit. V. art. 53. Quamnam autem radicem primitiuam pro basi adoptare velimus, in genere arbitrio nostro relinquitur; vnde intelligitur, etiam hic, vt in calculo logarithmico, plura quasi systemata dari posse *), quae quo vinculo connexa sint videamus. Sint a, b, duae radices primitiuae, aliusque numerus m, atque, quando a pro basi assumitur, index numeri $b \equiv \mathfrak{c}$, numeri m vero index $\equiv \mu$ (mod. $p-1$); quando autem b pro basi assumitur, index numeri $a \equiv \alpha$, numeri m vero $\equiv \nu$, (mod. $p-1$). Tum erit $\alpha\mathfrak{c} \equiv 1$ (mod. $p-1$); namque $a^{\mathfrak{c}} \equiv b$, quare $a^{\alpha\mathfrak{c}} \equiv b^{\alpha} \equiv a$ (mod. p), (hyp.), hinc $\alpha\mathfrak{c} \equiv 1$ (mod. $p-1$). Per simile ratiocinium inuenitur $\nu \equiv \alpha\mu$, atque $\mu \equiv \mathfrak{c}\nu$ (mod. $p-1$). Si igitur tabella indicum pro basi a constructa habetur, facile in aliam conuerti potest, vbi b basis. Si enim pro basi a ipsius b index est $\equiv \mathfrak{c}$, pro basi b ipsius a index erit $\equiv \frac{1}{\mathfrak{c}}$ (mod. $p-1$), multiplicandoque per hunc numerum omnes tabellae indices, habebuntur omnes indices pro basi b.

70. Quamuis autem plures indices numero dato contingere possint, aliis aliisque radicibus primitiuis pro basi acceptis, omnes tamen in eo conuenient, quod omnes eundem diuisorem maximum cum $p-1$ communem ha-

*) In eo autem differunt, quod in logarithmis systematum numerus est infinitus, hic vero tantus, quantus numerus radicum primitiuarum. Manifesto enim bases congruae idem systema generant.

bebunt. Si enim pro basi a, index numeri dati est m, pro basi b vero n, atque diuisores maximi his cum $p-1$ communes, μ, ν supponuntur esse inaequales, alter erit maior, ex. gr. $\mu > \nu$, adeoque μ ipsum n non metietur. At designato indice ipsius a, quando b pro basi assumitur, per α, erit (art. praec.) $n \equiv \alpha m \pmod{p-1}$ adeoque μ etiam ipsum n metietur. *Q. E. A.*

Hunc diuisorem maximum indicibus numeri dati, ipsique $p-1$ communem, a basi non pendere, etiam inde perspicuum, quod aequalis est ipsi $\frac{p-1}{t}$, designante t exponentem ad quem numerus, de cuius indicibus agitur, pertinet. Si enim index pro basi quacunque est k, erit t minimus numerus per quem k multiplicatus ipsius $p-1$ multiplum euadit, (excepta cifra) vidd. artt. 48, 58, siue minimus valor expressionis $\frac{0}{k} \pmod{p-1}$ praeter cifram; hunc autem aequalem esse diuisori maximo communi numerorum k et $p-1$ ex art. 29 nullo negotio deriuatur.

71. Porro facile demonstratur, basin ita semper accipere licere, vt numerus ad exponentem t pertinens indicem quemlibet datum nanciscatur, cuius quidem maximus diuisor cum $p-1$ communis $= \frac{p-1}{t}$. Designemus hunc breuitatis gratia per d, sitque index propositus $\equiv dm$, numerique propositi, quando quaelibet radix prima a pro basi accipitur, index $\equiv dn$, eruntque m, n ad $\frac{p-1}{d}$ siue ad t primi. Tum si $\cdot$ est valor expressionis $\frac{dn}{dm} \pmod{p-1}$, simul-

que ad $p-1$ primus, erit a^s radix primitiua, qua pro basi accepta numerus propositus indicem dm adipiscetur (erit enim $a^{sdm} \equiv a^{dn} \equiv$ numero proposito), id quod desiderabatur. Sed expressionem $\frac{dn}{dm}$ (mod. $p-1$) valores ad $p-1$ primos admittere, ita probatur. Aequiualet illa expressio huic: $\frac{n}{m}$ (mod. $\frac{p-1}{d}$) siue $\frac{n}{m}$ (mod. t) vid. art. 31, 2, eruntque omnes eius valores ad t primi; si enim aliquis valor e diuisorem cum t communem haberet, hic diuisor etiam ipsum me metiri deberet, adeoque etiam ipsum n, cui me secundum t congruus, contra hypoth., ex qua n ad t primus. Quando igitur omnes diuisores primi ipsius $p-1$ etiam ipsum t metiuntur, *omnes* expr. $\frac{n}{m}$ (mod. t) valores ad $p-1$ primi erunt multitudoque eorum $= d$; quando autem $p-1$ alios adhuc diuisores primos, f, g, h etc. implicat, ipsum t non metientes, ponatur valor quicunque expr. $\frac{n}{m}$ (mod. t) $\equiv e$. Tum autem quia omnes t, f, g, h etc. inter se primi, inueniri potest numerus ε, qui secundum t ipsi e, secundum f, g, h etc. vero numeris quibuscunque ad hos respectiue primos fiat congruus. (art. 32) Talis itaque numerus per nullum factorem primum ipsius $p-1$ diuisibilis adeoque ad $p-1$ primus erit, vti desiderabatur. Tandem haud difficile ex combinationum theoria deducitur, talium valorum multitudinem fore $= \frac{\text{p. f}-1.\ \text{g}-1.\ \text{h}-1.\ \text{etc.}}{\text{t. f. g. h. etc.}}$; sed ne digressio haec in nimiam molem excrescat, demonstrationem, quum ad institutum nostrum non sit adeo necessaria, omittimus.

72. Quamuis in genere prorsus arbitrarium sit, quaenam radix primitiua pro basi adoptetur, interdum tamen bases aliae prae aliis commoda quaedam peculiaria praebere possunt. In tabula I semper numerum 10 pro basi assumsimus, quando fuit radix primitiua; alioquin basin ita semper determinauimus vt numeri 10 index euaserit quam minimus, i. e. $= \frac{p-1}{t}$ denotante t exponentem ad quem 10 pertinuit. Quid vero hinc lucremur, in Sect. VI. ostendemus vbi eadem tabula ad alios adhuc vsus adhibebitur. Sed quoniam etiam hic aliquid arbitrarii remanere potest, vt ex art. praec. apparet: vt aliquid certi statueremus, ex omnibus radicibus primitiuis quaesitum praestantibus *minimam* semper pro basi eleximus. Ita pro $p = 73$, vbi $t = 8$ atque $d = 9$, habet $\frac{72.2}{8.3}$ i. e. 6 valores, qui sunt 5, 14, 20, 28, 39, 40. Assumsimus itaque minimum 5 pro basi.

73. Methodi radices primitiuas inueniendi maximam partem tentando innituntur. Si quis ea quae art. 55 docuimus cum iis quae infra de solutione congruentiae $x^n \equiv 1$ trademus confert omnia fere, quae per methodos directas effici possunt, habebit. Ill. Euler confitetur, *Opusc. Analyt. T. I. p.* 152, maxime difficile videri, hos numeros assignare, eorumque indolem ad profundissima numerorum mysteria esse referendam. At tentando satis expedite sequenti modo determinari possunt. Exercitatus operationis prolixitati per multifaria artificia particularia succurrere sciet: haec vero per vsum multo citius quam per praecepta ediscuntur

1°. Assumatur ad libitum numerus ad p (ita semper modulum designamus) primus, a, (plerumque ad calculi breuitatem conducit, si quam minimum accipimus, ex. gr. numerum 2) determineturque eius periodus (art. 46), i. e. residua minima ipsius potestatum, donec ad potestatem a^t perueniatur, cuius residuum minimum sit 1 *). Iam si fuerit $t = p - 1$, a est radix primitiua.

2°. Si vero $t < p - 1$, accipiatur alius numerus b in periodo ipsius a non contentus, inuestigeturque simili modo huius periodus. Designato exponente ad quem b pertinet per u, facile perspicitur u neque ipsi t aequalem neque ipsius partem aliquotam esse posse, in vtroque enim casu fieret $b^t \equiv 1$, quod esse nequit, quum periodus ipsius a omnes numeros amplectatur, quorum potestas exponentis t vnitati congrua (art. 53). Quodsi u fuerit $= p - 1$, erit b radix primitiua; si vero u non quidem $= p - 1$, sed tamen multiplum ipsius t, id lucrati sumus, vt numerus constet ad exponentem maiorem pertinens, adeoque scopo nostro, qui est inuenire numerum ad exponentem *maximum* pertinentem, propiores iam simus. Si vero u neque $= p - 1$, neque ipsius p multiplum, tamen numerum inuenire possumus ad exponentem ipsis t, u maiorem pertinentem, nempe ad exponentem minimo diuiduo communi numerorum t, u, aequalem. Sit hic $= y$, resolua-

*) Quisquis sponte perspiciet, non opus esse has potestates ipsas nouisse, quum cuiusuis residuum minimum facile ex residuo minimo potestatis praecedentis obtineri possit.

turque y ita in duos factores inter se primos, m, n, vt alter ipsum t, alter ipsum u metiatur *). Tum fiat potestas $\frac{t}{m}^{\text{ta}}$ ipsius $a, \equiv A$, potestas $\frac{u}{n}^{\text{ta}}$ ipsius $b, \equiv B \pmod{p}$, eritque productum AB numerus ad exponentem y pertinens; facile enim intelligitur, A ad exponentem m, B ad exponentem n pertinere; adeoque productum AB ad mn pertinebit, quia m, n inter se sunt primi, id quod prorsus eodem modo vti in art. 55, II processimus probari poterit.

3°. Iam si $y = p - 1$, AB erit radix primitiua; sin minus, simili modo vt antea alius numerus adhibendus erit, in periodo ipsius AB non occurrens; eritque hic aut radix primitiua, aut pertinebit ad exponentem ipso y maiorem, aut certe ipsius auxilio (vti ante) numerus ad exponentem ipso y maiorem pertinens inueniri poterit. Quum igitur numeri qui per repetitionem huius operationis prodeunt, ad exponentes continuo crescentes pertineant, manifestum est tandem numerum inuentum iri, qui ad exponentem *maximum* pertineat, i. e. radicem primam, *q. e. f.*

*) Quomodo hoc fieri possit ex art. 18 haud difficulter deriuatur. Resoluatur y in factores tales, qui sint aut numeri primi diuersi aut numerorum primorum diuersorum potestates. Horum quisque alterutrum numerorum t, u metietur (siue etiam vtrumque). Adscribantur singuli aut numero t aut numero u, prout illum aut hunc metiuntur: quando aliquis vtrumque metitur, arbitrarium est, cui adscribatur: productum ex iis qui ipsi t adscripti sunt, sit $= m$, productum e reliquis $= n$, facileque perspicietur m ipsum t, n ipsum u metiri, atque esse $mn = y$.

74. Per exemplum praecepta haec clariora fient. Sit $p = 73$, pro quo radix primitiua quaeratur. Tentemus primo numerum 2, cuius periodus prodit haec:

1. 2. 4. 8. 16. 32. 64. 55. 37. 1. etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. etc.

Quum igitur iam potestas exponentis 9 vnitati congrua fiat, 2 non est radix primitiua. Tentetur alius numerus in periodo ipsius 2 non occurrens ex. gr. 3, cuius periodus est haec:

1. 3. 9. 27. 8. 24. 72. 70. 64. 46. 65. 49. 1 etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12 etc.

Quare neque 3 est radix primitiua. Exponentium autem ad quos 2, 3 pertinent, (i. e. numerorum 9, 12) diuiduus communis minimus est 36, qui in factores 9 et 4 ad praecepta art. praec. resoluitur. Euehendus itaque 2 ad potestatem exponentis $\frac{9}{9}$, i. e. numerus 2 ipse retinendus; 3 autem ad potestatem exponentis 3: productum ex his est 54, quod itaque ad exponentem 36 pertinebit. Si denique ipsius 54 periodus computatur numerusque in hac non contentus ex. gr. 5 denuo tentatur, hunc esse radicem primitiuam, reperietur.

75. Antequam hoc argumentum deseramus, propositiones quasdam trademus, quae ob simplicitatem suam attentione haud indignae videntur.

Productum ex omnibus terminis periodi numeri cuiusuis est $\equiv 1$, *quando ipsorum multitudo, siue exponens ad quem numerus pertinet, est impar, et* $\equiv -1$, *quando ille exponens est par.*

Ex. Pro modulo 13, periodus numeri 5 constat ex his terminis, 1, 5, 12, 8 quorum productum $480 \equiv -1 \pmod{13}$.

Secundum eundem modulum periodus numeri 3 constat e terminis 1, 3, 9 quorum productum $27 \equiv 1 \pmod{13}$.

Demonstr. Sit exponens, ad quem numerus pertinet, t, atque index numeri, $\frac{p-1}{t}$, id quod si basis rite determinatur semper fieri potest (art. 71). Tum index producti ex omnibus periodi terminis erit $\equiv (1 + 2 + 3 + \text{etc.} + t - 1) \frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$ i. e. $\equiv 0 \pmod{p-1}$ quando t impar, et $\equiv \frac{p-1}{2}$, quando t par; hinc in priori casu productum illud $\equiv 1 \pmod{p}$; in posteriori vero $\equiv -1 \pmod{p}$, (art. 62). *Q. E. D.*

76. Si numerus iste in theor. praecedente est radix primitiua, eius periodus omnes numeros $1, 2, 3, \ldots\ldots p-1$ comprehendet, quorum productum itaque semper $\equiv -1$ (namque $p-1$ semper par, vnico casu $p=2$ excepto in quo -1 et $+1$ aequiualent). Theorema hoc elegans quod ita enunciari solet: *productum ex omnibus numeris numero primo dato minoribus, vnitate auctum per hunc primum est diuisibiles*, primum a cel. Waring est prolatum armigeroque Wilson adscriptum, *Meditt. algebr. Ed.* 3, *p.* 380. Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla *notatio* fingi possit, quae numerum primum exprimat. — At nostro quidem iudi-

cio huiusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. Postea ill. La Grange demonstrationem dedit, *Nouv. Mem. de l'Ac. de Berlin*, 1771. Innititur ea considerationi coefficientium ex euolutione producti $x+1$. $x+2$. $x+3$ .... $x+p-1$ oriundarum. Scilicet posito hoc producto $= x^{p-1} + Ax^{p-2} + Bx^{p-3} +$ etc. $+ Mx + N$, coefficientes A, B, *etc.*, M per p erunt diuisibiles, N vero erit $= 1.2.3 .... p-1$. Iam pro $x = 1$, productum per p diuisibile; tunc autem erit $\equiv 1 + N \pmod{p}$; quare necessario $1 + N$ per p diuidi poterit.

Denique ill. Euler in *Opusc. analyt. T. I. p.* 329 demonstrationem dedit, cum ea quam nos hic exposuimus conspirantem. Quodsi tales viri theorema hoc meditationibus suis non indignum censuerunt, non improbatum iri speramus, si aliam adhuc demonstrationem apponimus.

77. Quando secundum modulum p, productum duorum numerorum a, b vnitati est congruum, numeros a, b cum ill. Euler, *socios* vocemus. Tum secundum sect. praec. quiuis numerus positiuus ipso p minor socium habebit positiuum ipso p minorem et quidem vnicum. Facile autem probari potest ex numeris $1, 2, 3 .... p-1$; 1 et $p-1$ esse vnicos qui sibi ipsis sint socii: numeri enim sibi ipsis socii, radices erunt congruentiae $xx \equiv 1$; quae quoniam est secundi gradus plures quam duas radices, i. e. alias quam 1 et $p-1$ habe-

re nequit. Abiectis itaque his numerorum reliquorum 2, 3 .... $p-2$ bini semper erunt associati; quare productum ex ipsis erit $\equiv 1$ adeoque productum ex omnibus 1, 2, 3 ... $p-1$, $\equiv p-1$ siue $\equiv -1$. *Q. E. D.*

Ex. gr. pro $p=13$ numeri 2, 3, 4 .... 11 ita associantur: 2 cum 7; 3 cum 9; 4 cum 10; 5 cum 8; 6 cum 11; scilicet $2.7\equiv 1$; $3.9\equiv 1$ etc. Hinc $2.3.4 \ldots 11 \equiv 1$; adeoque $1.2.3 \ldots 12 \equiv -1$.

78. Potest autem theorema Wilsonianum generalius sic proponi. *Productum ex omnibus numeris, numero* quocunque *dato A minoribus simulque ad ipsum primis, congruum est secundum A, vnitati vel negatiue vel positiue sumtae.* Negatiue sumenda est vnitas, quando A est formae p^m, aut huiusce, $2p^m$, designante p numerum primum a 2 diuersum, insuperque quando $A=4$; positiue autem in omnibus casibus reliquis. Theorema, quale a cel. Wilson est prolatum, sub casu priori continetur. — Ex. gr. pro $A=15$ productum e numeris 1, 2, 4, 7, 8, 11, 13, 14 est $\equiv 1$ (mod. 15). Demonstrationem breuitatis gratia non adiungimus: obseruamus tantum, eam simili modo perfici posse vt in art. praec., excepto quod congruentia $xx\equiv 1$ plures quam duas radices habere potest, quae considerationes quasdam peculiares postulant. Posset etiam demonstratio ex consideratione indicum peti, similiter vt in art. 75, si ea quae mox de modulis non primis trademus conferantur.

79. Reuertimur ad enumerationem aliarum propositionum (art. 75).

Summa omnium terminorum periodi numeri cuiusuis est $\equiv o$, vti in ex art. 75, $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$.

Dem. Numerus de cuius periodo agitur, sit $= a$, atque exponens ad quem pertinet, $= t$, eritque summa terminorum omnium periodi, $\equiv 1 + a + aa + a^3 + \text{etc.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}$. At $a^t - 1 \equiv 0$: quare summa haec semper erit $\equiv 0$ (art. 22), nisi forte $a - 1$ per p sit diuisibilis, siue $a \equiv 1$; hunc igitur casum excipere oportet, si vel vnum terminum, *periodum* vocare velimus.

80. *Productum ex omnibus radicibus primitiuis est* $\equiv 1$, excepto vnico casu, $p = 3$; tum enim vna tantum datur radix prima, 2.

Demonstr. Si radix primitiua quaecunque pro basi assumitur, indices radicum omnium primitiuarum erunt numeri ad $p - 1$ primi simulque ipso minores. At horum numerorum summa, i. e. index producti ex omnibus radicibus primitiuis, est $\equiv 0 \pmod{p - 1}$ adeoque productum $\equiv 1 \pmod{p}$; facile enim perspicitur, si k fuerit numerus ad $p - 1$ primus, etiam $p - 1 - k$ ad $p - 1$ primum fore adeoque binos numeros ad $p - 1$ primos summam constituere per $p - 1$ diuisibilem; (k autem ipsi $p - 1 - k$ numquam aequalis esse potest, praeter casum, $p - 1 = 2$, siue $p = 3$, quem exce-

pimus; manifesto enim $\frac{p-1}{2}$ in omnibus reliquis casibus ad $p-1$ non est primus).

81. *Summa omnium radicum primitiuarum est aut* $\equiv 0$ (quando $p-1$ per *quadratum* aliquod est diuisibilis), *aut* $\equiv \pm 1$ (*mod.* p), (quando $p-1$ est productum e numeris primis inaequalibus; quorum multitudo si est par signum positiuum, si vero impar, negatiuum sumendum).

Ex. 1° pro $p=13$, habentur radices primitiuae 2, 6, 7, 11, quarum summa $26 \equiv 0$ (mod. 13). 2° pro $p=11$, radices primitiuae sunt 2, 6, 7, 8 quarum summa $23 \equiv +1$ (mod. 11). 3° pro $p=31$, radices primitiuae sunt 3, 11, 12, 13, 17, 21, 22, 24, quarum summa, $123 \equiv -1$ (mod. 31).

Demonstr. Supra demonstrauimus (art. 55, II), si p fuerit $= a^\alpha b^\beta c^\gamma$ etc. (designantibus a, b, c etc. numeros primos inaequales) atque A, B, C numeri quicunque ad exponentes a^α, b^β, c^γ etc. respectiue pertinentes, omnia producta ABC etc. exhibere radices primitiuas. Facile vero etiam demonstrari potest, quamuis radicem primitiuam per huiusmodi productum exhiberi posse et quidem vnico tantum modo *).

*) Determinentur scilicet numeri $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. ita, vt sit $\mathfrak{a} \equiv 1$ (mod. a^α) et $\equiv 0$ (mod. $b^\beta c^\gamma$ etc.); $\mathfrak{b} \equiv 1$ (mod. b^β) et $\equiv 0$ (mod. $a^\alpha c^\gamma$ etc.) etc. (vid. art. 32), vnde fiet $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} +$ etc. $\equiv 1$ (mod. $p-1$), (art. 19). Iam si radix primitiua quaecunque r, per productum ABC etc. exhiberi debet accipiatur $A \equiv r\mathfrak{a}$, $B \equiv r\mathfrak{b}$, $C \equiv r\mathfrak{c}$ etc., atque pertinebunt A ad exponentem a^α, B ad exponentem b^β etc.; productumque ex omnibus A, B, C etc. erit $\equiv r$ (mod. p); denique facile perspicitur A, B, C etc, alio modo determinari non posse.

Vnde sequitur haec producta loco ipsarum radicum primitiuarum accipi posse. At quoniam in his productis omnes valores ipsius A cum omnibus ipsius B etc. combinari oportet, omnium horum productorum summa aequalis est producto ex summa omnium valorum ipsius A, in summam omnium valorum ipsius B, in summam omnium valorum ipsius C etc. vti ex doctrina combinationum notum est. Designentur omnes valores ipsorum A; B etc., per A, A', A'' etc.; B, B', B'' etc. etc., eritque summa omnium radicum primitiuarum $\equiv (A + A' +$ etc.) $(B + B' +$ etc.) etc. Iam dico, si exponens α fuerit $= 1$, summam $A + A' + A'' +$ etc. fore $\equiv -1 \pmod{p}$, si vero α fuerit > 1, summam hanc fore $\equiv 0$. similiterque de reliquis $\mathfrak{C}, \gamma$ etc. Simulac haec erunt demonstrata, theorematis nostri veritas manifesta erit. Quando enim $p - 1$ per quadratum aliquod diuisibilis est, aliquis exponentium $\alpha, \mathfrak{C}, \gamma$ etc. vnitatem superabit, adeoque aliquis factorum, quorum producto congrua est summa omnium radicum primitiuarum, erit $\equiv 0$, et proin etiam productum ipsum: quando vero $p - 1$ per nullum quadratum diuidi potest, omnes exponentes $\alpha, \mathfrak{C}, \gamma$ etc. erunt $= 1$, vnde summa omnium radicum primitiuarum congrua erit producto ex tot factoribus, quorum quisque $\equiv -1$, quot habentur numeri a, b, c etc., adeoque erit $\equiv \pm 1$, prout horum numerorum multitudo par vel impar. Illa autem ita probantur.

1°. Quando $\alpha = 1$ atque A numerus ad exponentem a pertinens, reliqui numeri ad hunc

exponentem pertinentes erunt A^2, A^3 .... A^{a-1}. At $1 + A + A^2 + A^3 .... + A^{a-1}$ est summa periodi completae, adeoque $\equiv 0$ (art. 79), quare $A + A^2 + A^3 .... + A^{a-1} \equiv -1$.

2°. Quando autem $\alpha > 1$, atque A numerus ad exponentem a^α pertinens, reliqui numeri ad hunc exponentem pertinentes habebuntur, si ex his A^2, A^3, A^4 .... $A^{a^\alpha-1}$ reiiciuntur A^a, A^{2a}, A^{3a} etc., vid. art. 53; quare summa eorum erit $\equiv 1 + A + A^2 .... + A^{a^\alpha-1} - (1 + A^a + A^{2a} .... + A^{a^\alpha-a})$ i. e. congrua differentiae duarum periodorum, adeoque $\equiv 0$. *Q. E. D.*

82. Omnia quae hactenus exposuimus innituntur suppositioni, modulum esse numerum primum. Superest vt eum quoque casum consideremus, vbi pro modulo assumitur numerus compositus. Attamen quum hic neque proprietates tam elegantes eniteant, quam in casu priori, neque ad eas inueniendas artificiis subtilibus sit opus, sed potius omnia fere per solam principiorum praecedentium applicationem erui possint, omnes minutias hic exhaurire superfluum atque taediosum foret. Breuiter itaque quae huic casui cum priori sint communia quaeque propria exponemus.

83. Propositiones art. 45 — 48 generaliter iam sunt demonstratae. At prop. art. 49 ita immutari debet:

Si f designat, quot numeri dentur ad m primi simulipso m minores, i. e. si $f = \varphi m$ (art. 38): exponens, t, infimae potestatis numeri dati, a, ad m primi, quae secundum modulum m vnitati est congrua, vel erit $= f$ vel pars aliquota huius numeri.

Demonstratio prop. art. 49 etiam pro hoc casu valere potest, si modo vbique loco ipsius p, m, loco ipsius $p-1$, f, et loco numerorum $1, 2, 3, \ldots p-1$, numeri ad m primi simulque ipso m minores substituantur. Huc itaque lectorem ablegamus. Ceterum demonstrationes reliquae de quibus illic locuti sumus (art. 50, 51) non sine multis ambagibus ad hunc casum applicari possunt. — At respectu propositionum sequentium, art. 52 *sqq.* magna differentia incipit inter modulos, qui numerorum primorum sunt potestates, eosque, qui per plures numeros primos diuidi possunt. Seorsim itaque modulos prioris generis contemplabimur.

84. Si modulus $m = p^n$, designante p numerum primum, erit $f = p^{n-1}(p-1)$ (art. 38.) Iam si disquisitiones in artt. 51, 55 contentae ad hunc casum applicantur, mutatis mutandis vti in art. praec. praescripsimus, inuenietur, omnia quae ibi demonstrata sunt etiam pro hoc casu locum habere, si modo ante probatum esset, congruentiam, formae $x^t - 1 \equiv 0$ (mod. p^n) plures quam t radices diuersas habere non posse. Pro modulo primo hanc veritatem ex propositione generaliori art. 43 deduximus, quae autem in omni sua extensione de modulis primis tantummodo valet, neque adeo ad hunc casum applicanda. Attamen propositionem pro hoc casu particulari veram esse per methodum singularem demonstrabimus. Infra (sect. VIII.) idem facilius inuenire docebimus.

Demonstrandum proponimus nobis hoc theorema: *Si numerorum t et* $p^{n-1}(p-1)$ *diuisor communis maximus est e, congruentia* $x^t \equiv 1 \pmod{p^n}$ *habebit e radices diuersas.*

Sit $e = kp^\nu$ ita vt k factorem p non inuoluat, adeoque numerum $p-1$ metiatur. Tum congruentia $x^t \equiv 1$ secundum modulum p habebit k radices diuersas, quibus per A, B, C etc. designatis, radix quaecunque eiusdem congruentiae secundum modulum p^n, congrua esse debet secundum modulum p alicui numerorum A, B, C etc. Iam demonstrabimus, congruentiam $x \equiv 1 \pmod{p^n}$ habere p^ν radices ipsi A, totidem ipsi B etc. congruas secundum modulum p. Quo facto omnium radicum numerus erit kp^ν siue e, vti diximus. Illam vero demonstrationem ita adornabimus, vt *primo* ostendamus, si α fuerit radix ipsi A secundum modulum p congrua, etiam $\alpha + p^{n-\nu}$, $\alpha + 2p^{n-\nu}$, $\alpha + 3p^{n-\nu}$, ... $\alpha + (p^\nu - 1)\,p^{n-\nu}$ fore radices; *secundo*, numeros ipsi A secundum modulum p congruos alios quam qui in forma $\alpha + hp^{n-\nu}$ sint comprehensi (denotante h integrum quemcunque), radices esse non posse: vnde manifesto p^ν radices diuersae habebuntur, et non plures: atque idem etiam de radicibus, quae singulis B, C etc. sunt congruae, locum habebit: *tertio* docebimus, quomodo semper radix, ipsi A secundum p congrua, inueniri possit.

86. Theorema. *Si vti in art. praec. t est numerus per* p^ν, *neque vero per* $p^{\nu+1}$ *diuisibilis, erit* $(\alpha +$

$hp^\mu)^t - \alpha^t \equiv o \pmod{p^{\mu+\nu}}$, at $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$ Theorematis pars posterior locum non habet, quando $p = 2$ simulque $\mu = 1$.

Demonstratio huius theorematis ex euolutione potestatis binomii peti posset, si ostenderetur omnes terminos post secundum per $p^{\mu+\nu+1}$ diuisibiles esse. Sed quoniam consideratio denominatorum coefficientium in aliquot ambages deducit, methodum sequentem praeferimus.

Ponamus *primo* $\mu > 1$ atque $\nu = 1$, eritque, propter $x^t - y^t = (x - y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{etc.} + y^{t-1})$, $(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha$ etc. $+ \alpha^{t-1})$. At est $\alpha + hp^\mu \equiv \alpha \pmod{p^2}$, quare quisque terminus $(\alpha + hp^\mu)^{t-1}$, $(\alpha + h^\mu)^{t-2}\alpha$ etc. erit $\equiv \alpha^{t-1} \pmod{p^2}$ adeoque omnium summa $\equiv t\,\alpha^{t-1} \pmod{p^2}$ siue formae $t\,\alpha^{t-1} + V p^2$ denotante V numerum quemcunque. Hinc $(\alpha + hp^\mu)^t - \alpha^t$ erit formae $\alpha^{t-1} hp^\mu t + Vhp^{\mu+2}$, i. e. $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+}}$ et $\equiv o \pmod{p^{\mu+1}}$ Pro hoc itaque casu theorema est demonstratum.

Iam si theorema pro aliis ipsius ν valoribus verum non esset, manente etiamnum $\mu > 1$, limes aliquis necessario daretur, vsque ad quem theorema semper verum foret, vltra vero falsum. Sit minimus valor ipsius ν, pro quo falsum est $= \varphi$, vnde facile perspicitur, si t per $p^{\varphi-1}$ non autem per p^φ fuerit diuisibi-

lis, theorema adhuc verum esse, at si loco ipsius t substituatur tp, falsum. Habemus itaque

$$(\alpha + hp^\mu)^t \equiv \alpha^t + \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\varphi}}$$

siue $= \alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varphi}$ denotante u numerum indeterminatum. At quia pro $\nu = 1$ theorema iam est demonstratum, erit $(\alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1} hp^{\mu+1} t + \alpha^{tp-t} up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$,

adeoque etiam

$(\alpha + hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1} hp^\mu tp \pmod{p^{\mu+\varphi+1}}$ i. e. theorema etiam verum, si loco ipsius t substituitur tp, i. e. etiam pro $\nu = \varphi + 1$, contra hypothesin. Vnde manifestum pro omnibus ipsius ν valoribus theorema verum esse.

87. Superest casus vbi $\mu = 1$. Per methodum prorsus similem ei qua in art. praec. vsi sumus, sine adiumento theorematis binomialis demonstrari potest, esse

$$(\alpha + hp)^{t-1} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-1)\,hp \pmod{p^2}$$
$$\alpha\,(\alpha + hp)^{t-2} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-2)\,hp$$
$$\alpha\alpha\,(\alpha + hp)^{t-3} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-3)\,hp$$

etc.

vnde aggregatum erit (quia partium multitudo $= t$)

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\,\alpha^{t-2} hp \pmod{p^2}$$

At quoniam t per p diuisibilis, etiam $\frac{(t-1)t}{2}$ per p diuisibilis erit in omnibus casibus excepto eo vbi $p = 2$ de quo iam in art.

praec. monuimus. In reliquis autem casibus erit $\frac{(t-1)t}{2} \alpha^{t-2} hp \equiv 0 \pmod{p^2}$, adeoque etiam illud aggregatum $\equiv t\alpha^{t-2} \pmod{p^2}$ vt in art. praec. In reliquis demonstratio hic eodem modo procedit vt istic.

Colligimus igitur generaliter vnico casu $p = 2$ excepto, esse
$(\alpha + hp^\mu)^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$ et
$(\alpha + hp^\mu)^t$ *non* $\equiv \alpha^t$ pro quouis modulo quisit altior potestas ipsius p, quam haec, $p^{\mu+\nu}$, quoties quidem h per p non est diuisibilis, atque p^ν potestas suprema ipsius p quae numerum t diuidit.

Hinc protinus deriuantur propositiones 1. et 2. quas art. 85 demonstrandas nobis proposueramus: scilicet

primo, si $\alpha^t \equiv 1$, erit etiam $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

secundo si numerus aliquis α' ipsi A adeoque etiam ipsi α secundum modulum p congruus, neque vero huic secundum modulum $p^{n-\nu}$, congruentiae $x^t \equiv 1 \pmod{p^n}$ satisfaceret, ponamus α' esse $= \alpha + lp^\lambda$, ita vt l per p non sit diuisibilis, eritque $\lambda < \mu - \nu$, tunc autem $(\alpha + lp^\lambda)^t$ secundum modulum $p^{\lambda+\nu}$ ipsi α^t congruus erit, non autem secundum modulum p^μ, quae est altior potestas, quare α' radix congruentiae $x^t \equiv 1$ esse nequit.

88. *Tertium* vero fuit radicem aliquam congruentiae $x^t \equiv 1 \pmod{p_n}$, ipsi A con-

gruam, inuenire. Ostendemus hic tantummodo quomodo hoc fieri possit, si iam radix eiusdem congruentiae secundum modulum p^{n-1} innotuerit; manifesto hoc sufficit, quum a modulo p pro quo A est radix, ad modulum p^2, sicque deinceps ad omnes potestates consecutiuas progredi possimus.

Esto itaque α radix congruentiae $x^t \equiv 1 \pmod{p^{n-1}}$ quaeriturque radix eiusdem congruentiae secundum modulum p^n, ponatur haec $= \alpha + hp^{n-\nu-1}$, quam formam eam habere debere ex art. praec. sequitur (casum vbi $\nu = n-1$ postea seorsim considerabimus: maior vero quam $n-1$, ν esse nequit). Debet itaque esse $(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^n}$. At $(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$ Si itaque h ita demerminatur, vt fiat $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$; siue (quia per hyp. $1 \equiv \alpha^t \pmod{p^{n-1}}$ atque t per p^ν diuisibilis) ita vt fiat $\frac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1} h\frac{t}{p^\nu}$ per p diuisibilis, quaesito satisfactum erit. Hoc autem semper fieri posse ex Sect. praec. manifestum, quum t per altiorem ipsius p potestatem quam p^ν diuidi non posse hic supponamus, adeoque $\alpha^{t-1}\frac{t}{p^\nu}$ ad p sit primus.

Si vero $\nu = n-1$ i. e. t per p^{n-1} siue etiam per altiorem ipsius p potestatem diuisibilis quiuis valor A, congruentiae $x^t \equiv 1$ secundum modulum p satisfaciens eidem etiam secundum modulum p^n satisfaciet. Sit enim

$t = p^{n-1} \tau$, eritque $t \equiv \tau \pmod{p-1}$: quare quoniam $A^t \equiv 1 \pmod{p}$ erit etiam $A^\tau \equiv 1 \pmod{p}$. Ponatur itaque $A^\tau = 1 + hp$ eritque $A^t = (1 + hp)^{p^{n-1}} \equiv 1 \pmod{p^n}$ art. 87.

89. Omnia quae art. 57 sqq. adiumento theorematis, congruentiam $x^t \equiv 1$ plures quam t radices diuersas non habere eruimus, etiam pro modulo qui est numeri primi potestas locum habent, et si *radices primitiuae* vocantur numeri, qui ad exponentem $p^{n-1}(p-1)$ pertinent, siue in quorum periodis omnes numeri per p non diuisiuiles inueniuntur, etiam hic radices primitiuae exstabunt. Omnia autem quae supra de indicibus eorumque vsu tradidimus, nec non de solutione congruentiae $x^t \equiv 1$, ad hunc quoque casum applicari possunt. Quae quum nulli difficultat obnoxia sint omnia ex integro repetere superfluum foret. Praeterea radices congruentiae $x^t \equiv 1$ secundum modulum p^n e radicibus eiusdem congruentiae secundum p deducere docuimus. Sed de eo casu, ubi potestas aliqua numeri 2 est modulus quia supra exceptus fuit, aliqua adhuc sunt adiicienda.

90. *Si potestas aliqua numeri 2, altior quam secunda, puta 2^n pro modulo accipitur, numeri cuiusuis imparis potestas exponentis 2^{n-2}, vnitati est congrua.*

Ex. gr. $3^8 = 6561 \equiv 1 \pmod{32}$.

Quiuis enim numerus impar vel sub forma $1 + 4h$, vel sub hac $-1 + 4h$ compre-

henditur: vnde propositio protinus sequitur (theor. art. 85).

Quoniam igitur exponens ad quem quicunque numerus impar secundum modulum 2^n pertinet, diuisor ipsius 2^{n-2} esse debet, quiuis ad aliquem horum numerum pertinebit 1, 2, 4, 8. . . . 2^{2n-2}, ad quemnam vero pertineat ita facile diiudicatur. Sit numerus propositus $= 4h \pm 1$, atque exponens maximae potestatis numeri 2, quae ipsum h metitur, $= m$ (qui etiam $= o$ esse potest, quando scilicet h est impar); tum exponens ad quem numerus propositus pertinet, erit $= 2^{n-m-2}$, siquidem $n > m + 2$; si autem $n =$ vel $< m + 2$, numerus propositus est $\equiv \pm 1$ adeoque vel ad exponentem 1 vel ad exponentem 2 pertinebit. Numerum enim formae $\pm 1 + 2^{m+1}k$, (quae huic aequiualet, $4h \pm 1$) ad potestatem exponentis 2^{n-m-2} eleuatum vnitati secundum modulum 2^n congruum fieri, ad potestatem autem exponentis, qui est inferior numeri 2 potestas, incongruum, ex art. 86 nullo negotio deducitur. Numerus itaque quicunque formae $8k + 3$ vel $8k + 5$ ad exponentem 2^{n-2} pertinebit.

91. Hinc patet eo sensu quo supra expressionem accepimus, *radices primitiuas* hic non dari, nullos scilicet numeros, quorum periodus omnes numeros modulo minores ad ipsumque primos amplectatur. Attamen facile perspicitur, analogon hic haberi. Inuenitur enim, numeri formae $8k + 3$ potestatem exponentis imparis semper esse formae $8k + 3$,

potestatem autem exponentis paris, semper formae $8k + 1$; nulla igitur potestas formae $8k + 7$ esse potest. Quare quum periodus numeri formae $8k + 3$, ex 2^{n-2} terminis diuersit constet, quorum quisque aut formae $8k + 3$ aut huius, $8k + 1$, neque plures huiusmodi numeri modulo minores dentur quam 2^{n-2}, manifesto, quiuis numerus formae $8k + 1$ vel $8k + 3$ congruus est secundum modulum 2^n potestati alicui numeri cuiuscunque formae $8k + 3$. Simili modo ostendi potest periodum numeri formae $8k + 5$ comprehendere omnes numeros formarum $8k + 1$ et $8k + 5$. Si igitur numerus formae $8k + 5$ pro basi assumitur, omnes numeri formae $8k + 1$ et $8k + 5$, positiue, omnesque formae $8k + 3$ et $8k + 7$, negatiue sumti, indices reales nanciscentur, et quidem hic indices secundum 2^{n-2} congrui pro aequiualentibus sunt habendi. Hoc modo tabula nostra I intelligenda, vbi pro modulis 16, 32 et 64 (namque pro modulo 8 nulla tabula necessaria erit) semper numerum 5 pro basi accepimus. Ex. gr. numero 19 qui est formae $8n + 3$ adeoque *negatiue* sumendus, respondet pro modulo 64 index 7, id quod significat esse $5^7 \equiv -19 \pmod{64}$. Numeris autem formarum $8n + 1$, $8n + 5$ negatiue, atque numeris formarum $8n + 3$, $8n + 7$ positiue acceptis, indices quasi imaginarii tribuendi forent. Quos introducendo calculus indicum ad algorithmum perquam simplicem reduci potest. Sed quoniam, si haec ad omnem rigorem exponere vellemus, nimis longe euagari oporteret, hoc negotium ad aliam occasionem

nobis reseruamus, quando forsan fusius quantitatum imaginarium theoriam, quae nostro quidem iudicio a nemine hactenus ad notiones claras est reducta, pertractare suscipiemus. Periti hunc algorithmum facile ipsi eruent: qui minus sunt excercitati, perinde tamen tabula hac vti poterunt, vt ii qui recentiorum commenta de *logarithmis* imaginariis ignorant, logarithmis vtuntur, si quidem principia supra stabilita probe tenuerint.

92. Secundum modulum e pluribus primis compositum tantum non omnia quae ad residua potestatum pertinent ex theoria congruentiarum generali deduci possunt; quia vero infra congruentias quascunque secundum modulum e pluribus primis compositum ad congruentias, quarum modulus est primus aut primi potestas, reducere fusius docebimus, non est quod huic rei multum hic immoremur. Obseruamus tantum, bellissimam proprietatem, quae pro reliquis modulis locum habeat, quod scilicet semper exstent numeri quorum periodus omnes numeros ad modulum primos complectatur, hic deficere, excepto vnico casu, quando scilicet modulus est duplum numeri primi, aut potestatis numeri primi. Si enim modulus m redigitur ad formam $A^{a}B^{b}C^{c}$ etc. designantibus A, B, C etc. numeros primos diuersos, praeterea A^{a-1} $(A-1)$ disignatur per α, B^{b-1} $(B-1)$ per β etc. denique z est numerus ad m primus; erit $z^{\alpha} \equiv 1 \pmod{A^{a}}$ $z^{\beta} \equiv 1 \pmod{A^{b}}$ etc. Quodsi igitur μ est minimus numerorum α, β, γ etc. diuiduus communis, erit

$x^\mu \equiv 1$ secundum omnes modulos A^a, B^b etc. adeoque etiam secundum m, cui illorum productum est aequale. At excepto casu vbi m est duplum numeri primi aut potestatis numeri primi, numerorum α, β, γ etc. diuiduus communis minimus, ipsorum producto est minor (quoniam numeri α, β, γ etc. inter se primi esse nequeunt sed certe diuisorem 2 communem habent). Nullius itaque numeri periodus tot terminos comprehendere potest, quot dantur numeri ad modulum primi ipsoque minores, quia horum numerus producto ex α, β, γ etc. est aequalis. Ita ex. gr. pro $m = 1001$ cuiusuis numeri ad m primi potestas exponentis 60 vnitati est congrua, quia 60 est diuiduus communis numerorum 6, 10, 12. — Casus autem vbi modulus est duplum numeri primi aut duplum potestatis numeri primi illi vbi est primus aut primi potestas prorsus est similis.

93, Scriptorum in quibus alii geometrae de argumento in hac sectione pertractato egerunt, iam passim mentio est facta. Eos tamen qui quaedam fusius, quam nobis breuitas permisit, explicata desiderant, ablegamus imprimis ad sequentes ill. Euleri commentationes, ob perspicuitatem qua vir summus prae omnibus semper excelluit, maxime commendabiles.

Theoremata circa residua ex diuisione potestatum relicta. Com. nou. Petr. T. VII. p. 49. sqq.

Demonstrationes circa residua ex diuisione potestatum per numeros primos resultantia. Ibid. T. XVIII. p. 85 sqq.

Adiungi his possunt *Opusculorum analyt.* T. I, *dissertt.* 5 et 8.

Sectio Qvarta

de

CONGRVENTIIS SECVNDI GRADVS.

94. Theorema. *Numero quocunque, m, pro modulo accepto, ex numeris 0, 1, 2, 3.... $m-1$, plures quam $\frac{1}{2}m+1$ quando m est' par, siue plures quam $\frac{1}{2}m+\frac{1}{2}$, quando m est impar quadrato congrui fieri non possunt.*

Dem. Quoniam numerorum congruorum quadrata sunt congrua: quiuis numerus, qui vlli quadrato congruus fieri potest, etiam quadrato alicui cuius radix $< m$ congruus erit. Sufficit itaque residua minima quadratorum 0, 1, 4, 9.... $(m-1)^2$ considerare. At facile perspicitur, esse $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$ etc. Hinc etiam, quando m est par, quadratorum $\frac{1}{2}(m-1)^2$ et $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ et $(\frac{1}{2}m+2)^2$ etc. residua minima eadem erunt: quando vero m est impar, quadrata $(\frac{1}{2}m-\frac{1}{2})^2$ et $(\frac{1}{2}m+\frac{1}{2})^2$; $(\frac{1}{2}m-\frac{3}{2})^2$ et $(\frac{1}{2}m+\frac{3}{2})^2$ etc. erunt congrua. Vnde palam est, alios numeros, quam qui alicui ex quadratis 0, 1,

4, 9.... $(\frac{1}{2}m)^2$ congrui sint, quadrato congruos fieri non posse, quando m par; quando vero impar, quemuis numerum, qui vlli quadrato sit congruus, alicui ex his 0, 1, 4, 9... $(\frac{1}{2}m - \frac{1}{2})^2$ necessario congruum esse. Quare dabuntur ad summum in priori casu $\frac{1}{2}m + 1$ residua minima diuersa, in posteriori $\frac{1}{2}m + \frac{1}{2}$ *Q. E. D.*

95. *Exemplum.* Secundum modulum 13 quadratorum numerorum 0, 1, 2, 3... 6 residua minima inueniuntur, 0, 1, 4, 9, 3, 12, 10, post haec vero eadem ordine inuerso recurrunt 10, 12, 3, etc. Quare numerus quisque, nulli ex istis residuis congruus, siue qui alicui ex his est congruus, 2, 5, 6, 7, 8, 11, nulli quadrato congruus esse potest.

Secundum modulum 15 haec inueniuntur residua, 0, 1, 4, 9, 1, 10, 6, 4 post quae eadem ordine inuerso recurrunt. Hic igitur numerus residuuorum, quae quadrato congrua fieri possunt, minor adhuc est, quam $\frac{1}{2}n + \frac{1}{2}$, quum sint 0, 1, 4, 6, 9, 10. Numeri autem 2, 3, 5, 7, 8, 11, 12, 13, 14, et qui horum alicui sunt congrui, nulli quadrato secundum mod. 15 congrui fieri possunt.

96. Hinc colligitur, pro quouis modulo omnes numeros in duas classes distingui posse, quarum altera contineat numeros, qui quadrato alicui congrui fieri possint, altera eos qui non possint. Illos appellabimus *residua quadratica*

numeri istius quem pro modulo accepimus *), hos vero *ipsius non-residua quadratica*, siue etiam, quoties ambiguitas nulla inde oriri potest, simpliciter *residua* et *non-residua*. Ceterum palam est sufficere, si omnes numeri 0, 1, 2... $m-1$ in classes redacti sint: numeri enim congrui ad eandem classem erunt referendi.

Etiam in hac disquisitione a modulis primis initium faciemus, quod itaque subintelligendum erit, etiamsi expressis verbis non moneatur. Numerus primus 2 autem excludendus, siue numeri primi *impares* tantum considerandi.

96. *Numero primo p pro modulo accepto, numerorum* 1, 2, 3.... $p-1$ *semissis erunt residua quadratica, reliqui non-residua, i. e. dabuntur* $\frac{1}{2}(p-1)$ *residua, totidemque non-residua.*

Facile enim probatur, omnia quadrata 1, 4, 9... $\frac{1}{2}(p-1)^2$ esse incongrua. Scilicet si fieri posset $rr \equiv r'r'$ (mod. p) atque numeri r, r' inaequales et non maiores quam $\frac{1}{2}(p-1)$ posito $r > r'$ i. q. licet, fieret $(r-r')(r+r')$ positiuus et per p diuisibilis. At vter-

*) Proprie quidem hic casu secundo alio sensu vtimur, quam hucusque fecimus. Dicere scilicet oporteret, r esse residuum quadrati aa secundum modulum m quando $r \equiv aa$ (mod. m); at breuitatis gratia in hac sectione semper r *ipsius* m residuum quadraticum vocamus, neque hinc vlla ambiguitas metuenda. Expressionem enim, *residuum*, quando idem significat quod numerus congruus, abhinc non adhibebimus, nisi forte de residuus *minimis* sermo sit, vbi nullum dubium esse potest.

que factor $r - r'$, et $r + r'$ ipso p est minor, quare suppositio consistere nequit (art. 13). Habentur itaque $\frac{1}{2}(p-1)$ residua quadratica, inter hos numeros $1, 2, 3 \ldots p-1$ contenta; plura vero inter ipsos esse nequeunt quia accedente residuo oprodeunt $\frac{1}{2}(p+1)$, quem numerum omnium residuorum multitudo superare nequit. Quare reliqui numeri erunt non residua horumque multitudo $= \frac{1}{2}(p-1)$.

Quum cifra semper sit residuum, hanc numerosque per modulum diuisibiles ab inuestigationibus his excludimus, quia hic casus per se est clarus, theorematumque concinnitatem tantum turbaret. Ex eadem caussa etiam modulum 2 exclusimus.

97. Quum plura quae in hac Sect. exponemus etiam ex principiis Sect. praec. deriuari possint, neque inutile sit, eandem veritatem per methodos diuersas perscrutari, hunc nexum ostendemus. Facile vero intelligitur, omnes numeros quadrato congruos, indices *pares* habere, eos contra, qui quadrato nullo modo congrui fieri possint, impares. Quia vero $p-1$ est numerus par, tot indices pares erunt quot impares, scilicet $\frac{1}{2}(p-1)$, totidemque tum residua tum non residua dabuntur.

Exempla.

Pro modulis sunt residua

3 . . . . . 1.
5 . . . . . 1, 4.

7 . . . . . 1, 2, 4.
11 . . . . . 1, 3, 4, 5, 9.
13 . . . . . 1, 3, 4, 9, 10, 12.
17 . . . . . 1, 2, 4, 8, 9, 13, 15, 16.
etc.

reliqui vero numeri, his modulis minores non residua.

98. Theorema. *Productum e duobus residuis quadraticis numeri primi p, est residuum; productum e residuo in non residuum, est non residuum; denique productum e duobus non-residuis, residuum.*

Demonstr. I. Sint A, B residua e quadratis aa, bb oriunda siue $A \equiv aa$, $B \equiv bb$, eritque productum AB quadrato numeri ab congruum i. e. residuum.

II. Quando A est residuum, puta $\equiv aa$, B vero non residuum, AB erit non-residuum. Ponatur enim si fieri potest $AB \equiv kk$, sitque valor expressionis $\frac{k}{a}$ (mod. p) $\equiv b$; erit itaque $aaB \equiv aabb$, vnde $B \equiv bb$, i. e. B residuum contra hyp.

Aliter. Multiplicentur omnes numeri qui inter hos 1, 2, 3. . . . $p - 1$ sunt residua (quorum multiudo $= \frac{1}{2}(p - 1)$, per A omniaque producta erunt residua quadratica, et quidem erunt omnia incongrua. Iam si non-residuum B per A multiplicatur, productum nulli productorum quae iam habentur congruum erit; quare si residuum esset, haberentur $\frac{1}{2}(p + 1)$ residua incongrua inter quae nondum est residuum 0, contra art. 96.

III. Sint A, B, non-residua. Multiplicentur omnes numeri qui inter hos 1, 2, 3.... $p-1$ sunt residua per A, habebunturque $\frac{1}{2}(p-1)$ non-residua inter se incongrua (II); iam productum AB nulli illorum congruum esse potest; quodsi igitur esset non-residuum, haberentur $\frac{1}{2}(p+1)$ non-residua inter se incongrua, contra art. 95. Quare productum etc. *Q. E. D.*

Facilius adhuc haec theoremata e principiis sect. praec. deriuantur. Quia enim residuorum indices semper sunt pares, non-residuorum vero impares, index producti e duobus residuis vel non-residuis erit par, adeoque productum ipsum, residuum. Contra index producti e residuo in non-residuum erit impar adeoque productum ipsum non-residuum.

Vtraque demonstrandi methodus etiam pro his theorematibus adhiberi potest: *Expressionis* $\frac{a}{b}$ *(mod. p) valor erit residuum, quando numeri a, b simul sunt residua, vel simul non residua; contra autem erit non-residuum, quando numerorum a, b alter est residuum alter non-residuum.* Possunt etiam ex conuersione theorr. art. praec. obtineri.

99. Generaliter, productum ex quotcunque factoribus est residuum tum quando omnes sunt residua, tum quando non residuorum, quae inter eos occurrunt, multitudo est par; quando vero multitudo non residuorum quae inter factores reperiuntur est impar, productum erit non-residuum. Facile itaque diiudicari potest,

vtrum numerus compositus sit residuum, necne, si modo quid sint singuli ipsius factores constet. Quamobrem in tabula II numeros primos tautummodo recepimus. Oeconomia huius tabulae haec est. In margine positi sunt moduli,*) in facie vero numeri primi successiui; quando ex his aliquis fuit residuum moduli alicuius, in spatio vtrique respondente lineola collocata est, quando vero numerus primus fuit non residuum moduli, spatium respondens vacuum mansit.

100. Antequam ad difficiliora progrediamur, quaedam de modulis non primis adiicienda sunt.

Si numeri primi p, potestas aliqua p^n pro modulo assumitur (vbi p non esse 2 supponimus), omnium numerorum per p non diuisibilium moduloque minorum altera semissis erunt residua, altera non residua, i. e. vtrorumque multitudo $= \frac{1}{2}(p-1)p^{n-1}$.

Si enim r est residuum: quadrato alicui congruus erit, cuius radix moduli dimidium non superat, vid. art. 94. Iam facile perspicitur, dari $\frac{1}{2}(p-1)p^{n-1}$ numeros per p non diuisibiles modulique semisse minoribus; superest itaque vt demonstretur, omnium horum numerorum quadrata incongrua esse, siue residua quadratica diuersa suppeditare. Quodsi duorum numerorum a, b per p non diuisibilium

*) Quomodo etiam modulis compositis carere possimus mox docebimus,

modulique semisse minorum quadrata essent congrua, foret $aa - bb$ siue $(a - b)(a + b)$ per p^n diuisibilis (posito i. q. licet $a > b$) Hoc vero fieri non potest, nisi *vel* alter numerorum $a - b$, $a + b$ per p^n fuerit diuisibilis, quod fieri nequit, quoniam vterque $< p^n$, *vel* alter per p^m alter vero per $p^{n-\mu}$, i. e. vterque per p. Sed etiam hoc fieri nequit. Manifesto enim etiam summa et differentia $2a$ et $2b$ per p foret diuisibilis adeoque etiam a et b contra hyp. — Hinc tandem colligitur inter numeros per p non diuisibiles moduloque minores $\frac{1}{2}(p - 1)p^n$ residua dari, reliquos quorum multitudo aeque magna, esse non-residua *Q. E. D.* — Potest etiam theorema hoc ex consideratione indicum deriuari simili modo vt art. 97.

101. *Quiuis numerus per p non diuisibilis, qui ipsius p est residuum, erit residuum etiam ipsius p^n; qui vero ipsius p est non-residuum, etiam ipsius p^n non-residuum erit.*

Pars posterior huius propositionis per se est manifesta. Si itaque prior falsa esset, inter numeros ipso p^n minores simulque per p non diuisibiles plures forent residua ipsius p, quam ipsius p^n, *i. e.* plures quam $\frac{1}{2}p^{n-1}(p - 1)$. Nullo vero negotio perspici poterit, multitudinem residuorum numeri p inter illos numeros esse praecise $= p^{n-1}(p - 1)$.

Aeque facile est, quadratum reipsa inuenire, quod secundum modulum p^n residuo dato sit congruum, si quadratum huic residuo secundum modulum p congruum habetur.

Scilicet si quadratum habetur, aa, quod residuo dato A secundum modulum p^μ est congruum, deducitur inde quadratum ipsi A secundum modulum p^ν congruum (vbi $\nu > \mu$ et $=$ vel $< 2\mu$ supponitur) sequenti modo. Ponatur radix quadrati quaesiti $= \pm a + xp^\mu$, quam formam eam habere debere facile perspicitur; debetque esse $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A \pmod{p^\nu}$ siue propter $2\mu > \nu$, $A - aa \equiv \pm 2axp^\mu \pmod{p^\nu}$ Sit $A - aa = p^\mu d$, eritque, x valor expressionis $\pm \frac{d}{2a} \pmod{p^{\nu-\mu}}$ quae huic $\pm \frac{A - aa}{2ap^\mu} \pmod{p^\nu}$ aequiualet.

Dato igitur quadrato ipsi A secundum p congruo, deducitur inde quadratum ispi A secundum modulum p^2 congruum; hinc ad modulum p^4, hinc ad p^8 etc. ascendi poterit.

Ex. Proposito residuo 6, quod secundum modulum 5 quadrato 1 congruum, inuenitur quadratum 9^2 cui secundum 25 est congruum, 16^2 cui secundum 125 congruum etc.

102. Quod vero attinet ad numeros per p diuisibiles, patet, eorum quadrata per pp fore diuisibilia, adeoque omnes numeros per p quidem diuisibiles, neque vero per pp, ipsius p^n fore non residua. Generaliter vero, si proponitur numerus p^kA vbi A per p non est diuisibilis, hi casus erunt distinguendi:

1) Quando $k =$ vel $> n$, erit $p^kA \equiv o \pmod{p^n}$, i. e. residuum.

2) Quando $k < n$ atque impar, erit p^kA non residuum.

Si enim esset $p^k A \equiv p^{2\varkappa+1} A \equiv ss \pmod{p^n}$, ss per $p^{2\varkappa+1}$ diuisibilis esset, id quod aliter fieri nequit, quam si fuerit s per $p^{2\varkappa+1}$ diuisibilis. Tunc vero ss etiam per $p^{2\varkappa+2}$ diuisibilis, adeoque etiam (quia $2^\varkappa + 2$ certo non maior quam n) $p^k A$, i. e. $p^{2\varkappa+1} A$; siue A per p, contra hyp.

3) Quando $k < n$ atque par. Tum $p^k A$ erit residuum vel non-residuum ipsius p^n, prout A est residuum vel non-residuum ipsius p. Quando enim A est residuum ipsius p, erit etiam residuum ipsius p^{n-k}. Posito autem $A \equiv aa \pmod{p^{n-k}}$ erit $Ap^k \equiv aap^k \pmod{p^n}$ aap^k vero est quadratum. Quando autem A est non-residuum ipsius p, $p^k A$ residuum ipsius p^n esse nequit. Ponatur enim $p^k A \equiv aa \pmod{p^n}$, eritque necessario aa per p^k diuisibilis. Quotiens erit quadratum cui A secundum modulum p^{n-k} adeoque etiam secundum modulum p congruus, i. e. A erit residuum ipsius p contra hyp.

103. Quoniam casum $p = 2$ exclusimus, de hoc adhuc quaedam dicenda. Quando numerus 2 est modulus, numerus quicunque erit residuum, non-residua nulla erunt. Quando vero 4 est modulus, omnes numeri impares formae $4k+1$ erunt residua, omnes vero formae $4k+3$ non-residua. Tandem quando 8 aut altior potestas numeri 2 est modulus, omnes numeri impares formae $8k+1$ erunt residua, reliqui vero, seu ii qui sunt formarum $8k+3$, $8k+5$, $8k+7$, erunt non-residua. Pars posterior huius propositionis inde clara, quod quadratum cuiusuis numeri imparis, siue sit formae $4k+1$, siue formae $4k-1$, fit formae $8k+1$. Priorem ita probamus.

1) Si duorum numerorum vel summa vel differentia per 2^{n-1} est diuisibilis, numerorum quadrata erunt congrua secundum modulum 2^n. Si enim alter ponitur $= a$, erit alter formae $2^{n-1}h \pm a$, cuius quadratum inuenitur $\equiv aa \pmod{2^n}$.

2) Quiuis numerus impar, qui ipsius 2^n est residuum quadraticum, congruus erit quadrato alicui, cuius radix est numerus impar et $< 2^{n-2}$ Sit enim quadratum quodcunque cui numerus ille congruus, aa atque numerus $a \equiv \pm \alpha \pmod{2^{n-1}}$ ita vt α moduli semissem non superet (art. 4), eritque $aa \equiv \alpha\alpha$. Quare etiam numerus propositus erit $\equiv \alpha\alpha$. Manifesto vero tum a tum α erunt impares atque $\alpha < 2^{n-2}$.

3) Omnium numerorum imparium ipso 2^{n-2} minorum quadrata secundum modulum 2^n incongrua erunt, Sint enim duo tales numeri r et s, quorum quadrata si secundum 2^n essent congrua, foret $(r-s)(r+s)$ per 2^n diuisibilis (posito $r > s$). Facile vero perspicitur numeros $r-s$, $r+s$, simul per 4 diuisibiles esse non posse, quare si alter tantummodo per 2 est diuisibilis, alter vt productum per 2^n diuisibilis fieret, per 2^{n-1} diuisibilis esse deberet, *Q. E. A.* quoniam vterque $< 2^{n-1}$.

4) Quodsi denique haec quadrata ad *residua* sua *minima positiua* reducuntur, habebuntur 2^{n-3} residua quadratica diuersa modulo minora, quorum quoduis erit formae $8k+1$.

Sed quum praecise 2^{n-3} numeri formae $8k + 1$ modulo minores exstent, necessario hi omnes inter illa residua reperientur. *Q. E. D.*

Vt quadratum numero dato formae $8k + 1$ secundum modulum 2^n congruum inueniatur, methodus similis adhiberi potest, vt in art. 102; vid. etiam art. 88. — Denique de numeris paribus eadem valent, quae art. 102 generaliter exposuimus.

104. Circa multitudinem valorum diuersorum (i. e. secundum modulum incongruorum), quos expressio talis $V = \sqrt{A}(\text{mod. } p^n)$ admittit, siquidem A est residuum ipsius p^n, facile e praecc. colliguntur haec. (Numerum p supponimus esse primum, vt ante, et breuitatis caussa casum $n = 1$ statim includimus). I. Si A per p non est diuisibilis, V *vnum* valorem habet pro $p = 2$, $n = 1$, puta $V \equiv 1$; *duos*, quando p est impar, nec non pro $p = 2$, $n = 2$, puta ponendo vnum $\equiv v$, alter erit $\equiv -v$; *quatuor* pro $p = 2$, $n > 2$, scilicet ponendo vnum $\equiv v$, reliqui erunt $\equiv -v$, $2^{n-2} + v$, $2^{n-2} - v$. II. Si A per p diuisibilis est, neque vero per p^n, sit potestas altissima ipsius p ipsum A metiens $p^{2\mu}$ (manifesto enim ipsius exponens par esse debebit) atque $A = ap^{2\mu}$. Tunc patet, omnes valores ipsius V per p^μ diuisibiles esse, et quotientes e diuisione ortos fieri valores expr. $V' = \sqrt{a}(\text{mod. } p^{n-2\mu})$; hinc omnes valores diuersi ipsius V prodibunt, multiplicando omnes valores expr. V' inter 0 et $p^{n-\mu}$ sitos per p^μ; quare illi exhibebuntur per vp^μ, $vp^\mu + p^{n-\mu}$, $vp^\mu + 2p^{n-\mu} \ldots vp^\mu + (p^\mu - 1)p^{n-\mu}$,

si v indefinite omnes valores *diuersos* expr. V exprimit, ita vt illorum multitudo fiat p^μ, $2p^\mu$ vel $4p^\mu$, prout multitudo horum (per casum I) est 1, 2 vel 4. III. Si A per p^n diuisibilis est, facile perspicietur, statuendo $n = 2m$ vel $= 2m - 1$, prout par est vel impar, omnes numeros per p^m diuisibiles, neque vllos alios, esse valores ipsius V; quare omnes valores diuersi hi erunt $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, quorum multitudo p^{n-m}.

105. Superest casus, vbi modulus m e pluribus numeris primis compositus est. Sit $m = abc\ldots$, designantibus a, b, c etc. numeros primos diuersos aut primorum diuersorum potestates, patetque statim, si n sit residuum ipsius m, fore etiam n residuum singulorum a, b, c etc., adeoque n certo nonresiduum ipsius m esse, si fuerit NR. vllius e numeris a, b, c etc. Vice versa autem, si n singulorum a, b, c etc. residuum est, etiam residuum producti m erit. Supponendo enim, $n \equiv A^2, B^2, C^2$ etc. sec. mod. a, b, c etc. resp., patet, si numerus N ipsis A, B, C etc. sec. mod. a, b, c etc. resp. congruus eruatur (art. 32), fore $n \equiv NN$ secundum omnes hos modulos adeoque etiam secundum productum m. — Quum facile perspiciatur, hoc modo e combinatione *cuiusuis* valoris ipsius A siue expr. $\sqrt{n}(\text{mod. } a)$ cum *quouis* valore ipsius B cum *quouis* valore ipsius C etc. oriri valorem ipsius N siue expr. $\sqrt{n}(\text{mod. } m)$, nec non e combinationibus diuersis produci diuersos N, et e cunctis cunctos: multitudo omnium valorum diuersorum ipsius N aequalis

erit producto e multitudinibus valorum ipsorum A, B, C etc. quas determinare in art. praec. docuimus. — Porro manifestum est, si vnus valor expressionis $\sqrt{n}$ (mod. m) siue ipsius N fuerit notus, hunc simul fore valorem omnium A, B, C etc.; et quum hinc per art. praec. omnes reliqui valores harum quantitatum deduci possint, facile sequitur, ex vno valore ipsius N omnes reliquos obtineri posse.

Ex. Sit modulus 315 cuius residuum an non-residuum sit 46, quaeritur. Diuisores primi numeri 315 sunt 3, 5, 7, atque numerus 46 residuum cuiusuis eorum quare etiam ipsius 315 erit residuum. Porro, quia $46 \equiv 1$, et $\equiv 64$ (mod. 9); $\equiv 1$ et $\equiv 16$ (mod. 5); $\equiv 4$ et $\equiv 25$ (mod. 7), inueniuntur radices quadratorum, quibus 46 secundum modulum 315 congruus, 19, 26, 44, 89, 226, 271, 289, 296.

106. Ex praecedentibus colligitur, si tantummodo semper dignosci possit vtrum *numerus primus* datus numeri *primi dati* residuum sit an non-residuum, omnes reliquos casus ad hunc reduci posse. Pro illo itaque casu criteria certa omni studio nobis erunt indaganda. Antequam em hanc perquisitionem aggrediamur, criterium quoddam exhibemus ex Sect. petitum quod quamuis in praxi nullum fere vsum habeat tamen propter simplicitatem atque generalitatem memoratu dignum est.

Numerus quicunque A per numerum primum $2m + 1$ non diuisibilis, huius primi residuum est vel non-residuum, prout $A^m \equiv +1$ vel $\equiv -1$ (mod. $2m + 1$).

Sit enim pro modulo $2m + 1$ in systemate quocunque numeri A index, a, eritque a par, quando A est residuum ipsius $2m + 1$, impar vero quando A non-residuum. At numeri A^m index erit ma, i. e. $\equiv 0$ vel $\equiv m$ (mod. $2m$), prout a par vel impar. Hinc denique A^n in priori casu erit $\equiv +1$, in posteriori vero $\equiv -1$ (mod. $2m + 1$). V. artt. 57, 62.

Ex. 3 ipsius 13 est residuum quia $3^6 \equiv 1$ (mod. 13), 2 vero ipsius 13 non-residuum, quoniam $2^6 \equiv -1$ (mod. 13).

At quoties numeri examinandi mediocriter sunt magni, hoc criterium ob calculi immensitatem prorsus inuitile erit.

107. Facillimum quidem est, proposito modulo, omnes assignare numeros, qui ipsius residua sunt vel non residua. Scilicet si ille numerus ponitur $= m$, determinari debent quadrata, quorum radices semissem ipsius m non superant, siue etiam numeri his quadratis secundum m congrui (ad praxin methodi adhuc expeditiores dantur), tuncque omnes numeri horum alicui secundum m congrui, erunt residua ipsius m, omnes autem numeri nulli istorum congrui erunt non-residua. — At quaestio inuersa, *proposito numero aliquo, assignare omnes numeros quorum ille sit residuum vel non-residuum*, multo altioris est indaginis. Hoc itaque problema, a cuius solutione illud quod in art. praec. nobis proposuimus pendet, in sequentibus perscrutabimur, a casibus simplicissimis inchoantes.

108. THEOREMA. *Omnium numerorum formae* $4n + 1$, -1 *est residuum quadraticum, omnium vero numerorum primorum formae* $4n + 3$, *non-residuum.*

Ex. — 1 est residuum numerorum 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc., e quadratis numerorum 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22 etc. respetiue oriundum; contra non-residuum est numerorum 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 etc.

Mentionem huius theor. iam in art. 64 fecimus. Demonstratio vero facile ex art. 106 petitur. Etenim pro numero primo formae $4n + 1$ est $(-1)^{2n} \equiv 1$, pro numero autem formae $4n + 3$ habetur $(-1)^{2n+1} \equiv -1$. Conuenit haec demonstratio cum ea quam *l. c.* tradidimus. Sed propter theorematis elegantiam atque vtilitatem non superfluum erit, alio adhuc modo idem ostendisse.

109. Designemus complexum omnium residuorum numeri primi p, quae ipso p sunt minora, excluso residuo o, per literam C, et quoniam horum residuorum multitudo semper $= \frac{p-1}{2}$, manifestum est, eam fore parem, quoties p sit formae $4n + 1$, imparem vero, quoties p sit formae $4n + 3$. Dicantur, ad instar art. 77, vbi de numeris in genere agebatur, *residua socia* talia, quorum productum $\equiv 1 \pmod{p}$; manifesto enim si r est residuum, etiam $\frac{1}{r} \pmod{p}$ residuum erit. Et quoniam idem residuum plura socia inter residua C habere nequit, patet omnia residua C in classes distribui posse,

quarum quaeuis bina residua socia contineat. Iam perspicuum est, si nullum residuum daretur, quod sibi ipsi esset socium, i. e. si quaeuis classis bina residuae *inaequalia* contineret, omnium residuorum numerum fore duplum numeri omnium classium; quodsi vero aliqua dantur residua sibi ipsis socia, i. e. aliquae classes quae vnicum tantum residuum aut, si quis malit, idem residuum bis continent, posita harum classium multitudine $= a$, reliquarumque multitudine $= b$; erit omnium residuorum C numerus $= a + 2b$. Quare quando p est formae $4n + 1$, erit a numeros par; quando autem p est formae $4n + 3$, erit a impar. At numeri ipso p minores alii, quam 1 et $p - 1$, sibi ipsis socii esse nequeunt (vid. art. 77); priorque 1 certo inter residua occurrit; vnde in priori casu $p - 1$ (seu quod hic idem valet, -1) debet esse residuum, in posteriori vero non-residuum; alias enim in illo casu foret $a = 1$, in hoc autem $= 2$, quod fieri nequit.

110. Etiam haec demonstratio ill. Eulero debetur, qui et priorem primus inuenit. V. *Opusc. Anal.* T. I. *p* 135. — Facile quisquis videbit eam similibus principiis innixam esse, vt demonstratio nostra secunda theor. Wilsoniani art. 77. Si vero hoc theorema supponere velimus, facilius adhuc demonstratio exhiberi poterit. Scilicet inter numeros 1, 2, 3... $p - 1$ erunt $\frac{p-1}{2}$ residua quadratica ipsius p totidemque non-residua; quare non-residuorum multitudo erit par, quando p est formae $4n + 3$. Hinc productum ex omnibus numeris

1, 2, 3 . . . $p - 1$ in priori casu erit residuum, in posteriori non-residuum (art. 99). At productum hoc semper $\equiv -1 \pmod{p}$; adeoque etiam -1 in priori casu residuum, in posteriori non-residunm erit.

111. Si itaque r est residuum numeri alicuius primi formae $4n + 1$, etiam $-r$ huius primi residuum erit, omnia autem talis numeri non-residua, etiam signo contrario sumta non-residua manebunt. Contrarium euenit pro numeris primis formae $4n + 3$, quorum residua quando signum mutatur, non-residua fiunt et vice versa, vid. art. 98.

Ceterum facile ex praecadentibus deriuatur regula generalis: -1 residuum omnium numerorum qui neque per 4 neque per ullum numerum primum formae $4n + 3$, diuidi possunt; omnium reliquorum non-residuum. V. artt. 103 et 105.

112. Progredimur ad residua $+2$ et -2.

Si ex tabula II colligimus omnes numeros primos quorum residuum est $+2$, hos habebimus: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Facile autem animaduertitur, inter hos numeros nullos inueniri formarum $8n + 3$ et $8n + 5$.

Videamus itaque, num haec inductio ad certitudinem euehi possit.

Primum obseruamus quemuis numerum compositum formae $8n + 3$ vel $8n + 5$ neces-

*) Quando igitur de numero quocunque loquemur quatenus numeri formae $4n + 1$ residuum vel non-residuum est, ipsius signum omnino negligere siue etiam signum anceps $\pm$ ipsi tribuere poterimus.

sario factorem primum alterutrius formae $8n + 3$ vel $8n + 5$, inuoluere; manifesto enim e solis numeris primis formarum $8n + 1$, $8n + 7$, alii numeri quam qui sunt formae $8n + 1$ vel $8n + 7$, componi nequeunt. Quodsi itaque inducto nostra generaliter est vera, nullus omnino numerus formae $8n + 3$, $8n + 5$ dabitur, cuius residuum $+ 2$; sicque nullus certe numerus huius formae infra 100 exstat, cuius residuum sit -2. Si autem vltra hunc limitem tales numeri repirirentur, ponamus minimum omnium $= t$. Erit itaque t vel formae $8n + 3$ vel $8n + 5$; $+ 2$ ipsius residuum erit, omnium autem numerorum similium minorum non-residuum. Ponatur $2 \equiv aa \pmod{t}$ poteritque a ita semper accipi vt sit impar simulque $< t$, (habebit enim a ad minimum duos valores positiuos ipso t minores quorum summa $= t$, quorumque adeo alter par alter impar v. art. 104. 105). Quo facto sit $aa = 2 + tu$, siue $tu = aa - 2$, eritque aa formae $8n + 1$, tu igitur formae $8n - 1$, adeoque u formae $8n + 3$ vel $8n + 5$, prout t est formae posterioris vel prioris. At ex aequatione $aa = 2 + tu$ sequitur, etiam $2 \equiv a \pmod{u}$ *i. e.* 2 etiam ipsius u residuum fore. Facile vero perspicitur, esse $u < t$; quare t non est minimus numerus inductioni nostrae contrarius contra hyp. Vnde manifesto sequitur id quod per inductionem inueneramus generaliter verum esse.

Combinando haec cum prop. art. 111. sequentia theoremata nanciscimur.

I. *Numerorum omnium primorum formae* $8n+3$, $+2$ *erit non residuum,* -2 *vero residuum.*

II. *Numerorum omnium primorum formae* $8n+5$, *tum* $+2$ *tum* -2 *erunt non residua.*

113, Per similem inductionem ex tab. II inueniuntur numeri primi quorum residuum est -2 hi: 3, 11, 17, 19, 41, 59, 67, 73, 83, 89, 97 *). Inter quos quum nulli inueniantur formarum $8n+5$, $8n+7$, num etiam haec inductio theorematis generalis vim adipisci possit inuestigemus. Ostenditur simili modo vt in art. praec. quemuis numerum compositum formae $8n+5$ vel $8n+7$, factorem primum inuoluere formae $8n+5$ vel formae $8n+7$, ita vt, si inductio nostra generaliter vera, -2 nullius omnino numeri formae $8n+5$ vel $8n+7$ residuum esse possit. Si autem tales numeri darentur, ponatur omnium minimus $= t$, fiatque $-2 = aa - tu$. Vbi si vti supra a impar ipsoque t minor accipitur, u erit formae $8n+5$ vel $8n+7$, prout t formae $8n+7$ vel $8n+5$. At ex eo quod $aa+2 = tu$ atque $a < t$; quisquis facile deriuari poterit, etiam u ipso t minorem fore. Denique -2 etiam ipsius u residuum erit; i. e. t non erit minimus numerus qui inductioni nostrae aduersatur, contra hyp. Quare necessario -2 omnium numerorum formarum $8n+5$, $8n+7$ non residuum.

*) Considerando scilicet -2 tamquam productum ex $+2$ et -1 V. art. III.

Combinando haec cum propp. art. 111, prodeunt theoremata haec:

I. *Omnium numerorum primorum formae* $8n + 5$, *tum* -2, *tum* $+2$ *sunt non-residua*, vti iam in art. praec. inuenimus.

II. *Omnium numerorum primorumm formae* $8n + 7$, -2 *est non-residuum*, $+2$ *vero residuum.*

Ceterum in vtraque demonstratione pro a etiam valorem parem accipere potuissemus; tunc autem casum vbi a fuisset formae $4n + 2$, ab eo distinguere oportuisset, vbi a formae $4n$. Euolutio autem perinde procedit vti supra, nullique difficultati est obnoxia.

114. Vnus adhuc superest casus, scilicet vbi numerus primus est formae $8n + 1$. Hic vero methodum praecedentem eludit, artificiaque prorsus peculiaria postulat.

Sit pro modulo primo $8n + 1$, radix quaecunque primitiua, a, eritque (art. 62) $a^{4n} \equiv -1 \pmod{8n+1}$, quae congruentia ita etiam exhiberi potest, $(a^{2n} + 1)^2 \equiv 2a^{2n} \pmod{8n+1}$, siue etiam ita, $(a^{2n} - 1)^2 \equiv -2a^{2n}$. Vnde sequitur tum $2a^{2n}$, tum $-2a^{2n}$ ipsius $8n + 1$ esse residuum: at quia a^{2n} est quadratum per modulum non diuisibile, manifesto etiam tum $+2$ tum -2 residua erunt (art. 98.)

115. Haud inutile erit, adhuc aliam huius theorematis demonstrationem adiicere, quae similem relationem ad praecedentem habet, vt theorematis art. 108 demonstratio secunda

(art. 109) ad primam (art. 108). Periti facilius tunc perspicient, binas demonstrationes tam illas quam has non adeo heterogeneas esse, quam primo forsan aspectu videantur.

I. Pro modulo quocunque primo formae $4m + 1$, inter numeros ipso minores $1, 2, 3 \ldots 4m$, reperientur m qui biquadrato congrui esse possunt, reliqui vero $3m$ non poterunt.

Facile quidem hoc ex principiis sect. praec. deriuatur, sed etiam absque his demonstratio haud difficilis. Demonstrauimus enim pro tali modulo -1 semper esse residuum quadraticum. Sit itaque $ff \equiv -1$ patetque, si z fuerit numerus quicunque per modulum non diuisibilis, quaternorum numerorum $+z$, $-z$, $+fz$, $-fz$ (quos incongruos esse facile perspicitur) biquadrata inter se congrua fore; porro manifestum est biquadratum numeri cuiuscunque, qui nulli ex his quatuor congruus, illorum biquadratis congruum fieri non posse, (alias enim congruentia $x^4 \equiv z^4$ quae est quarti gradus plures quam 4 radices haberet, contra art. 43). Hinc facile colligitur, omnes numeros $1, 2, 3, \ldots 4m$, tantummodo m biquadrata incongrua praebere, quibus inter eosdem numeros m congrui reperientur, reliqui autem nulli biquadrato congrui esse poterunt.

II. Secundum modulum primum formae $8n + 1$, -1 biquadrato congruus fieri poterit (-1 erit *residuum biquadraticum* huius numeri primi).

Omnium enim residuorum biquadraticorum ipso $8n + 1$ minorum (cifra exclusa) multitudo erit $= 2n$ i. e. par. Porro facile probatur, si r fuerit residuum biquadraticum ipsius $8n + 1$, etiam valorem expr. $\frac{1}{r}$ (mod. $8n + 1$) fore tale residuum. Hinc omnia residua biquadratica in classes simili modo distribui poterunt, vti in art. 109 residua quadratica distribimus: nec non reliqua demonstrationis pars prorsus eodem modo procedit vt illic.

III. Iam sit $g^4 \equiv -1$, et h valor expr. $\frac{1}{g}$ (mod. $8n + 1$). Tunc erit $(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$ (propter $gh \equiv 1$). At $g^4 \equiv -1$, adeoque $-h^2 \equiv g^4 h^2 \equiv g^2$, vnde tandem $g^2 + h^2 \equiv 0$, atque $(g \pm h)^2 \equiv \pm 2$ *i. e.* tum $+2$, tum -2 residuum quadraticum ipsius $8n + 1$. *Q. E. D.*

116. Ceterum ex praec. facile regula sequens generalis deducitur: $+2$ *est residuum numeri cuiusuis, qui neque per* 4, *neque per vllum primum formae* $8n + 3$ *vel* $8n + 5$ *diuidi potest, reliquorum autem* (ex. gr. omnium numerorum formarum $8n + 3$, $8n + 5$, siue sint primi, siue compositi) *non-residuum.*

-2 *est residuum numeri cuiusuis, qui neque per* 4, *neque per vllum primum formae* $8n + 5$ *vel* $8n + 7$ *diuidi potest, omnium autem reliquorum non-residuum.*

Theoremata haec elegantia iam sagaci Fermatio innotuerunt, *Op. Mathem.* p. 168.

Demonstrationem vero quam se habere professus est, nusquam communicauit. Postea ab ill. Euler frustra semper est inuestigata: at ill. La Grange primus demonstrationem rigorosam reperit, *Nouv. Mem. de l'Ac. de Berlin* 1775. p. 349, 351. Quod ill. Eulerum adhuc latuisse videtur, quando scripsit diss. in *Opusc. Analyt.* conseruatam, T. I. p. 259.

117. Pergimus ad residua + 3 et — 3. A posteriori initium faciamus.

Reperiuntur ex tab. II. numeri primi quorum residuum est — 3, hi: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, inter quos nullus inuenitur formae $6n + 5$. Quod vero etiam vltra tabulae limites nulli primi huius formae dantur quorum residuum — 3, ita demonstramus: Primo patet quemuis numerum compositum formae $6n + 5$ necessario factorem primum aliquem eiusdem formae inuoluere. Quousque igitur nulli numeri primi formae $6n + 5$ dantur, quorum residuum — 3, eousque tales etiam compositi non dabuntur. Quodsi vero vltra tabulae nostrae limites tales numeri darentur, sit omnium minimus $= t$, ponaturque $-3 = aa - tu$. Tunc erit, si acceperis a parem ipsoque t minorem, $u < t$, atque — 3 residuum ipsius u. Sed quando a formae $6n \pm 2$, tu erit formae $6n + 1$, adeoque u formae $6u + 5$, *Q. E. A.* quia t minimum esse numerum inductioni nostrae aduersantem supposuimus. Quando vero a formae $6n$, erit tu formae $36n + 3$ adeoque $\frac{1}{3}tu$ formae $12n + 1$,

quare $\frac{1}{3}u$ erit formae $6n + 5$; patet autem -3 etiam ipsius $\frac{1}{3}u$ residuum fore, atque esse $\frac{1}{3}u < t$, *Q. E. A.* Manifestum itaque, -3 nullius numeri formae $6n + 5$ residuum esse posse.

Quoniam quisque numerus formae $6n + 5$ necessario vel sub forma $12n + 5$, vel sub hac $12n + 11$ continetur, prior autem forma sub hac $4n + 1$, posterior sub hac $4n + 3$, haec habentur theoremata:

I. *Cuiusuis numeri primi formae* $12n + 5$, *tum* -3 *tum* $+3$ *non-residuum est.*

II. *Cuiusuis numeri primi formae* $12n + 11$, -3 *est non-residuum,* $+3$ *vero residuum.*

118. Numeri quorum residuum est $+3$ ex tabula II. inueniuntur hi: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, inter quos nulli sunt formae $12n + 5$, vel $12n + 7$. Nullos autem omnino numeros formarum $12n + 5$, $12n + 7$ dari quorum $+3$ sit residuum, eodem prorsus modo, vt in artt. 112, 113, 117, comprobari potest, quare hoc negotio supersedemus. Habemus itaque collato art. 111 theoremata:

I. *Numeri cuiusuis primi formae* $12n + 5$, *non-residua sunt tum* $+3$ *tum* -3, (vti iam in art. praec. inuenimus).

II. *Numeri cuiusuis primi formae* $12n + 7$ *non-residuum est* $+3$, -3 *vero residuum.*

119. Nihil autem per hanc methodum pro numeris formae $12n + 1$ inueniri potest, qui proin artificia singularia requirunt. Ex inductione quidem facile colligitur, omnium numerorum primorum huius formae residua esse $+3$ et -3. Manifesto autem demonstrari tantummodo debet, numerorum talium residuum esse -3, quia tunc necessario etiam $+3$ residuum esse debet (art. 111). Ostendemus autem generalius, -3 esse residuum numeri cuiusuis primi formae $3n + 1$.

Sit p huiusmodi primus atque a numerus pro modulo p ad exponentem 3 pertinens (quales dari ex art. 55 manifestum, quia 3 submultiplum ipsius $p - 1$). Erit itaque $a^3 \equiv 1 \pmod{p}$ i. e. $a^3 - 1$ siue $(a^2 + a + 1)(a - 1)$ per p diuisibilis. Sed patet a esse non posse $\equiv 1 \pmod{p}$, quia 1 ad exponentem 1 pertinet, quare $a - 1$ per p diuisibilis non erit; sed $a^2 + a + 1$ erit, hincque etiam $4aa + 4a + 4$; i. e. erit $(2a + 1)^2 \equiv -3 \pmod{p}$ siue -3 residuum ipsius p. *Q. E. D.*

Ceterum patet, hanc demonstrationem (quae a praecedentibus est independens) etiam numeros primos formae $12n + 7$ complecti quos iam in art. praec. absoluimus.

Obseruare adhuc conuenit, hanc analysin ad instar methodi in artt. 109, 115 vsitatae exhiberi posse, at breuitatis gratia huic rei non immoramur.

120. Colliguntur facile ex praec. theoremata haec (vid. artt. 102, 103, 105).

I. — 3 *est residuum omnium numerorum, qui neque per* 8, *neque per* 9, *neque per vllum numerum primum formae* $6n + 5$ *diuidi possunt, non-residuum autem omnium reliquorum.*

II. + 3 *est residuum omnium numerorum, qui neque per* 4, *neque per* 9, *neque per vllum primum formae* $12n + 5$ *vel* $12n + 7$ *diuidi possunt, omnium reliquorum non-residuum.*

Teneatur imprimis casus particularis hic:

— 3 est *residuum* omnium numerorum primorum formae $3n + 1$, seu quod idem est *omnium, qui ipsius* 3 *sunt residua, non-residuum* vero omnium numerorum primorum formae $6n + 5$, seu, excluso numero 2, omnium formae $3n + 2$, i. e. *omnium qui ipsius* 3 *sunt non-residua.* Facile vero perspicitur omnes reliquos casus ex hoc sponte sequi.

Propositiones ad residua + 3 et — 3 pertinentia iam Fermatio notae fuerunt, *Opera Wallisii* T. II. p. 857. At ill. Euler primus demonstrationes tradidit, *Comm. nou. Petr.* T. VIII. p. 105 sqq. Eo magis est mirandum, demonstrationen propositionum ad residua + 2 et — 2 pertinentium, prorsus similibus artificiis innixas, semper ipsius sagacitatem fugisse. Vid. etiam comment. ill. La Grange, *Nouv. Mem. de l'Ac. de Berlin*, 1775 p. 352.

121. Per inductionem deprehenditur, + 5 nullius numeri imparis formae $5n + 2$, vel $5n + 3$ residuum esse, i. e. nullius numeri impa-

ris qui ipsius non-residuum sit. Hanc vero regulam nullam exceptionem pati, ita demonstratur. Sit numerus minimus, si quis datur, ab hac regula excipiendus $= t$, qui itaque numeri 5 est non-residuum, 5 autem ipsius t residuum. Sit $aa = 5 + tu$, ita vt a sit par ipsoque t minor. Erit igitur u impar ipsoque t minor, + 5 autem ipsius u residuum erit. Quodsi iam a per 5 non est diuisibilis, etiam u non erit; manifesto autem tu ipsius 5 est residuum, quare quum t ipsius 5 sit non-residuum, etiam u non-residuum erit; i. e. datur non-residuum numeri 5 cuius residuum est + 5, ipso t minus, contra hyp. Si vero a per 5 est diuisibilis, ponatur $a = 5b$, atque $u = 5v$, vnde $tv \equiv -1 \equiv 4 \pmod 5$, *i. e.* tv erit residuum numeri 5. In reliquis demonstratio perinde procedit vt in casu priori.

122. Omnium igitur numerorum primorum, qui simul sunt ipsius 5 non-residua simulque formae $4n + 1$, i. e. omnium numerorum primorum formae $20n + 13$ vel $20n + 17$, tum + 5 quam — 5 non residua erunt; omnium autem numerorum primorum formae $20n + 3$ vel $20n + 7$, non residuum erit + 5, — 5 residuum.

Potest vero prorsus simili modo demonstrari, — 5 esse non-residuum omnium numerorum primorum formarum $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$, facileque perspicitur hinc sequi, + 5 esse residuum omnium numerorum primorum formae $20n + 11$, vel $20n + 19$, non-

residuum autem omnium formae $20n + 13$, vel $20n + 17$. Et quoniam quiuis numerus primus, praeter 2 et 5 (quorum residuum ± 5), in aliqua harum formarum continetur $20n + 1$, 3, 7, 9, 11, 13, 17, 19, patet, de omnibus iam iudicium ferri posse, exceptis iis qui sint formae $20n + 1$, vel formae $20n + 9$.

123. Ex inductione facile deprehenditur, $+5$ et -5 esse residua omnium numerorum primorum formae $20n + 1$, vel $20 + 9$. Quodsi hoc generaliter verum est, lex elegans habebitur, $+5$ *esse residuuum omnium numerorum primorum qui ipsius* 5 *sint residua*, (hi enim in alterutra formarum $5n + 1$ vel $5n + 4$ siue in aliqua harum, $20n + 1$, 9, 11, 19, continentur, de quarum tertia et quarta illud iam ostensum est) *non-residuum vero omnium numerorum qui ipsius* 5 *sint non-residua*, vt iam supra demonstrauimus. Clarum autem est, hoc theorema sufficere, ad diiudicandum, vtrum $+5$ (eoque ipso, -5, si tamquam productum ex $+5$ et -1 consideretur) numeri cuiuscunque dati residuum sit an non-residuum. Denique obseruetur huius theorematis cum illo quod art. 120 de residuo -3 exposuimus analogia.

At verificatio illius inductionis non adeo facilis. Quando numerus primus formae $20n + 1$, siue generalius formae $5n + 1$ proponitur, res simili modo absolui potest, vt in artt. 114, 119. Sit scilicet numerus quicunque pro modulo $5n + 1$ ad exponentem 5 pertinens a, quales dari ex sect. praec. manifestum, erit-

que $a^5 \equiv 1$, siue $(a - 1)(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{5n + 1}$. At quia nequit esse $a \equiv 1$, neque adeo $a - 1 \equiv 0$; necessario erit $a^4 + a^3 + a^2 + a + 1 \equiv 0$. Quare etiam $4(a^4 + a^3 + a^2 + a + 1) = (2aa + a + 2)^2 - 5a^2$ erit $\equiv 0$ i. e. $5a^2$ erit residuum ipsius $5n + 1$, adeoque etiam 5, quia a^2 est residuum per $5n + 1$ non diuisibile (a enim per $5n + 1$ non diuisibilis propter $a^5 \equiv 1$). *Q. E. D.*

At casus, vbi numerus primus formae $5n + 4$ proponitur, subtiliora artificia postulat. Quoniam vero propositiones quarum ope negotium absoluitur in sequentibus generalius tractabuntur, hic breuiter tantum eas attingimus.

I. Si p est numerus primus atque b non-residuum quadraticum datum ipsius p, valor expressionis $(A)\ldots \dfrac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$ (ex qua euoluta irrationalitatem abire facile perspicitur), semper per p diuisibilis erit, quicunque numerus pro x assumatur. Patet enim ex inspectione coefficientium qui ex euolutione ipsius A obtinentur, omnes terminos a secundo vsque ad penultimum (incl.) per p diuisibiles fore, adeoque esse $A \equiv 2(p + 1)(x^p + xb^{\frac{p-1}{2}})$, (mod. p). At quoniam b ipsius p non-residuum est, erit $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, (art. 106); x^p autem semper est $\equiv x$ (sect. praec.) vnde fit $A \equiv 0$. *Q. E. D.*

II. In congruentia $A \equiv 0 \pmod{p}$, indeterminata x habet p dimensiones, omnesque

numeri 0, 1, 2.... $p - 1$ illius radices erunt. Iam ponatur e esse diuisorem ipsius $p + 1$, eritque expressio $\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$ (quam per B designamus) si euoluitur, ab irrationalitate libera, indeterminata x in ipsa $e - 1$ dimensiones habebit, constatque ex analyseos primis elementis, A per B (indefinite) esse diuisibilem. Iam dico $e - 1$ valores ipsius x dari, quibus in B substitutis, B per p diuisibilis euadat. Ponatur enim $A = BC$, habebitque x in C dimensiones $p - e + 1$, adeoque congruentia $C \equiv 0 \pmod{p}$ non plures quam $p - e + 1$ radices. Vnde facile patet, omnes reliquos numeros ex his 0, 1, 2, 3.... $p - 1$, quorum multitudo $= e - 1$, congruentiae $B \equiv 0$ radices fore.

III. Iam ponatur p esse formae $5u + 4$, $e = 5$, b non-residuum ipsius p, atque numerum a ita determinatum, vt sit $\frac{(a + \sqrt{b})^5 - (a - \sqrt{b})^5}{\sqrt{b}}$ per p diuisibilis. At illa expressio fit $= 10a^4 + 20aab + 2bb = 2((b + 5aa)^2 - 20a^4)$. Erit igitur etiam $(b + 5aa)^2 - 20a^4$ per p diuisibilis i. e, $20a^4$ residuum ipsius p; at quoniam $4a^4$ residuum est per p non diuisibile (facile enim intelligitur, a per p diuidi non posse), etiam 5 residuum ipsius p erit. *Q. E. D.*

Hinc patet theorema in initio huius articuli prolatum generaliter verum esse. —

Obseruamus adhuc, demonstrationes pro vtroque casu ill. La Grange deberi, *Mem. de l'Ac. de Berlin* 1775, p. 352 sqq.

124. Per similem methodum demonstratur,

— 7 *esse non-residuum cuiusuis numeri primi q ipsius* 7 *sit non-residuum.*

Ex inductione vero concludi potest,

— 7 *esse residuum cuiusuis numeri qui ipsius* 7 *sit residuum.*

At hoc a nemine hactenus rigorose demonstratum. Pro iis quidem residuis ipsius 7, qui sunt formae $4n - 1$, facilis est demonstratio; etenim per methodum ex praec. abunde notam ostendi potest, $+7$ semper esse talium numerorum primorum non-residuum, adeoque -7 residuum. Sed parum hinc lucramur: reliqui enim casus per hanc methodum tractari nequeunt. Vnum quidem adhuc casum simili mod. vt artt. 119, 123 absoluere possumus. Scilicet si p est numerus primus formae $7n + 1$, atque a pro modulo p ad exponentem 7 pertinens, facile perspicitur $\frac{4(a^7 - 1)}{a - 1} = (2a^3 + a^2 - a - 2)^2 + 7(a^2 - a)^2$ per p diuisibilem, adeoque $-7(a^2 - a)^2$ ipsius p residuum fore. At $(a^2 - a)^2$, tamquam quadratum, ipsius p residuum est, insuperque per p non diuisibile; quum enim a ad exponentem 7 pertinere supponatur, neque $\equiv 0$, neque $\equiv 1 \pmod{p}$ esse potest, i. e. neque a

neque $a - 1$ per p diuisibilis erit, adeoque etiam quadratum $(a-1)^2\, a^2$. Vnde manisto etiam 7 ipsius p residuum erit. *Q. E. D.* — At primi numeri formae $7n + 2$ vel $7n + 4$ omnes methodos hucusque traditas eludunt. Ceterum etiam haec demonstratio ab ill. La Grange primum est detecta *l. c.* — Infra *sect.* VII. docebimus generaliter, expressionem $\frac{4(x^p - 1)}{x - 1}$ semper ad formam $X^2 \mp p\, Y^2$ reduci posse, (vbi signum superius est accipiendum quando p est numerus primus formae $4n + 1$, inferius quando est formae $4n + 3$), denotantibus X, Y functiones rationales ipsius x, a fractionibus liberas. Hanc discerptionem ill. La Grange vltra casum $p = 7$ non perfecit v. *l. c.* p. 352.

125. Quoniam igitur methodi praecedentes ad demonstrationes generales stabiliendas non sufficiunt, iam tempus est, aliam ab hoc defectu liberam exponere. Initium facimus a theoremate, cuius demonstratio satis diu operam nostram elusit, quamuis primo aspectu tam obuium videatur, vt quidam ne necessitatem quidem demonstrationis intellexerint. Est vero hoc: *Quemuis numerum, praeter quadrata positiue sumta aliquorum numerorum primorum non-residuum esse.* Quia vero hoc theoremate tantummodo tamquam auxiliari ad alia demonstranda vsuri sumus, alios casus hic non explicamus quam quibus ad hunc finem indigemus. De reliquis casibus postea sponte idem consta-

bit. Ostendemus itaque, *quemuis numerum primum formae* $4n + 1$, *siue positiue siue negatiue accipiatur* *), *non-residuum esse aliquorum numerorum primorum*, et quidem talium qui ipso sint minores.

Primo, quando numerus primus p, formae $4n + 1$, *negatiue* sumendus proponitur, sit $2a$ numerus par proxime maior quam $\sqrt{p}$; tum facile perspicitur, $4aa$ semper fore $< 2p$ siue $4aa - p < p$. At $4aa - p$ est formae $4n + 3$, $+ p$ autem residuum quadraticum ipsius $4aa - p$, (quoniam $p \equiv 4aa \pmod{4aa - p}$); quodsi igitur $4aa - p$ est numerus primus, $- p$ ipsius non-residuum erit; sin minus, necessario factor aliquis ipsius $4aa - p$ formae $4n + 3$ erit; et quum $+ p$ etiam huius residuum esse debeat, $- p$ ipsius non-residuum erit. *Q. E. D.*

Pro numeris primis *positiue* sumendis duos casus distinguimus. *Primo* sit p numerus primus formae $8n + 5$. Sit a numerus quicunque positiuus $< \sqrt{\frac{1}{2}p}$. Tum $8n + 5 - 2aa$ erit numerus positiuus formae $8n + 5$ vel $8n + 3$, prouta par vel impar) adeoque necessario per numerum aliquem primum formae $8n + 3$ vel $8n + 5$ diuisibilis, productum enim ex quotcunque numeris formae $8n + 1$ et $8n + 7$ neque formam $8n + 3$ neque hanc $8n + 5$ habere potest. Sit hic q, eritque $8n + 5 \equiv 2a^2 \pmod{q}$. At 2

*) $+ 1$ autem excipi oportere per se manifestum est.

ipsius q non-residuum erit (art. 112), adeoque etiam $2a^2$ *) et $8n + 5$. *Q. E. D.*

126. Sed numerum quemuis primum formae $8n + 1$ positiue acceptum semper alicuius numeri primi ipso minoris non residuum esse, per artificia tam obuia demonstrari nequit. Quum autem haec veritas maximi sit momenti, demonstrationem rigorosam, quamuis aliquantum prolixa sit, praeterire non possumus. Praetermittus sequens

LEMMA. *Si habentur duae series numerorum, A, B, C, etc. . . . . (I), A', B', C', etc. . . . . (II),* (vtrum terminorum multitudo in vtraque idem sit necne nihil interest) *ita comparatae, vt, denotante p numerum quemcunque primum aut numeri primi potestatem, terminum aliquem secundae seriei (siue etiam plures) metientem, totidem ad minimum termini in serie prima sint per p diuisibiles, quot sunt in secunda: tum dico productum ex omnibus numeris (I) diuisibile fore per productum ex omnibus numeris (II).*

Exempl. Constet (I) e numeris 12, 18, 45; (II) ex his 3, 4, 5, 6, 9. Tum diuisibiles erunt per 2, 4, 3, 9, 5 in (I) 2, 1, 3, 2, 1 termini, in (II) 2, 1, 3, 1, 1 termini, respectiue; productum autem omnium terminorum (I) = 9720 diuisibile est per productum omnium terminorum (II), 3240.

*) Art 98. Patet enim a^2 esse residuum ipsius q per q non diuisibile, nam alias etiam numerus primus p per q foret diuisibilis. *Q. E. A.*

Demonstr. Sit productum ex omnibus terminis (I) $= Q$, productum omnium terminorum seriei (II), $= Q'$. Patet quemuis numerum primum qui sit diuisor ipsius Q' etiam ipsius Qdiuisorem fore. Iam ostendemus quemuis factorem primum ipsius Q', in Q totidem ad minimum dimensiones habere quot habeat in Q'. Esto talis diuisor p, ponaturque, in serie (I) a terminos esse per p diuisibiles neque vero per p^2, b terminos per p^2 non autem per p^3 diuisibiles, c terminos per p^3 non autem per p^4 etc. similia denotent literae a', b', c' etc. pro serie (II), perspicieturque facile, p in Q habere $a + b + c +$ etc. dimensiones, in Q' vero $a' + b' + c' +$ etc. At a' certe non maior quam a, b' non maior quam b etc. (hyp.); quare $a' + b' + c'$ etc. certo non erit $> a + b + c$ etc. — Quum itaque nullus numerus primus in Q' plures dimensiones habere possit, quam in Q, Q per Q' diuisibilis erit (art. 17) *Q. E. D.*

127. Lemma. *In progressione* 1, 2, 3, 4.... n, *plures termini esse nequeunt per numerum quemcunque* h *diuisibiles, quam in hac* $a, a + 1, a + 2, \ldots\ldots a + n - 1$ *ex totidem terminis constante.*

Nullo enim negotio perspicitur si n fuerit multiplum ipsius h, in vtraque progressione $\frac{n}{h}$ terminos fore per h diuisibiles; sin minus, ponatur $n = h + f$, ita vt f sit $< h$, eruntque in priori serie e termini per h diuisibiles, in posteriori autem vel totidem vel $e + 1$.

Hinc tamquam Coroll. sequitur propositio ex numerorum figuratorum theoria nota, sed a nemine, ni fallimur, hactenus directe demonstrata, $\frac{a \cdot a+1 \cdot a+2 \ldots a+n-1}{1 \cdot 2 \cdot 3 \ldots n}$ semper esse numerum integrum.

Denique Lemma hoc generalius ita proponi potuisset:

In progressione a, $a+1$, $a+1$, ... $a+n-1$ totidem ad minimum dantur termini secundum modulum h numero cuicunque dato, r, congrui, quot in hac, 1, 2, 3.... n termini per h diuisibiles.

128. Theorema. *Sit a numerus quicunque formae $8n+1$, p numerus quicunque ad a primus, cuius residuum $+a$, tandem m numerus arbitrarius: tum dico, in progressione a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$, $2(a-16)$, ... $2(a-m^2)$, vel $\frac{1}{2}(a-m^2)$, prout m par vel impar, totidem ad minimum dari terminos per p diuisibiles quot dentur in hac 1, 2, 3.... $2m+1$.* Priorem progressionem designamus per (I) posteriorem per (II).

Demonstr. I. Quando $p = 2$, in (I) omnes termini praeter primum, i. e. m termini diuisibiles erunt; totidem autem erunt in (II).

II. Sit p numerus impar, vel numeri imparis duplum vel quadruplum, atque $a \equiv rr \pmod{p}$. Tum in progressione, $-m$, $-(m-1)$, $-(m-2)$ ..... $+m$ (quae terminorum multitudine cum (I) et (II) conuenit et per

(III) designabitur) totidem ad minimum termini erunt secundum modulum p ipsi r congrui, quot in serie (II) per p diuisibiles (art. praec.). Inter illos autem, bini, qui signo tantum, non magnitudine, discrepent, occurrere nequeunt*). Tandem quisque eorum correspondentem habebit in serie (I), qui per p erit diuisibilis. Scilicet si fuerit $\pm b$ aliquis terminus seriei (III) ipsi r secundum p congruus, erit $a - bb$ per p diuisibilis. Quodsi igitur b est par, terminus seriei (I), $2(a - bb)$, per p diuisibilis erit. Si vero b impar, terminus $\frac{1}{2}(a-bb)$ per p diuisibilis erit: namque manifesto $\frac{a-bb}{p}$ erit integer *par*, quoniam $a - bb$ per 8, p autem ad summum per 4 diuisibilis (a enim per hyp. est formae $8n + 1$, bb autem ideo quod est numeri imparis quadratum eiusdem formae erit, quare differentia erit formae $8n$). Hinc tandem concluditur, in serie (I) totidem terminos esse per p diuisibiles, quot in (III) sint ipsi r secundum p congrui, *i. e.* totidem aut plures quam in (II) sint per p diuisibiles. *Q. E. D.*

III. Sit p formae $8n$, atque $a \equiv rr \pmod{2p}$. Facile enim perspicitur, a, quum ex hyp. ipsius p sit residuum, etiam ipsius $2p$ residuum

*) Si enim esset $r \equiv -f \equiv +f \pmod{p}$, fieret $2f$ per p diuisibilis, adeoque etiam $2a$ (propter $ff \equiv a \pmod{p}$) Hoc autem aliter fieri nequit, quam si $p = 2$, quum per hyp. a ad p sit primus. Sed de hoc casu iam seorsim diximus.

fore. Tum in serie (III) totidem ad minimum termini erunt ipsi r secundum p congrui, quot in (II) sunt per p diuisibiles, illique omnes magnitudine erunt inaequales. At cuique eorum respondebit aliquis in (I) per p diuisibilis. Si enim $+b$ vel $-b \equiv r \pmod{p}$, erit $bb \equiv rr \pmod{2p}$, *) adeoque terminus $\frac{1}{2}(a - rr)$ per p diuisibilis, multoque magis $2(a - rr)$. Quare in (I) totidem ad minimum termini erunt per p diuisibiles quam in (II). *Q. E. D.*

129. Theorema. *Si a est numerus primus formae $8n + 1$, necessario infra $2\sqrt{a}$ dabitur aliquis numerus primus cuius non-residuum sit a.*

Demonstr. Esto, si fieri potest, a residuum omnium primorum ipso $2\sqrt{a}$ minorum. Tum facile perspicietur, a etiam omnium numerorum compositorum ipso $2\sqrt{a}$ minorum residuum fore (conferantur praecepta per quae diiudicare docuimus, vtrum numerus propositus sit numeri compositi residuum necne; art. 105). Sit numerus proxime minor quam $\sqrt{a} = m$. Tum in serie (I)..... a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$.... $2(a - mm)$, vel $\frac{1}{2}(a - mm)$, totidem aut plures termini erunt per numerum quemcunque ipso $2\sqrt{a}$ minorem diuisibiles, quam in hac (II)..... 1, 2, 3, 4.... $2m + 1$ (art. praec.). Hinc vero sequitur, productum ex omnibus terminis (I) per productum omnium terminorum (II) diuisibile

*) Erit scilicet $bb - rr = (b - r)(b + r)$ e duobus factoribus compositus, quorum alter per p diuisibilis (hyp.), alter per 2 (quia tum b tum r sunt impares); adeoque $bb - rr$ per $2p$ diuisibilis.

esse, (art. 126). At illud est aut $= a\,(a-1)\,(a-4)\ldots\,(a-mm)$ aut semissis huius producti (prout m aut par aut impar). Quare productum $a(a-1)(a-4)\ldots(a-mm)$ certo per productum omnium terminorum (II) diuidi poterit, et, quia omnes hi termini ad a sunt primi, etiam productum illud omisso factore a. Sed productum ex omnibus terminis (II) ita etiam exhiberi potest, $(m+1)\cdot((m+1)^2-1)\cdot((m+1)^2-4)\ldots((m+1)^2-m^2)$. Fiet igitur

$$\frac{1}{(m+1)^2}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdot\ldots\cdot\frac{a-m^2}{(m+1)^2-m^2}$$

numerus integer, quamquam sit productum ex fractionibus vnitate minoribus: quia enim necessario $\sqrt{a}$ irrationalis esse debet; erit $m+1 > \sqrt{a}$, adeoque $(m+1)^2 > a$. Hinc tandem concluditur suppositionem nostram locum habere non posse. *Q. E. D.*

Iam quia a certo > 4, erit $2\sqrt{a} < a$, dabiturque adeo aliquis primus $< a$ cuius non residuum a.

130. Postquam rigorose demonstrauimus quemuis numerum primum formae $4n+1$, et positiue et negatiue acceptum, alicuiuis numeri primi ipso minoris non residuum esse, ad comparationem exactiorem et generaliorem numerorum primorum quatenus vnus alterius residuum vel non residuum est, statim transimus.

Omni rigore supra demonstrauimus, -3 et $+5$ esse residua vel non-residua omnium numerorum primorum, qui ipsorum 3, 5 respectiue sint residua vel non-residua.

Per inductionem autem circa numeros sequentes institutam, inuenitur:

— 7, — 11, + 13, + 17, — 19, — 23, + 29, — 31, + 37, + 41, — 43, — 47, + 53, — 59 etc. esse residua vel non-residua omnium numerorum primorum, qui, positiui sumti, illorum primorum respectiue sint residua vel non-residua. Inductio haec perfacile adiumento tabulae II confici potest.

Quiuis autem leui attentione adhibita obseruabit, ex his numeris primis signo positiuo affectos esse eos, qui sint formae $4n + 1$, negatiuo autem eos, qui sint formae $4n + 3$.

131. Quod hic per inductionem detexi-mus, generaliter locum habere mox demonstrabimus. Antequam autem hoc negotium adeamus, necesse erit, omnia quae ex theoremate, si verum esse supponitur, sequuntur, eruere. Theorema ipsum ita enunciamus.

Si p est numerus primus formae $4n + 1$, erit $+ p$, si vero p formae $4n + 3$, erit $- p$ residuum vel non-residuum cuiusuis numeri primi qui positiue acceptus ipsius p est residuum vel non-residuum.

Quia omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio *theorematis fundamentalis*, qua in sequentibus vtemur, haud absona erit.

Vt ratiocinia nostra quam breuissime exhiberi possint, per a, a', a'' etc. numeros primos

formae $4n + 1$, per b, b', b'' etc. numeros primos formae $4n + 3$ denotabimus; per A, A', A'' etc. numeros quoscunque formae $4n + 1$, per B, B', B'' etc. autem numeros quoscunque formae $4n + 3$; tandem litera R duabus quantitatibus interposita indicabit, priorem sequentis esse residuum, sicuti litera N significationem contrariam habebit. Ex. gr. $+ 5R11$, $\pm 2N5$, indicabit $+ 5$ ipsius 11 esse residuum, $+ 2$ vel $- 2$ esse ipsius 5 non-residuum. Iam collato theoremate fundamentali cum theorematibus art. 111, sequentes propositiones facile deducentur.

Si	erit
1. $\pm aRa'$	$\pm a'Ra$
2. $\pm aNa'$	$\pm a'Na$
3. $\begin{cases} + aRb \\ - aNb \end{cases}$	$\pm bRa$
4. $\begin{cases} + aNb \\ - aRb \end{cases}$	$\pm bNa$
5. $\pm bRa$	$\begin{cases} + aRb \\ - aNb \end{cases}$
6. $\pm bNa$	$\begin{cases} + aNb \\ - aRb \end{cases}$
7. $\begin{cases} + bRb' \\ - bNb' \end{cases}$	$\begin{cases} + b'Nb \\ - b'Rb \end{cases}$
8. $\begin{cases} + bNb' \\ - bRb' \end{cases}$	$\begin{cases} + b'Rb \\ - b'Na \end{cases}$

132. In his omnes casus, qui, duos numeros primos comparando, occurrere possunt, continentur: quae sequuntur, ad numeros quoscunque pertinent: sed harum demonstrationes minus sunt obuiae.

	Si	erit
9.	$\pm aRA\ldots\ldots$	$\pm ARa$
10.	$\pm bRA\ldots\ldots$	$\begin{cases} + ARb \\ - ANb \end{cases}$
11.	$+ aRB\ldots\ldots$	$\pm BRa$
12.	$- aRB\ldots\ldots$	$\pm BNa$
13.	$+ bRB\ldots\ldots$	$\begin{cases} - BRb \\ + BNb \end{cases}$
14.	$- bRB\ldots\ldots$	$\begin{cases} - BRb \\ + BNb \end{cases}$

Quum omnium harum propositionum demonstrationes ex iisdem principiis sint petendae, necesse non erit omnes euoluere: demonstratio prop. 9, quam apponimus tamquam exemplum inseruire potest. Ante omnia autem obseruetur, quemuis numerum formae $4n + 1$ aut nullum factorem formae $4n + 3$ habere, aut duos, aut quatuor etc. i. e. multitudinem talium factorum (inter quos etiam aequales esse possunt) semper fore parem: quemuis vero formae $4n + 3$ multitudinem imparem factorum formae $4n + 3$ (i. e. aut vnum aut tres aut

quinque etc.) implicare. Multitudo factorum formae $4n + 1$ indeterminata manet.

Prop. 9 ita demonstratur. Sit A productum e factoribus primis a', a'', a''' etc., b, b', b'' etc.; eritque factorum b, b', b'' multitudo par (possunt etiam nulli adesse, quod eodem redit). Iam si a est residuum ipsius A, erit residuum etiam omnium factorum a', a'', a''' etc. b, b', b'' etc. quare per propp. 1, 3 art. praec. singuli hi factores erunt residua ipsius a, adeoque etiam productum A. — A vero idem esse debet. — Quodsi vero — a est residuum ipsius A, eoque ipso omnium factorum a', a'' etc. b, b' etc.; singuli a', a'' etc erunt ipsius a residua, singuli b, b' etc. autem non residua. Sed quum posteriorum multitudo sit par, productum ex omnibus, *i. e.* A, ipsius a residuum erit, hincque etiam — A.

133. Inuestigationem adhuc generalius instituamus. Contemplemur duos numeros quoscunque impares inter se primos, signis quibuscunque affectos, P et Q. Concipiatur P sine respectu signi sui in factores suos primos resolutus, designeturque per p, quot inter hos reperiantur quorum non-residuum sit Q. Si vero aliquis numerus primus, cuius non-residuum est Q, pluries inter factores ipsius P occurrit, pluries etiam numerandus erit. Similiter sit q multitudo factorum primorum ipsius Q, quorum non-residuum est P. Tum numeri p, q certam relationem mutuam habebunt ab

indole numerorum P, Q pendentem. Scilicet si alter numerorum p, q est par vel impar, numerorum P, Q forma docebit, vtrum alter par sit vel impar. Haec relatio in sequenti tabula exhibetur.

Erunt p, q simul pares vel simul impares, quando numeri P, Q habent formas:

1. $+A, +A'$
2. $+A, -A'$
3. $+A, +B$
4. $+A, -B$
5. $-A, -A'$
6. $+B, -B'$

Contra numerorum p, q alter erit par, alter impar, quando numeri P, Q habent formas:

7. $-A, +B$
8. $-A, -B$
9. $+B, +B'$
10. $-B, -B'$.

Ex. Sint numeri propositi — 55 et + 1197, qui ad casum quartum erunt referendi. Est autem 1197 non-residuum vnius factoris primi ipsius 55, scilicet numeri 5, — 55 autem non-residuum trium factorum primorum ipsius 1197, scilicet numerorum 3, 3, 19.

Si P et Q numeros primos designant, propositiones hae abeunt in eas quas art. 131 tra-

didimus. Hic scilicet p et q maiores quam 1 fieri nequeunt, quare quando p ponitur esse par necessario erit $= 0$ i. e, Q erit residuum ipsius P, quando vero p est impar, Q ipsius P non-residuum erit. Et vice versa. Ita scriptis a, b loco ipsorum A, B, ex 8 sequitur, si $-a$ fuerit residuum vel non-residuum ipsius b, fore $-b$ non-residuum vel residuum ipsius a, quod cum 3 et 4 art. 131 conuenit.

Generaliter vero patet, Q residuum ipsius P esse non posse nisi fuerit $p = 0$; si igitur p impar, Q certo ipsius P non-residuum erit.

Hinc etiam propp. art. praec. sine difficultate deriuari possunt.

Ceterum mox patebit, hanc repraesentationem generalem plus esse quam speculationem sterilem, quum theorematis fundamentalis demonstratio completa absque ea vix perfici possit.

134. Aggrediamur nunc deductionem harum propositionum.

I. Concipiatur, vt ante, P in factores suos primos resolutus, signis neglectis, insuperque etiam Q in factores quomodocunque resoluatur, ita tamen vt signi ipsius Q ratio habeatur. Combinentur illi singuli cum singulis his. Tum si s designat multitudinem omnium combinationum, in quibus factor ipsius Q est non-residuum factoris ipsius P, p et s vel simul pares vel

simul impares erunt. Sint enim factores primi ipsius P, hi f, f' f'' etc. et inter factores in quibus Q est resolutus, sint m qui ipsius f sint non-residua, m' non-residua ipsius f', m'' non-residua ipsius f'' etc. Tum facile quisquis perspiciet, fore $s = m + m' + m'' +$ etc., p autem exprimere quot numeri inter ipsos m, m', m'' etc. sint impares. Vnde sponte patet, s fore parem, quando p sit par, imparem quando p sit impar.

II. Haec generaliter valent, quomodocunque Q in factores sit resolutus. Descendamus ad casus particulares. Contemplemur primo casus, vbi alter numerorum, P, est positiuus, alter vero, Q, vel formae $+A$ vel formae $-B$. Resoluantur P, Q in factores suos primos, attribuatur singulis factoribus ipsius P signum positium, singulis autem factoribus ipsius Q signum positiuum vel negatiuum, prout sunt formae a vel b; tunc autem manifesto Q fiet vel formae $+A$ vel $-B$ vti requiritur. Combinentur factores singuli ipsius P cum singulis factoribus ipsius Q, designetque vt ante s multitudinem combinationum in quibus factor ipsius Q est non residuum factoris ipsius P, similiterque t multitudinem combinationum in quibus factor ipsius P est non-residuum factoris ipsius Q. At ex theoremate fundamentali sequitur illas combinationes indenticas fore cum his adeoque $s = t$. Tandem ex iis quae modo demonstrauimus sequitur esse $p \equiv s \pmod 2$; $q \equiv t \pmod 2$, vnde fit $p \equiv q \pmod 2$.

Habentur itaque propp. 1, 3, 4 et 6 art. 133.

Propositiones reliquae per methodum similem directe erui possunt, sed vna consideratione noua indigent; facilius autem ex praecedentibus sequenti modo deriuantur.

III. Denotent rursus P, Q, numerus quoscunque impares inter se primos, p, q multitudinem factorum primorum ipsorum P, Q, quorum non-residua Q, P respectiue. Tandem sit p' multitudo factorum primorum ipsius P, quorum non-residuum est $-Q$ (quando Q per se est negatiuus, manifesto $-Q$ numerum positiuum indicabit). Iam omnes factores primi ipsius P in quatuor classes distribuantur.

1) in factores formae a, quorum residuum est Q.

2) factores formae b, quorum residuum Q. Horum multitudo sit χ.

3) factores formae a, quorum non-residuum est Q. Horum multitudo sit ψ.

4) factores formae b, quorum non-residuum Q. Quorum multitudo $= \omega$.

Tum facile perspicitur fore $p = \psi + \omega$, $p' = \chi + \psi$.

Iam quando P est formae $\pm A$, erit $\chi + \omega$ adeoque etiam $\chi - \omega$ numerus par: quare fiet $p' = p + \chi - \omega \equiv p \pmod 2$; quando vero P est formae $\pm B$, per simile ratiocinium in-

uenitur, numeros p, p' sec. mod. 2 incongruos fore.

IV. Applicemus haec ad casus singulos. Sit primo tum P, tum Q formae $+A$, eritque ex prop. 1. $p \equiv q \pmod 2$; at erit $p' \equiv p \pmod 2$; quare etiam $p' \equiv q \pmod 2$. Quod conuenit cum prop. 2. — Simili modo si P est formae $+A$, Q formae $-A$, erit $p \equiv q \pmod 2$ ex prop. 2 quam modo demonstrauimus; hinc, ob $p' \equiv p$, erit $p' \equiv q$. Est itaque etiam prop. 5 demonstrata.

Eodem modo prop. 7 ex 3; prop. 8 vel ex 4 vel ex 7; prop. 9 ex 6; ex eademque prop. 10 deriuantur.

135. Per art. praec. propositiones art. 133 non quidem sunt demonstratae, sed tamen earum veritas a veritate theorematis fundamentalis quam aliquantisper supposuimus pendere ostensa est. At ex ipsa deductionis methodo manifestum est, illas valere pro numeris P, Q, si modo theorema fundamentale pro omnibus factoribus primis horum numerorum inter se comparatis locum habeat, etiamsi generaliter verum non sit. Nunc igitur ipsius theorematis fundamentalis demonstrationem aggrediamur. Cui praemittimus sequentem explicationem.

Theorema fundamentale vsque ad numerum aliquem M verum esse dicemus, si valet pro duobus numeris primis quibuscunque, quorum neuter ipsum M superat.

Simili modo intelligi debet, si theoremata artt. 131, 132, 133 vsque ad aliquem terminum vera esse dicemus. Facile vero perspicitur, si de veritate theorematis fundamentalis vsque ad aliquem terminum constet, has propositiones vsque ad eundum terminum locum esse habituras.

136. Theorema fundamentale pro numeris paruis verum esse per inductionem facile confirmari, atque sic limes determinari potest vsque ad quem certo loco teneat. Hanc inductionem institutam esse postulamus: prorsus autem indifferens est quousque eam persequuti simus; sufficeret adeo, si tantummodo vsque ad numerum 5 eam confirmauissemus, hoc autem per vnicam obseruationem absoluitur, quod est $+ 5N3$, $\pm 3N5$.

Iam si theorema fundamentale generaliter verum non est, dabitur limes aliquis, T, vsque ad quem valebit, ita tamen vt vsque ad numerum proxime maiorem, $T + 1$, non amplius valeat. Hoc autem idem est ac si dicamus, dari duos numeros primos quorum maior sit $T + 1$, et qui inter se comparati theoremati fundamentali repugnent, binos autem alios numeros primos quoscunque, si modo ambo ipso $T + 1$ sint minores, huic theoremati esse consentaneos. Vnde sequitur, propositiones artt. 131, 132, 133 vsque ad T etiam locum habituras. Hanc vero suppositionem consistere non posse nunc ostendemus. Erunt autem secundum formas diuersas, quas tum

$T + 1$, tum numerus primus ipso $T + 1$ minor, quem cum $T + 1$ comparatum theoremati repugnare supposuimus, habere possunt, casus sequentes distinguendi. Numerum istum primum per p designamus.

Quando tum $T + 1$ tum p sunt formae $4n + 1$, theorema fundamentale duobus modis falsum esse posset, scilicet si simul esset, *vel* $\pm pR(T + 1)$ et $\pm(T + 1)Np$, *vel simul* $\pm pN(T + 1)$ et $\pm(T + 1)Rp$.

Quando tum $T + 1$ tum p sunt formae $4n + 3$, theor. fund. falsum erit, si simul fuerit *vel* $+ pR(T + 1)$, et $-(T + 1)Np$ (siue quod eodem redit $- pN(T + 1)$ et $+(T+1)Rp$); *vel* $+ pN(T + 1)$ et $-(T + 1)Rp$ (siue $- pR(T + 1)$ et $+(T + 1)Np$).

Quando $T + 1$ est formae $4n + 1$, p vero formae $4n + 3$, theor. fund. falsum erit, si fuerit *vel* $\pm pR(T + 1)$ et $+(T + 1)Np$ (siue $-(T + 1)Rp$); *vel* $\pm pN(T + 1)$ et $-(T + 1)Np$ (siue $+(T + 1)Rp$).

Quando $T + 1$ est formae $4n + 3$, p vero formae $4n + 1$, theor. fund. falsum erit, si fuerit *vel* $+ pR(T + 1)$, (siue $- pN(T+1)$) et $\pm(T + 1)Np$, *vel* $+ pN(T + 1)$ (siue $- pR(T + 1)$), et $\pm(T + 1)Rp$.

Si demonstrari poterit, nullum horum octo casuum locum habere posse, simul certum erit, theorematis fundamentalis veritatem nul-

lis limitibus circumscriptam esse. Hoc itaque negotium nunc aggredimur: at quoniam alii horum casuum ab aliis sunt dependentes, eundum ordinem, quo eos hic enumerauimus seruare non licebit.

137. *Casus primus. Quando* $T + 1$ *est formae* $4n + 1$, $(= a)$, *atque* p *eiusdem formae; insuper vero* $\pm pRa$, *non potest esse* $\pm aNp$. Hic casus supra fuit primus.

Sit $+ p \equiv e^2 \pmod{a}$, atque e par et $< a$, (quod semper obtineri potest). Iam duo casus sunt distinguendi.

I. Quando e per p non est diuisibilis. Ponatur $e^2 = p + af$, eritque f positiuus, formae $4n + 3$ (siue formae B), $< a$, et per p non diuisibilis. Porro erit $e^2 \equiv p \pmod{f}$, i. e. pRf adeoque ex prop. 11 art. 132 $\pm fRp$ (quia enim p, $f < a$, pro his propositiones istae valebunt). At est etiam $af\ Rp$, quare fiet quoque $\pm a\ Rp$.

II. quando e per p est diuisibilis, ponatur $e = gp$, atque $e^2 \equiv p + aph$, siue $pg^2 = 1 + ah$. Tum erit h formae $4n + 3$ (B), atque ad p et g^2 primus. Porro erit $pg^2\ Rh$, adeoque etiam $p\ Rh$, hinc (prop. 11 art. 132), $= h\ Rp$. At est etiam $- ah\ Rp$, quia $- ah \equiv 1 \pmod{p}$; quare fiet etiam $\mp aRp$.

138. *Casus secundus. Quando* $T + 1$ *est formae* $4n + 1$, $(= a)$, p *formae* $4n + 3$, *atque*

$\pm p\ R\,(T+1)$, *non potest esse* $+\,(T+1)\,Np$, *siue* $-\,(T+1)\,Rp$. Hic casus supra fuit quintus.

Sit vt supra $e^2 = p + fa$ atque e par et $< a$.

I. Quando e per p non est diuisibilis, erit etiam f per p non diuisibilis. Praeterea autem erit f positiuus, formae $4n+1$ (siue A), atque $< a$; $+\,pRf$, adeoque (prop. 10 art. 132) $+\,fRp$. Sed est etiam $+\,faRp$, quare fiet $+\,aRp$, siue $-\,aNp$.

II. Quando e per p est diuisibilis, sit $e = pg$, atque $f = ph$. Erit itaque $g^2p = 1 + ha$. Tum h erit positiuus, formae $4n+3$ (B), et ad p et g^2 primus. Porro $+\,g^2pRh$, adeoque $+\,pRh$; hinc fit (prop, 13 art 132) $-\,hRp$. At est $-\,haRp$, vnde fit $+\,aRp$ atque $-\,aNp$.

139. *Casus tertius. Quando* $T+1$ *est formde* $4n+1$, $(=a)$, p *eiusdem formae, atque* $\pm\,pNa$: *non potest esse* $\pm\,aNp$. (Supra casus secundus).

Capiatur aliquis numerus primus ipso a minor, cuius non-residuum sit $+a$, quales dari supra demonstrauimus (art. 125, 129). Sed hic duos casus seorsim considerare oportet, prout hic numerus primus fuerit formae $4n+1$ vel $4n+3$; non enim demonstratum fuit, dari tales numeros primos *vtriusque* formae.

I. Sit iste numerus primus formae $4n+1$ et $= a'$. Tum erit $\pm\,a'Na$ (art. 137) adeoque

$\pm a'pRa$. Sit igitur $e^2 \equiv a'p \pmod{a}$ atque e par, $< a$. Tunc iterum quatuor casus erunt distinguendi.

1) Quando e neque per p neque per a' est diuisibilis. Ponatur $e^2 = a'p \pm af$, signis ita acceptis vt f fiat positiuus. Tum erit $f < a$, ad a' et p primus atque pro signo superiori formae $4n + 3$, pro inferiori formae $4n + 1$. Designemus breuitatis gratia per $[x, y]$ multitudinem factorum primorum numeri y quorum non-residuum est x. Tum erit $a'pRf$ adeoque $[a'p, f] = 0$. Hinc erit $[f, a'p]$ numerus par, (prop. 1, 3, art. 133.), i. e. aut $= 0$ aut $= 2$. Quare erit f aut residuum vtriusque numerorum a', p, aut neutrius. Illud autem est impossibile, quum $\pm af$ sit residuum ipsius a', atque $\pm aNa'$ (hyp.); vnde fit $\pm fNa'$. Hinc f debet esse vtriusque numerorum a', p non-residuum. At propter $\pm afRp$ erit $\pm aNp$. *Q. E. D.*

2) Quando e per p, neque vero per a' est diuisibilis, sit $e = gp$, atque $g^2p = a' \pm ah$, signo ita determinato, vt h fiat positiuus. Tum erit $h < a$, ad a', g, et p primus, atque pro signo superiori formae $4n + 3$, pro inferiori vero formae $4n + 1$. Ex aequatione $g^2p = a' \pm ah$ si per p, et a' multiplicatur, nullo negotio deduci potest, $pa'Rh$..... (α); $\pm ahpRa'$ ....(β) $aa'hRp$..... (γ). Ex (α) sequitur $[pa', h] = 0$, adeoque (prop, 1, 3, art. 153) $[h, pa']$ par, i. e. erit h non-residuum vel vtriusque p, a', vel

neutrius. *Priori in casu* ex (ζ) sequitur, $\pm apNa'$, et quum per hyp. sit $\pm aNa'$, erit $\pm pRa'$, Hinc per theor. fundam. quod pro numeris p', a' ipso $T+1$ minoribus valet, $\pm a'Rp$. Hinc et ex eo quod hNp, fit per (γ) $\pm aNp$ *Q. E. D. Posteriori casu* ex (ζ) sequitur $\pm apRa'$, hinc $\pm pNa'$, $\pm a'Np$ hincque tandem et ex hRp fit ex (γ) $\pm aNp$ *Q. E. D.*

3) Quando e per a' non autem per p est diuisibilis. Pro hoc casu demonstratio tantum non eodem modo procedit vt in praec., neminemque qui hanc penetrauit poterit morari.

4) Quando e tum per a' tum per p est diuisibilis adeoque etiam per productum $a'p$ (numeros a',p enim *inaequales* esse supponimus, quia alias id quod demonstrare operam damus, esse aNa' iam in hypothesi aNp contentum foret), sit $e = ga'p$ atque $g^2a'p = 1 \pm ah$. Tum erit $h < a$, ad a' et p primus atque pro signo superiori formae $4n+3$, pro inferiori formae $4n+1$. Facile vero perspicitur, ex ista aequatione deduci posse haec $a'pRh$, $\pm ahpRa'$, $\pm aa'hRp$; quae cum iis quae in (2) inuenimus conueniunt. In reliquis autem demonstratio est eadem.

II. Quando iste numerus primus est formae $4n+3$, demonstratio praecedenti tam similis est, vt eam apponere superfluum nobis visum sit. In eorum gratiam qui per se eam euoluere gestiunt (quod maxime commenda-

mus), id tantum obseruamus, postquam ad talem aequationem $e^2 = bp \pm af$ (designante b illum numerum primum) peruentum fuerit, ad perspicuitatem profuturum, si vtrumque signum seorsim consideretur.

140. *Casus quartus.* *Quando* $T + 1$ *est formae* $4n + 1$, $(= a)$, p *formae* $4n + 3$, *atque* $\pm pNa$, *non poterit esse* $+ aRp$, *siue* $- aNp$. (Casus sextus supra).

Etiam huius casus demonstrationem quum prorsus similis sit demonstrationi casus tertii breuitatis gratia omittimus.

141. *Casus quintus.* *Quando* $T + 1$ *est formae* $4n + 3$, $(= b)$, p *eiusdem formae, atque* $+ pRb$ (*siue* $- pNb$), *nequit esse* $+ bRp$, *siue* $- bNp$. (Casus tertius supra).

Sit $p \equiv e^2 \pmod{b}$, atque e par et $< b$.

I. Quando e per p non est diuisibilis. Ponatur $e^2 = p + bf$, eritque f positiuus, formae $4n + 3$, $< b$ atque ad p primus. Porro erit pRf adeoque per prop. 13. art 132, $- fRp$. Hinc et ex $+ bfRp$ fit $- bRp$ adeoque $+ bNp$ *Q. E. D.*

II. Quando e per p est diuisibilis, sit $e = pg$, atque $ggp = 1 + bh$. Tum erit h formae $4n + 1$ atque ad p primus, $p \equiv g^2 p^2 \pmod{h}$, adeoque pRh; hinc fit $+ hRp$ (prop.

10 art. 132), vnde et ex — $bhRp$ sequitur — bRp, siue + bNp. *Q. E. D.*

142. *Casus sextus. Quando* $T + 1$ *est formae* $4n + 3$, $(= b)$, p *formae* $4n + 1$, *atque* pRb, *non poterit esse* $\pm bNp$. Supra casus septimus.

Demontrationem praecedenti omnino similem, omittimus.

143. *Casus septimus. Quando* $T + 1$ *est formae* $4n + 3$, $(= b)$, p *eiusdem formae atque* $+ pNb$ *siue* $- pRb$, *non poterit esse* $+ bNp$ *siue* $- bRp$. (Casus quartus supra)

Sit $-p \equiv e^2 \pmod{b}$, atque e par et $< b$.

I. Quando e per p non diuisibilis. Sit $-p = e^2 - bf$ eritque f positiuus, formae $4n+1$, ad p primus ipsoque b minor (etenim e certo non maior quam $b - 1$, $p < b - 1$, quare erit $bf = e^2 + p < b^2 - b$. i. e. $f < b - 1$). Porro erit $- pRf$, hinc (prop. 10 art. 132) $+ fRp$, vnde et ex $+ bfRp$ fit $+ bRp$, siue $- bNp$.

II. Quando e per p est diuisibilis, sit $e = pg$, atque $g^2p = -1 + bh$. Tum erit h positiuus, formae $4n + 3$, ad p primus et $< b$. Porro erit pRh, vnde fit (prop. 14 art 132) $+ hRp$. Hinc et ex bRp equitur $+ bRp$ siue $- bNp$. *Q. E. D.*

144. *Casus octauus. Quando* $T + 1$ *est formae* $4n + 3$, $(=b)$, *p formae* $4n + 1$, *atque* $+ pNb$ *siue* $- pRb$, *non poterit esse* $\pm bRp$. Casus vltimus supra.

Demonstratio perinde procedit vt in casu praecedente.

145. In demonstrat. praec. semper pro *e* valorem parem accepimus (art. 137. 144); obseruare conuenit, etiam valorem imparem adhiberi potuisse, sed tum plures adhuc distinctiones introducendae fuissent. Qui his disquisitionibus delectantur, haud inutile facient, si vires suas in euolutione horum casuum exercitent. Praeterea theoremata ad residua $+ 2$ et $- 2$ pertinentia tunc supponi debuissent; quum vero nostra demonstratio absque his theorematibus sit perfecta, nouam hinc methodum nanciscimur, illa demonstrandi. Quae minime est contemnenda, quum methodi, quibus supra pro demonstratione theorematis, ± 2 esse residuum cuiusuis numeri primi formae $8n + 1$, vsi sumus, minus directae videri possint. Reliquos casus (qui ad numeros primos formarum $8n + 3$, $8n + 5$, $8n + 7$ spectant) per methodus supra traditas demonstratos, illudque theorema tantummodo per inductionem inuentum esse supponemus; hanc autem inductionem per sequentes reflexiones ad certitudinis gradum euehemus.

Si ± 2 omnium numerorum primorum formae $8n + 1$ residuum non esset, ponatur

minimus primus huius formae, cuius non-residuum ± 2, $= a$, ita vt pro omnibus primis ipso a minoribus theorema valeat. Tum accipiatur numerus aliquis primus $< \frac{1}{2}a$, cuius non-residuum a (qualem dari ex art. 129 facile deducitur). Sit hic $= p$ eritque per theor. fund. pNa. Hinc fit $\pm 2pRa$. — Sit itaque $e^2 \equiv 2p$ (mod. a) ita vt e sit impar atque $< a$. Tum duo casus erunt distinguendi.

I. Quando e per p non est diuisibilis. Sit $e^2 = 2p + aq$ eritque q positiuus, formae $8n + 7$ vel formae $8n + 3$, (prout p est formae $4n + 1$ vel $4n + 3$), $< a$, atque per p non diuisibilis. Iam omnes factores primi ipsius q in quatuor classes distribuantur, sint scilicet e formae $8n + 1$, f formae $8n + 3$, g formae $8n + 5$, h formae $8n + 7$; productum e factoribus primae classis sit E, producta e factoribus secundae, tertiae, quartae classis respectiue, F, G, H*). His ita factis, consideremus *primo* casum vbi p est formae $4n + 1$, siue q formae $8n + 7$. Tum facile perspicitur fore $2RE$, $2RH$, vnde pRE, pRH, hincque tandem ERp, HRp. Porro erit 2 non-residuum cuiusuis factoris formae $8n + 3$ aut $8n + 5$, adeoque etiam p; hinc quiuis talis factor non-residuum ipsius p; vnde facile concluditur FG fore ipsius p residuum, si $f + g$ fuerit par, non-residuum, si $f + g$ fuerit impar. At $f + g$ impar esse non potest; facile enim perspicietur omnes casus enumerando, $EFGH$ siue q fieri

*) Si ex aliqua classe nulli factores adessent, loco producti ex his 1 scribere oporteret.

vel formae $8n + 3$ vel $8n + 5$, si fuerit $f + g$ impar, quidquid sint singuli e, f, g, h. contra hyp. Erit igitur $FGRp$, $EFGHRp$, siue qRp, hincque tandem, propter $aqRp$, aRp *contra hyp.* *Secundo* quando p est formae $4n + 3$, simili modo ostendi potest, fore pRE adeoque ERp, — pRF adeoque FRp, tandem $g + h$ parem hincque $GHRp$, vnde tandem sequitur qRp, aRp *contra hyp.*

II. Quando e per p diuisibilis, demonstratio simili modo adornari, et a peritis (quibus solis hic articulus est scriptus) haud difficulter euolui poterit. Nos breuitatis gratia eam omittimus.

146. Per theorema fundamentale atque propositiones ad residua — 1 et $\pm$ 2 pertinentes semper determinari potest vtrum numerus quicunque datus numeri primi dati residuum sit an non-residuum. At haud inutile erit, reliqua etiam quae supra tradidimus hic iterum in conspectum producere, vt omnia coniuncta habeantur quae sunt necessaria ad solutionem

Problematis: *Propositis duobus numeris quibuscunque P, Q, inuenire, vtrum alter Q, alterius P residuum sit an non-residuum.*

Sol. I. Sit $P = a^\alpha b^\beta c^\gamma$ etc. designantibus a, b, c etc. numeros primos inaequales positiue acceptos (nam P manifesto absolute est sumendus). Breuitatis gratia in hoc art. *relationem* duorum numerorum x, y simpliciter di-

cemus eam quatenus prior x posterioris y residuum est vel non-residuum. Pendet igitur relatio ipsorum Q, P a relationibus ipsorum Q, a^α Q, b^β etc. (art. 105).

II. Vt relatio ipsorum Q, a^α (de reliquis enim Q, b^β etc. idem valet) innotescat, duo casus distinguendi.

1. Quando Q per a est diuisibilis. Ponatur $Q = Q'a^e$, ita vt Q' per a non sit diuisibilis. Tunc si $e = \alpha$ vel $e > \alpha$, erit QRa^α; si vero $e < \alpha$ atque impar, erit QNa^α: tandem si $e < \alpha$ atque par, habebit Q ad a^α eandem relationem quam habet Q' ad $a^{\alpha-e}$. Reductus est itaque hic casus ad

2. Quando Q per a non est diuisibilis. Hic denuo duos casus distinguimus.

(A) Quando $a = 2$. Tunc semper erit QRa^α, quando $\alpha = 1$; quando vero $\alpha = 2$, requiritur, vt sit Q formae $4n + 1$; denique quando $\alpha = 3$ vel > 3. Q debet esse formae $8n + 1$. Quae conditio si locum habet, erit QRa^α.

(B) Quando a est alius numerus primus. Tunc Q ad a^α eandem relationem habebit quam habet ad a. (V. art. 101).

III. Relatio numeri cuiuscunque Q ad numerum primum a (imparem) ita inuestigatur.

Quando $Q > a$, substituatur loco ipsius Q ipsius residuum minimum positiuum secundum modulum a*). Hoc ad a eandem relationem habebit quam habet Q.

Porro resoluatur Q, siue numerus ipsius loco assumtus, in factores suos primos p, p', p'' etc., quibus adiungendus factor — 1, quando Q est negatiuus. Tum constat relationem ipsius Q ad a pendere a relationibus singulorum p, p', p'' etc. ad a. Scilicet si inter illos factores sunt $2m$ non-residua ipsius a erit QRa, si vero $2m + 1$, erit QNa. Facile autem perspicitur, si inter factores p, p', p'' etc., bini aut quaterni aut seni aut generaliter $2k$ aequales occurrant hos tuto eiici posse.

IV. Si inter factores p, p', p'' reperiuntur — 1 et 2, horum relatio ad a ex artt. 108, 112, 113, 114 inueniri potest. Reliquorum autem relatio ad a pendet a relatione ipsius a ad ipsos (*theor. fund.*, atque propp. art. 131). Sit p vnus ex ipsis, inuenieturque, (tractando numerus a, p eodem modo vt antea Q et a illis respectiue maiores) relationem ipsius a ad p aut per artt. 108—114 determinari posse (si scilicet residuum minimum ipsius a (mod. p) nullos factores primos impares habeat), aut insuper a relatione ipsius p ad numeros quosdam primos ipso p minores pendere. Idem valet de reliquis factoribus p', p'' etc. Facile

*) *Residuum* in signific. art. 4. — Plerumque praestat residuum *absolute* minimum accipere.

iam perspicitur per continuationem huius operationes tandem ad numeros peruentum iri quorum relationes per propp. artt. 108—114 determinari possint. Per exemplum haec clariora fient.

Ex. Quaeritur relatio numeri + 453 ad 1236. Est $1236 = 4.3.103$; $+453 R 4$ per II. 2 (*A*); $+453 R 3$ per II. 1. Superest igitur vt relatio ipsius + 453 ad 103 exploretur. Eadem autem erit quam habet + 41 ($\equiv 453$, mod. 103) ad 103; eadem ipsius + 103 ad 41 (*theor. fund.*), siue ipsius — 20 ad 41. At est $-20 R 41$; namque $-20 = -1.2.2.5$; $-1 R 41$, (art. 108); atque $+5 R 41$ ideo quod $41 \equiv 1$ adeoque ipsius 5 residuum est (theor. fund.). Hinc sequitur $+453 R 103$, hincque tandem $+453 R 1236$. Est autem reuera $453 \equiv 297^2$ (mod. 1236).

147. Proposito numero quocunque *A*, *formulae* certae exhiberi possunt, sub quibus omnes numeri ad *A* primi quorum residuum est *A* continentur, siue omnes qui esse possunt *diuisores* numerorum formae $xx - A$ (designante xx quadratum indeterminatum) *). Sed breuitatis gratia ad eos tantum diuisores respiciemus, qui sunt impares atque ad *A* primi, quum ad hos casus reliqui facile reduci possint.

*) Huiusmodi numeros simpliciter *diuisores ipsius* $xx - A$ dicemus vnde sponte patet quid sint *non-diuisores*.

Sit primo A aut numerus primus positiuus formae $4n + 1$, aut negatiuus formae $4n - 1$. Tum secundum theorema fundamentale omnes numeri primi, qui, positiue sumti, sunt residua ipsius A, erunt diuisores ipsius $xx - A$: omnes autem numeri primi (excepto numero 2 qui semper est diuisor) qui ipsius A sunt non residua erunt non diuisores ipsius $xx - A$. Sint omnia residua ipsius A ipso A minora (exclusa cifra), r, r' r'' etc. omnia non-residua vero n, n' n'' etc. Tum quiuis numerus primus, in aliqua formarum $Ak + r$, $Ak + r'$, $Ak + r''$ etc. contentus, erit diuisor ipsius $xx - A$, quiuis autem primus in aliqua formarum $Ak + n$, $Ak + n'$ etc. contentus non-diuisor erit, designante k numerum integrum indeterminatum. Illas formas dicimus *formas diuisorum ipsius* $xx - A$, has vero *formas non-diuisorum*. Vtrorumque multitudo erit $\frac{1}{2}(A - 1)$. Porro si B est numerus compositus impar atque ARB, omnes factores primi ipsius B in aliqua formarum primorum continentur adeoque etiam B. Quare *quiuis* numerus impar in forma non-diuisorum contentus, erit non-diuisor formae $xx - A$. Sed hoc theorema conuertere non licet; nam si B est non-diuisor compositus impar formae $xx - A$, inter factores primos ipsius B aliqui non-diuisores erunt, quorum multitudo si est *par*, B nihilominus in aliqua forma diuisorum reperietur, V. art. 99.

Ex. Hoc modo pro $A = -11$ formae diuisorum ipsius $xx + 11$ inueniuntur hae:

$11k + 1, 3, 4, 5, 9$, formae non diuisorum autem erunt $11k + 2, 6, 7, 8, 10$. Erit itaque -11 non-residuum omnium numerorum imparium, qui in aliqua posteriorum formarum continentur, residuum autem omnium primorum ad aliquam priorum pertinentium.

Similes formae dantur pro diuisoribus atque non-diuisoribus ipsius $xx - A$, quemcunque numerum designet A. Sed facile perspicitur, eos ipsius A valores tantummodo considerari oportere, qui per nullum quadratum sint diuisibiles; patet enim si fuerit $A = a^2 A'$, omnes diuisores *) ipsius $xx - A$ etiam fore diuisores ipsius $xx - A'$, similiterque non-diuisores. — Distinguemus autem tres casus, 1) quando A est formae $+(4n + 1)$ vel $-(4n - 1)$. 2) quando A est formae $-(4n + 1)$ vel $+(4n - 1)$. 3) quando A est par siue formae $\pm(4n + 2)$

148. *Casus primus*, quando A est formae $+(4n + 1)$ vel $-(4n - 1)$. Resoluatur A in factores suos primos, tribuaturque iis qui sunt formae $4n + 1$ signum positiuum, iis vero qui sunt formae $4n - 1$ signum negatiuum (vnde fiet productum ex ipsis $= A$). Sint hi factores a, b, c, d etc. Distribuantur omnes numeri ipso A minores et ad A primi in duas classes, et quidem in primam classem omnes nu-

*) Nempe qui sint primi ad A.

meri qui sunt nullius ex numeris a, b, c, d etc. non-residua, aut duorum, aut quatuor aut generaliter multitudinis paris; in secundam vero ii, qui sunt non residua vnius ex numeris a, b, c etc. aut trium etc. aut generaliter multitudinis imparis. Designentur priores per r, r' r'', etc. posteriores per n, n', n'' etc. Tum formae $Ak + r$, $Ak + r'$ $Ak + r''$ etc. erunt formae diuisorum ipsius $xx - A$, formae vero $Ak - n$, $Ak - n'$ etc. erunt formae non-diuisorum ipsius $xx - A$ (*i. e. numerus quicunque primus, praeter 2, erit diuisor aut non diuisor ipsius* $xx - A$ *prout in aliqua formarum priorum aut posteriorum continetur*). Si enim p est numerus primus positiuus atque alicuius ex numeris a, b, c etc. residuum vel non-residuum, hic ipse numerus ipsius p residuum vel non-residuum erit (theor. fund.). Quare si inter numeros a, b, c etc. sunt m, quorum non-residuum est p, totidem erunt non-residua ipsius p, adeoque si p in aliqua formarum priorum continetur, erit m par et ARp, si vero in aliqua posteriorum, erit m impar atque ANp.

Ex. Sit $A = +105, = -3 \times +5 \times -7$. Tum numeri r, r', r'', etc. erunt hi: 1, 4, 16, 46, 64, 79, (qui sunt non-residua nullius numerorum 3, 5, 7); 2, 8, 23, 32, 53, 92 (qui sunt non-residua numerorum 3, 5,; 26, 41, 59, 89, 101, 104 (qui sunt non residua numerorum 3, 7); 13, 52, 73, 82, 97, 103 (qui sunt non-residua numerorum 5, 7). — Numeri autem n, n', n'' etc. erunt hi: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68,

83. Seni primi sunt non-residua ipsius 3, seni posteriores non-residua ipsius 5, tum sequuntur non-residua ipsius 7, tandem ii qui sunt non-residua omnium trium simul.

Facile ex combinationum theoria atque artt. 32, 96 deducitur, numerorum r, r', r'' etc. multitudinem fore $= t\,(1 + \frac{l.\,l-1}{1.\,2} + \frac{l.\,l-1.\,l-2.\,l-3}{1.\,2.\quad 3.\quad 4} \ldots\ldots)$, numerorum n, n', n'' etc. multitudinem $= t\,(l + \frac{l.\,l-1.\,l-2}{1.\,2.\quad 3} + \frac{l.\,l-1.\ldots\,l-4}{1.\,2.\quad\ldots\quad 5} \ldots)$, vbi l designat multitudinem numerorum a, b, c etc.; $t = 2^{-l}(a-1)(b-1)(c-1)$ etc., et vtraque series continuanda donec abrumpatur. (Dabuntur scilicet t numeri, qui sunt residua omnium a, b, c etc. $\frac{t.\,l.\,l-1}{1.\,2.}$, qui sunt non-residua duorum etc. sed demonstrationem hanc fusius explicare breuitas non permittit). Vtriusque autem seriei summa *) est $= 2^{l-1}$. Scilicet posterior prodit ex hac $1 + (l-1) + \frac{l-1}{1.}\frac{l-2}{2}$ etc. iungendo terminum secundum et tertium, quartum et quintum etc. posterior vero ex eadem ungendo terminum primum atque secundum, tertium et quartum etc. Dabuntur

*) Neglecto factore t.

itaque tot formae diuisorum ipsius $xx - A$, quot dantur formae non-diuisorum, scilicet $\frac{1}{2}(a-1)(b-1)(c-1)$ etc.

149. *Casum secundum et tertium* hic simul contemplari possumus. Poterit scilicet A semper hic poni $= (-1)Q$, aut $= (+2)Q$ aut $= (-2)Q$, designante Q numerorum formae $+(4n+1)$, aut $-(4n+1)$, quales in art praec. consideramus. Sit generaliter $A = \alpha Q$. ita vt sit α aut $= -1$, aut $= \pm 2$. Tum erit A residuum omnium numerorum, quorum residuum est aut vterque α et Q, aut neuter; non-residuum autem omnium, quorum non residuum alteruter tantum numerorum α, Q. Hinc formae diuisorum ac non-diuisorum ipsius $xx - A$ facile deriuantur. Si $\alpha = -1$ distribuantur omnes numeri ipso $4A$ minores ad ipsumque primi in duas classes, in priorem ii, qui sunt in aliqua forma diuisorum ipsius $xx - Q$, simulque in forme $4n+1$, iique, qui sunt in aliqua forma non-diuisorum ipsius $xx - Q$ simulque in forma $4n+3$; in posteriorem reliqui. Sint priores r, r', r'' etc., posteriores n, n', n'' etc., eritque A residuum omnium numerorum primorum in aliqua formarum $4Ak+r$, $4Ak+r'$, $4Ak+r''$ etc. contentorum, non-residuum autem omnium primorum in aliqua formarum $4Ak+n$, $4Ak+n'$ etc. contentorum. — Si $\alpha = \pm 2$, distribuantur omnes numeri ipso $8Q$ minores ad ipsumque primi in duas classes, in primam ii, qui continentur in aliqua forma diuisorum ipsius $xx - Q$ simulque in aliquaformarum $8n+1$, $8n$

$+ 7$ pro signo superiori, vel formarum $8n + 1$, $8n + 3$ pro inferiori, iique qui contenti sunt in aliqua forma non-diuisorum ipsius $xx - Q$ simulque in aliqua harum $8n + 3$, $8n + 5$ pro signo superiori, vel harum $8n + 5$, $8n + 7$ pro inferiori, — in secundam reliqui. Tum designatis numeris classis prioris per r, r', r'' etc., numerisque classis posterioris per n, n', n'' etc. $\pm 2Q$ erit residuum omnium numerorum primorum in aliqua formarum $8Qk + r$, $8Qk + r'$, $8Qk + r''$ etc. contentorum, omnium autem primorum in aliqua formarum $8Qk + n$, $8Qk + n'$, $8Qk + n''$ etc. non-residuum. Ceterum facile demonstrari potest, etiam hic totidem formas diuisorum ipsius $xx - A$ datum iri ac non-diuisorum.

Ex. Hoc modo inuenitur $+ 10$ esse residuum omnium numerorum primorum in aliqua formarum $40k + 1$, 3, 9, 13, 27, 31, 37, 39, contentorum, non-residuum vero omnium primorum, qui sub aliqua formarum $40k + 7$, 11, 17, 19, 21, 23, 29, 33 continentur.

150. Formae hae plures habent proprietates satis memorabiles, quarum tamen vnam tantummodo apponimus. Si B est numerus compositus ad A primus, inter cuius factores primos occurrunt $2m$, qui in aliqua forma non-diuisorum ipsius $xx - A$ continentur, B in aliqua forma diuisorum ipsius $xx - A$ contentus erit; si vero multitudo factorum primorum ipsius B in aliqua forma non-diuisorum ipsius

$xx - A$ contentus erit. Demonstrationem quae non est difficilis omittimus. Hinc vero sequitur, non modo quemuis numerum primum sed etiam quemuis compositum imparem ad A primum, qui in aliqua forma non-diuisorum contineatur, non-diuisorem fore; necessario enim aliquis factor primus talis numeri debet esse non-diuisor.

151. Theorema fundamentale, quod sane inter elegantissima in hoc genere est referendum, in eadem forma simplici, in qua supra propositum est, a nemine hucusque fuit prolatum. Quod eo magis est mirandum, quum aliae quaedam propositiones illi superstruendae ex quibus ad illud facile reueniri potuisset, ill. Eulero iam innotuerint. Formas certas dari, in quibus omnes diuisores primi numerorum formae $xx - A$ contineantur, aliasque in quibus omnes non-diuisores primi numerorum eiusdem formae sint comprehensi, ita vt hae illas excludant, nouerat, methodumque illas formas inueniendi eruerat: sed omnes ipsius conatus ad demonstrationem perueniendi semper irriti fuerunt, veritatique illi per inductionem inuentae maiorem tantummodo verisimilitudinem conciliauerunt. In aliqua quidem tractatione, *Nouae demonstrationes circa diuisores numerorum formae* $xx + nyy$, quae in Acad. Petrop. recitata est 1775 Nou. 20, et post mortem viri summi in *T. I. Nou. Act.* huius Ac. p. 47 sqq. est conseruata, voti se compotem credidisse videtur: sed hic error irrepsit, scilicet p. 65. *tacite* supposuit, formas tales diuisorum

et non-diuisorum exstare *), vnde non difficile erat *quales* esse debeant deriuare: methodus autem qua vsus est ad comprobationem illius suppositionis haud idonea videtur. In alio schediasmate, *De criteriis aequationis* $fxx + gyy = hzz$ *vtrumque resolutionem admittat necne*, *Opusc. Anal. T. I.* (vbi f, g, h sunt dati, x, y, z indeterminati) per inductionem inuenit, si aequatio pro aliquo valore ipsius $h = s$ solubilis sit, eandem pro quouis alio valore ipsi s secundum mod. $4fg$ congruo, siquidem sit numerus primus, solubilem fore, ex qua propositione suppositio de qua diximus haud difficile demonstrari potest. Sed etiam huius theorematis demonstratio omnes ipsius labores elusit **), quod non est mirandum, quia nostro iudicio a theoremate fundamentali erat proficiscendum. Ceterum veritas huius propositionis ex iis quae in sect. sequenti docebimus sponte demanabit.

Post Eulerum, clar. Le Gendre eidem argumento operam nauauit, in egregia tract. *Re-*

*) Nempe dari numeros r, r', r'' etc. $< n$, n', n'' etc omnes diuersos et $< 4A$ tales vt omnes diuisores primi ipsius $xx - A$ sub aliqua formarum $4Ak + r$, $4Ak + r'$ etc. contineatur, omnesque non-diuisores primi sub aliqua harum $4Ak + n$, $4Ak + n'$ etc. (designante k numerum indeterminatum).

**) Vti ipse fatetur, l. c. p. 216 „Huius elegantissimi theorematis demonstratio adhuc desideratur, postquam a pluribus iamdudum frustra est inuestigata.... Quocirca plurimum is praestitisse censendus erit, cui successerit demonstrationem huius theorematis inuenire.“ — Quanto ardore vir immortalis demonstrationem huius theorematis aliorumque, quae tantummodo casus speciales theor. fundam. sunt, desiderauerit, videre licet ex multis aliis locis Opusc. Anali. Conf. *Additamentum ad diss. VIII, T. I.* et *diss. XIII, T. II.* pluresque diss. in Comment. Petrop., iam passim laudatae.

cherches d'analyse indeterminée, Hist. de l'Ac. des Sc. 1785 p. 465 *sqq.*, vbi peruenit ad theorema, quod si rem ipsam spectas cum th. fund. idem est, scilicet designantibus p, q duos numeros primos positiuos, fore residua absolute minima potestatum $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$ sec. mod. q, p resp. aut ambo $+1$, aut ambo -1, quando aut p aut q sit formae $4n+1$; quando vero tum p tum q sit formae $4n+3$, alterum res. min fore $+1$, alterum -1, p 516, ex quo sec. art. 106. deriuatur, *relationem* (in signif. art. 146 acceptam) ipsius p ad q ipsiusque q ad p *eandem* esse, quando aut p aut q sit formae $4n+1$, *oppositam*, quando tum p tum q sit formae $4n+3$. Propos. haec inter propp art. 131 est contenta, sequitur etiam ex 1, 3, 9, art 133; vicissim autem theor. fund. ex ipsa deriuari potest. Clar. Le Gendre etiam demonstrationem tentauit, de qua quum perquam ingeniosa sit in Sect. seq. fusius loquemur. Sed quoniam in ea plura sine demonstratione supposuit (vti ipse fatetur p. 520. *Nous avons supposé seulement* etc.), quae partim a nemine hucusque sunt demonstrata, partim nostro quidem iudicio sine theor. fund. ipso demonstrari nequeunt: via quam ingressus est, ad scopum deducere non posse videtur, nostraque demonstratio pro prima erit habenda. — Ceterum infra *duas alias demonstrationes* eiusdem grauissimi theorematis trademus, a praec. et inter se toto coelo diuersas.

152. Hactenus congruentiam puram $xx \equiv A \pmod{m}$ tractauimus, ipsiusque resolubilitatem dignoscere docuimus. *Radicum ipsarum*

inuestigatio per art. 105 ad eum casum est reducta, vbi m est aut primus aut primi potestas, posterior vero per art. 101 ad eum vbi m est primus. Pro hoc autem casu ea quae in art. 61 *sqq* tradidimus vna cum iis quae in sect. V et VIII docebimus, omnia fere complectuntur quae per mothodos directas erui possunt. Sed hae vbi sunt applicabiles plerumque infinities prolixiores sunt quam indirectae quas in sect. VI. docebimus, adeoque non tam propter vtilitatem suam in praxi quam propter pulcritudinem memorabiles. — *Congruentiae secundi gradus non purae* ad puras facile reduci possunt. Proposita congruentia $axx + bx + c \equiv o$ secundum mod. m soluenda, huic aequiualebit congruentia $4aaxx + 4abx + 4ac \equiv o$ (mod. $4am$), i. e. quiuis numerus alteri satisfaciens etiam alteri satisfaciet. Haec vero ita exhiberi potest $(2ax + b)^2 \equiv bb - 4ac$ (mod. $4am$), vnde omnes valores ipsius $2ax+b$ minores quam $4am$ si qui dantur inueniri possunt. Quibus per r, r', r'' etc. designatis, omnes solutiones congr. prop. deducentur ex solutionibus congruentiarum $2ax \equiv r - b$, $2ax \equiv r' - b$ etc (mod. $4am$) etc., quas in sect. II inuenire docuimus. Ceterum obseruamus, solutionem plerumque per varia artificia contrahi posse, ex gr. loco congr. prop. aliam inueniri posse $a'xx + 2b'x + c' \equiv o$, illi aequipollentem, et in qua a' ipsum m metiatur; haec vero de quibus Sect. vltima conferri potest, hic explicare breuitas non permittit.

SECTIO QVINTA

DE

FORMIS AEQVATIONIBVSQVE INDETERMINATIS

SECVNDI GRADVS.

153. In hac sectione imprimis de functionibus duarum indeterminatarum x, y, huius formae, $axx + 2bxy + cyy$, vbi a, b, c sunt integri dati tractabimus, quas *formas secundi gradus*, siue simpliciter *formas* dicemus. Huic disquisitioni superstruetur solutio problematis famosi, inuenire omnes solutiones aequationis cuiuscunque indeterminatae secundi gradus duas incognitas implicantis, siue hae incognitae valores integros siue rationales tantum nancisci debeant. Problema hoc quidem iam ab ill. La Grange in omni generalitate est solutum, multaque insuper ad naturam *formarum* pertinentia tum ab hoc ipso magno geometra, tum ab ill. Eulero partim primum inuenta, partim, a Fermatio olim inuenta, demonstrationibus munita. Sed nobis acriter formarum perquisitioni insistentibus tam multa noua se obtulerunt, vt totum argumen-

tum ab integro resumere operae pretium duxerimus, eo magis, quod Virorum illorum inuenta, multis locis sparsa, paucis innotuisse comperti sumus; porro quod methodus per quam haec tractabimus nobis ad maximam partem est propria; tandem quod nostra sine noua illorum expositione ne intelligi quidem possent. Nullum vero dubium nobis esse videtur, quin multa eaque egregia in hoc genere adhuc lateant in quibus alii vires suas exercere possint. Ceterum quae ad veritatum insignium historiam pertinent, loco suo semper trademus.

Formam $axx + 2bxy + cyy$, quando de indeterminatis x, y non agitur, ita designabimus, (a, b, c). Haec itaque expressio denotabit indefinite summam trium partium, producti numeri dati a in quadratum indeterminatae cuiuscunque; producti duplicati numeri b in hanc indeterminatam in aliam indeterminatam; producti numeri c in quadratum huius secundae indeterminatae. Ex. gr. $(1, 0, 2)$ exprimet summam quadrati et quadrati duplicati. Ceterum, quamuis formae (a, b, c) et (c, b, a) idem designent, si ad *partes ipsas* tantum respicimus, tamen different si insuper ad partium *ordinem* attendimus; quare sedulo eas in posterum distinguemus; quid vero inde lucremur in sequentibus sufficienter patebit.

154. Numerum aliquem datum per formam datam *repraesentari* dicemus, si formae indeterminatis tales valores integri tribuuntur,

vt ipsius valor numero dato fiat aequalis. Hic habebimus sequens

THEOREMA. *Si numerus M ita per formam* (a, b, c) *repraesentari potest, vt indeterminatarum valores, per quos hoc efficitur, inter se sint primi: erit* $bb - ac$ *residuum quadraticum numeri M.*

Dem. Sint valores indeterminatarum m, n, scilicet $amm + 2bmn + cnn = M$, accipianturque numeri μ, ν ita vt sit $\mu m + \nu n = 1$ (art. 40). Tum per euolutionem facile probatur esse, $(amm + 2bmn + cnn)(a\nu\nu - 2b\mu\nu + c\mu\mu) = (\mu(mb + nc) - \nu(ma + nb))^2 - (bb - ac)(m\mu + n\nu)^2$, siue $M(a\nu\nu - 2b\mu\nu + c\mu\mu) = (\mu(mb+nc) - \nu(ma + nb))^2 - (bb - ac)$. Quare erit $bb - ac \equiv (\mu(mb+nc) - \nu(ma + nb))^2 \pmod{M}$, *i. e.* $bb - ac$ residuum quadraticum ipsius M.

Numerum $bb - ac$, a cuius indole proprietates formae (a, b, c) imprimis pendere, in sequentibus docebimus, *determinantem* huius formae vocabimus.

155. Erit itaque $\mu(mb + nc) - \nu(ma+nb)$ valor expressioris $\sqrt{(bb - ac)} \pmod{M}$. Constat autem, numeros μ, ν infinitis modis ita determinari posse vt sit $\mu m + \nu n = 1$, vnde alii aliique valores illius expressionis prodibunt, qui quem nexum inter se habeant videamus. Sit non modo $\mu m + \nu n = 1$, sed etiam $\mu' m + \nu' n = 1$, ponaturque $\mu(mb + nc) - \nu(ma+nb) = v$, $\mu'(mb + nc) - \nu'(ma + nb) = v'$. Multiplicando aequationem $\mu m + \nu n = 1$ per μ', al-

teram $\mu' m + \nu' n = 1$ per μ, et subtrahendo fit $\mu' - \mu = n(\mu'\nu - \mu\nu')$ similiterque multiplicando illam per ν' hanc per ν fit subtrahendo $\nu' - \nu = m(\mu\nu' - \mu'\nu)$. Hinc statim prodit $v' - v = (\mu\nu' - \mu'\nu)(amm + 2bmn + cnn) = (\mu'\nu - \mu\nu')M$, siue $v' \equiv v \pmod{M}$. Quomodocunque igitur μ, ν determinentur, formula $\mu(mb + nc) - \nu(ma + nb)$ valores *diuersos* (i. e. incongruos) expressionis $\nu(bb - ac) \pmod{M}$ dare nequit. Si itaque v est valor quicunque illius formulae: repraesentationem numeri M per formam $axx + 2bxy + cyy$ eam vbi $x = m$, $y = n$, *pertinere* dicemus *ad valorem* v, *expressionis* $\sqrt{(bb - ac)} \pmod{M}$. Ceterum facile ostendi potest, si valor formulae illius aliquis sit v atque $v' \equiv v \pmod{M}$, loco numerorum μ, ν, qui dant v, alios μ', ν' accipi posse, qui dent v'. Scilicet faciendo $\mu' = \mu + \frac{n(v' - v)}{M}$, $\nu' = \nu - \frac{m(v' - v)}{M}$, fiet $\mu' m + \nu' n = \mu m + \nu n = 1$, valor autem formulae ex μ', ν' prodiens superabit valorem ex μ, ν prodeuntem quantitate $(\mu'\nu - \mu\nu')M$, quae fit $= (\mu m + \nu n)(v' - v) = v' - v$, siue valor ille erit $= v'$.

156 Si duae repraesentiones eiusdem numeri M per eandem formam (a, b, c) habentur, in quibus indeterminatae valores inter se primos habent: hae vel ad eundem valorem expr. $\sqrt{(bb - ac)} \pmod{M}$ pertinere possunt vel ad diuersos. Sit $M = amm + 2bmn + cnn = am'm' + 2bm'n' + cn'n'$, atque $\mu m + \nu n = 1$, $\mu m' + \nu' n' = 1$, patetque si fuerit

$\mu(mb+nc)-\nu(ma+nb) \equiv \mu'(m'b+n'c)-\nu'(m'a+n'b) \pmod{M}$, congruentiam semper manere, quicunque alii valores idonei pro $\mu, \nu; \mu', \nu'$ accipiantur, in quo casu vtramque repraesentationem ad *eundem* valorem expr. $\sqrt{(bb-ac)} \pmod{M}$ pertinere dicemus; si vero congruentia pro vllis valoribus ipsorum $\mu, \nu; \mu', \nu'$ locum non habet, pro nullis locum habebit, repraesentationesque ad valores *diuersos* pertinebunt. Si vero $\mu(mb+nc)-\nu(ma+nb) \equiv -(\mu'(m'b+n'c)-\nu'(m'a+n'b))$: repraesentationes ad valores *oppositos* expr. $\sqrt{(bb-ac)}$ pertinere dicentur. Omnibus hisce denominationibus etiam vtemur, quando de pluribus repraesentationibus eiusdem numeri per formas *diuersas*, sed quae eundem determinantem habent, agitur.

Ex. Sit forma proposita haec $(3, 7, -8)$ cuius determinans $= 73$. Per hanc formam habentur repraesentationes numeri 57 hae: $3.13^2+14.13.25-8.25^2$; $3.5^2+14.5.9-8.9^2$. Pro prima poni potest $\mu = 2, \nu = -1$, vnde prodit valor expr. $\sqrt{73} \pmod{57}$ ad quam repr. pertinet $= 2(13.7-25.8)+(13.3+25.7) = -4$. Simili modo repraesentatio secunda pertinere inuenitur, faciendo $\mu = 2, \nu = -1$, ad valorem $+4$. Quare ambae repraesentationes ad valores oppositos pertinent.

Antequam vlterius progredimur, obseruamus, formas quarum determinans $= 0$ ab inuestigationibus sequentibus prorsus exclusas esse, quippe quae theorematum concinnitatem tantummodo turbarent, adeoque tractationem peculiarem postulent.

157. Si forma, F, cuius indeterminatae sunt x, y in aliam F', cuius indeterminatae sunt x', y' per substitutiones tales $x = \alpha x' + \beta y'$, $x = \gamma x' + \delta y'$ transmutari potest, ita vt α, β, γ, δ sint integri: priorem *implicare* posteriorem, siue posteriorem *sub priori contentam esse* dicemus. Sit forma F haec $axx + 2bxy + cyy$, forma F' vero haec $a'x'x' + 2b'x'y' + c'y'y'$, habebunturque sequentes tres aequationes:

$$a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$$
$$b' = a\alpha\beta + b(\alpha\beta + \beta\gamma) + c\gamma\delta$$
$$c' = a\beta\beta + 2b\beta\delta + c\delta\delta.$$

Multiplicando aequationem secundam per se ipsam, primam per tertiam, et subtrahendo fit deletis partibus se destruentibus $b'b' - a'c' = (bb - ac)(\alpha\delta - \beta\gamma)^2$. Vnde sequitur determinantem formae F' per determinantem formae F diuisibilem et quotientem esse quadratum; manifesto igitur hi determinantes *eadem signa* habebunt. Quodsi itaque insuper forma F' per similem substitutionem in formam F transmutari potest, *i. e.* si tum F' sub F, tum F sub F' contenta est, formarum determinantes erunt aequales *) atque $(\alpha\delta - \beta\gamma)^2 = 1$. In hoc casu formas *aequiualentes* dicemus. Quare ad formarum aequiualentiam aequalitas determinantium est conditio necessaria, licet illa ex hac sola minime sequatur. —

*) Manifestum est ex analysi praecedente hanc propositionem etiam ad formas quarum determinans $= o$, patere. Sed aequatio $(\alpha\delta - \beta\gamma)^2 = 1$ ad hunc casum non est extendenda.

Substitutionem $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, vocabimus *transformationem propriam*, si $\alpha\delta - \beta\gamma$ est numerus positiuus, *impropriam*, si $\alpha\delta - \beta\gamma$ est negatiuus; formam F' *proprie* aut *improprie* sub forma F contentam esse dicemus, si F per transformationem propriam aut impropriam in formam F' transmutari potest. Si itaque formae F, F' sunt aequiualentes, erit $(\alpha\delta - \beta\gamma)^2 = 1$, adeoque si transformatio est propria, $\alpha\delta - \beta\gamma = +1$, si est impropria, $= -1$. — Si plures transformationes simul sunt propriae, aut simul impropriae, *similes* eas dicemus; propriam contra et impropriam *dissimiles*.

158. *Si formarum F, F' determinantes sunt aequales atque F' sub F contenta: etiam F sub F' contenta erit et quidem proprie vel improprie prout F' sub F proprie vel improprie continetur.* Transeat F in F' ponendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ transibitque F' in F ponendo $x' = \delta x - \beta y$, $y' = -\gamma x + \alpha y$. Patet enim per hanc substitutionem ex F' fieri idem, quod fiat ex F ponendo $x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y)$; $y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$ siue $x = (\alpha\delta - \beta\gamma)x$, $y = (\alpha\delta - \beta\gamma)y$. Hinc vero manifesto ex F fit $(\alpha\delta - \beta\gamma)^2 F$ *i. e.* rursus F (art. praec.). Perspicuum autem est, transformationem posteriorem esse propriam vel impropriam, prout prior sit propria vel impropria.

Si tum F' sub F, tum F sub F' *proprie* continetur, formas *proprie aequiualentes*, si illae sub inuicem improprie, vocabimus *improprie ae-*

quiualentes. — Ceterum vsus harum distinctionum mox innotescet.

Exempl. Forma $2xx - 8xy + 3yy$ per substitutiones $x = 2x' + y'$, $y = 3x + 2y'$ transit in formam $-13xx - 12xy - 2yy$, haec vero in illam factis $x' = 2x - y$, $y' = -3x + 2y$. Quare formae $(2, -4, 3)$, $(-13, -6, -2)$ erunt *proprie aequiualentes.*

Problemata quae tractare iam aggrediemur sunt haec: I. Propositis duabus formis quibuscunque eundem determinantem habentibus inuestigare vtrum sint aequiualentes necne, vtrum proprie aut improprie aut vtroque modo, nam etiam hoc fieri potest. Quando vero determinantes inaequales habent, annon saltem altera alteram implicet, proprie vel improprie vel vtroque modo. Denique inuenire omnes transformationes alterius in alteriam, tam proprias quam improprias. II. Proposita forma quacunque, inuenire vtrum numerus datus per eam repraesentari possit omnesque repraesentationes assignare. Sed quoniam formae determinantis negatiui hic aliam methodum requirunt quam formae determinantis positiui, primo trademus ea quae vtrisque sunt communia, tum vero formas cuiusuis generis seorsim considerabimus.

159. *Si forma F formam F' implicat, haec vero formam F'', forma F etiam formam F'' implicabit.*

Sint indeterminatae formarum F, F', F'' respectiue x, y; x', y'; x'', y'' transeatque F in F' ponendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; F' in F'' ponendo $x' = \alpha' x'' + \beta' y''$, $= \gamma' x'' + \delta' y''$ patetque, F in F'' transmutatum iri ponendo $x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'')$, $y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$, siue $x = (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y''$, $y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''$. Quare F ipsam F'' implicabit.

Quia $(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$, adeoque positiuus, si tum $\alpha\delta - \beta\gamma$ tum $\alpha'\delta' - \beta'\gamma'$ positiuus aut vterque negatiuus, negatiuus vero si alter horum numerorum positiuus alter negatiuus: forma F formam F'' *proprie* implicabit, si F ipsam F' et F' ipsam F'' eodem modo implicant, *improprie* si diuerso.

Hinc sequitur, si quotcunque formae habeantur F, F', F', F'' etc., quarum quaeuis sequentem implicet, primam implicaturam esse vltimam. et quidem *proprie*, si multitudo formarum, quae sequentem suam improprie implicant, fuerit par, improprie si multitudo haec impar.

Si forma F formae F' est aequiualens, formaque F' formae F'': forma F formae F'' aequiualens erit, et quidem proprie, si forma F formae F' eodem modo aequiualet vt forma F' formae F'', improprie, si diuerso.

Quia enim formae F, F', his F', F'', respectiue, sunt aequiualentes, tum illae has resp.

implicabunt, adeoque F ipsam F'', tum hae illas. Quare F, F'' aequiualentes erunt. Ex praec. vero sequitur, F ipsam F'' proprie vel improprie implicare, prout F ipsi F' et F' ipsi F'' eodem modo vel diuerso sint aequiualentes, vt et F'' ipsam F: quare in priori casu F, F'' proprie, in posteriori improprie aequiualentes erunt.

Formae $(a, -b, c)$, (c, b, a), $(c, -b, a)$ *formae* (a, b, c) *aequiualent, et quidem duae priores, improprie; vltima, proprie.*

Nam $axx + 2bxy + cyy$, transit in $ax'x' - 2bx'y' + cy'y'$, ponendo $x = x' + oy'$, $y = ox' + y'$, quae transformatio est impropria propter $1 \times -1 - o.\ o = -1$; in formam $cx'x' + 2bx'y' + ay'y'$ vero per transformationem impropriam $x = ox' + y'$, $y = x' + o.\ y$; et in formam $cx'x' - 2bx'y' + ay'y'$ per propriam $x = o.\ x - y'$, $y = x' + o.\ y'$.

Hinc manifestum est, quamuis formam, formae (a, b, c) aequiualentem, vel ipsi, vel formae $(a, -b, c)$ *proprie* aequiualere; similiterque, si qua forma formam (a, b, c) implicet aut sub ipsa contineatur, eam vel formam (a, b, c) vel formam $(a, -b, c)$ proprie implicare, aut sub alterutra proprie contineri. Formas (a, b, c), $(a, -b, c)$ *oppositas* vocabimus.

160. Si formae (a, b, c), (a', b', c') eundem determinantem habent, insuperque est $c = a'$ et $b \equiv -b'$ (mod. c), siue $b + b' \equiv o$

(mod. c). formas has *contiguas* dicemus, et quidem, quando determinatione accuratiori opus est, priorem posteriori *a parte prima*, posteriorem priori *a parte vltima* contiguam dicemus.

Ita ex. gr. forma (7, 3, 2), formae (3, 4, 7) a parte vltima contigua, forma (3, 1, 3) oppositae suae (3, — 1, 3) ab vtraque parte.

Formae contiguae semper sunt proprie aequiualentes. Nam forma $axx + 2bxy + cyy$ transit in formam contiguam $cx'x' + 2b'x'y' + c'y'y'$ per substitutionem $x = -y'$, $y = x' + \frac{b+b'}{c} y'$ (quae est propria ob $0 \times \frac{b+b'}{c} - 1 \times -1 = 1$), vti per euolutionem adiumento aequationis $bb - ac = b'b' - cc'$ facile probatur; $\frac{b+b'}{c}$ vero per hyp. est integer. — Ceterum hae difinitiones et conclusiones locum non habent, si $c = a' = 0$. Hic vero casus occurrere nequit, nisi in formis quarum determinans est numerus quadratus.

Formae (a, b, c), (a', b', c') proprie aequiualentes sunt, si $a \equiv a'$, $b \equiv b'$ (mod. a). Forma enim (a, b, c) formae $(c, -b, a)$ proprie aequiualet (art praec.), haec vero formae $(a' b', c')$ a parte prima contigua erit.

161. *Si forma (a, b, c) formam $(a' b', c')$ implicat, quiuis diuisor communis numerorum a, b, c etiam numeros a', b', c' metietur, et quiuis diuisor communis numerorum a, $2b$, c ipsos a', $2b'$, c'.*

Si enim forma $axx + 2bxy + cyy$ per substitutiones $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ in formam $a'x'x' + 2b'x'y' + c'y'y'$ transit: habebuntur hae aequationes:

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a'$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$a\beta\beta + 2b\beta\delta + c\delta\delta = c'$$

vnde propositio statim sequitur (pro parte secunda propos. loco aequationis secundae hanc adhibendo $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$).

Hinc sequitur maximum diuisorem communem numerorum a, b ($2b$), c simul metiri diuisorem communem maximum numerorum a', b' ($2b'$), c'. Quodsi igitur insuper forma (a', b', c') formam (a, b, c) implicat, i. e. formae sunt aequiualentes, diuisor communis maximus numerorum a, b ($2b$), c, diuisori communi maximo numerorum a', b' ($2b'$), c' aequalis erit, quoniam tum ille hunc metiri debet, tum hic illum. Si itaque, in hoc casu, a, b ($2b$), c diuisorem communem non habent, i. e. si maximus $= 1$, etiam a', b'($2b'$), c' diuisorem communem non habebunt.

162. Problema. *Si forma* $AXX + 2BXY + CYY \ldots F$, *formam* $axx + 2bxy + cyy \ldots f$, *implicat, atque transformatio aliqua illius in hanc est data: ex hac omnes reliquas transformationes ipsi similes deducere.*

Solutio. Sit transformatio data haec $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$, ponamusque primo

aliam huic similem datam esse $X = \alpha' x + \mathfrak{C}' y$, $Y = \gamma' x + \delta' y$, vt quid inde sequatur inuestigemus. Tum positis determinantibus formarum F, f, $= D$, d, atque $\alpha\delta - \mathfrak{C}\gamma = e$, $\alpha'\delta' - \mathfrak{C}'\gamma' = e'$, erit (art. 157), $d = Dee = De'e'$, et quum ex hyp. e, e' eadem signa habeant, $e = e'$, Habebuntur autem sequentes sex aequationes:

$$A\alpha\alpha + 2B\alpha\gamma + C\gamma\gamma = a. \quad [1]$$
$$A\alpha'\alpha' + 2B\alpha'\gamma' + C\gamma'\gamma' = a. \quad [2]$$
$$A\alpha\mathfrak{C} + B(\alpha\delta + \mathfrak{C}\gamma) + C\gamma\delta = b. \quad [3]$$
$$A\alpha'\mathfrak{C}' + B(\alpha'\delta' + \mathfrak{C}'\gamma') + C\gamma'\delta' = b. \quad [4]$$
$$A\mathfrak{C}\mathfrak{C} + 2B\mathfrak{C}\delta + C\delta\delta = c. \quad [5]$$
$$A\mathfrak{C}'\mathfrak{C}' + 2B\mathfrak{C}'\delta' + C\delta'\delta' = c. \quad [6]$$

Si breuitatis gratia numeros $A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'$, $A(\alpha\mathfrak{C}' + \mathfrak{C}\alpha') + B(\alpha\delta' + \mathfrak{C}\gamma' + \gamma\mathfrak{C}' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')$, $A\mathfrak{C}\mathfrak{C}' + B(\mathfrak{C}\delta' + \delta\mathfrak{C}') + C\delta\delta'$ per a', $2b'$, c' designamus, ex aequ. praecc. sequentes nouas deducemus*):

$$a'a' - D(\alpha\gamma' - \gamma\alpha')^2 = aa. \quad [7]$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \mathfrak{C}\gamma' - \gamma\mathfrak{C}' - \delta\alpha') = 2ab \quad [8]$$
$$4b'b' - D((\alpha\delta' + \mathfrak{C}\gamma' - \gamma\mathfrak{C}' - \delta\alpha')^2 + 2ee') = 2bb + 2ac,$$
vnde fit, addendo $2Dee' = 2d = 2bb - 2ac$,
$$4b'b' - (\alpha\delta' + \mathfrak{C}\gamma' - \gamma\mathfrak{C}' - \delta\alpha')^2 = 4bb. \quad [9]$$
$$a'c' - D(\alpha\delta' - \gamma\mathfrak{C}')(\mathfrak{C}\gamma' - \delta\alpha') = bb,$$

*) Origo harum aequationum haec est: 7 fit ex 1. 2 (i. e. si aequatio (1) in aequationem (2) multiplicatur, siue potius, si illius pars prior in partem priorem huius multiplicatur, illiusque pars posterior in posteriorem huius, productaque aequalia ponuntur); 8 ex 1. 4 + 2. 3; sequens quae non est numerata ex 1. 6 + 2. 5 + 3. 4 + 3. 4; sequens non numerata ex 3. 4; 11 ex 3. 6 + 4. 5; 12 ex 5. 6. Simili designatione etiam in sequentibus semper vtemur. Euolutionem vero lectoribus relinquere debemus.

vnde subtrahendo $D(\alpha\delta - \mathfrak{G}\gamma)(\alpha'\delta' - \mathfrak{G}'\gamma') = bb - ac$, fit

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\mathfrak{G}\delta' - \delta\mathfrak{G}') = ac. \quad [10]$$
$$2b'c' - D(\alpha\delta' + \mathfrak{G}\gamma' - \gamma\mathfrak{G}' - \delta\alpha')(\mathfrak{G}\delta' - \delta\mathfrak{G}') = 2bc \quad [11]$$
$$c'c' - D(\mathfrak{G}\delta' - \delta\mathfrak{G}')^2 = cc. \quad [12]$$

Ponamus iam, diuisorem communem maximum numerorum a, $2b$, c esse m numerosque $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ita determinatos vt fiat $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$ (art. 40); multiplicentur aequationes 7, 8, 9, 10, 11, 12 resp. per $\mathfrak{A}\mathfrak{A}$, $2\mathfrak{A}\mathfrak{B}$, $\mathfrak{B}\mathfrak{B}$, $2\mathfrak{A}\mathfrak{C}$, $2\mathfrak{B}\mathfrak{C}$, $\mathfrak{C}\mathfrak{C}$ summenturque producta. Quodsi iam breuitatis caussa ponimus

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T. \quad [13]$$
$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \mathfrak{G}\gamma' - \gamma\mathfrak{G}' - \delta\alpha') + \mathfrak{C}(\mathfrak{G}\delta' - \delta\mathfrak{G}') = U \quad [14]$$

vbi T, U manifesto erunt integri, prodibit:

$$TT - DUU = mm.$$

Deducti itaque sumus ad hanc conclusionem elegantem, *ex binis quibuscunque transformationibus similibus formae F in f sequi solutionem aequationis indeterminatae* $tt - Duu = mm$, *in integris*, scilicet $t = T$, $u = U$. Ceterum quum in ratiociniis nostris non supposuerimus, transformationes esse *diuersas*: *vna* adeo transformatio bis considerata solutionem praebere debet. Tum vero fit propter $\alpha' = \alpha$, $\mathfrak{G}' = \mathfrak{G}$ etc. $a' = a$, $b' = b$, $c' = c$, adeoque $T = m$, $U = o$, quae solutio per se est obuia.

Iam primam transformationem solutionemque aequationis indeterminatae tamquam cognitas consideremus, et quomodo hinc altera transformatio deduci possit, siue quomodo α', $\mathfrak{G}'$, γ', δ',

ab his $\alpha, \mathfrak{G}, \gamma, \delta$, T, U pendeant, inuestigemus. Ad hunc finem multiplicamus primo aequationem [1] per $\delta\alpha' - \mathfrak{G}\gamma'$, [2] per $\alpha\delta' - \gamma\mathfrak{G}'$, [3] per $\alpha\gamma' - \gamma\alpha'$, [4] per $\gamma\alpha' - \alpha\gamma'$, addimusque producta, vnde prodibit:

$$(e + e')\, a' = (\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')\, a \;\ldots\; [15]$$

Simili modo fit ex $(\delta\mathfrak{G}' - \mathfrak{G}\delta')([1] - [2]) + (\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')\,([3] + [4]) + (\alpha\gamma' - \gamma\alpha')\,([5] - [6])$:

$$2(e + e')\, b' = 2(\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')\, b \ldots [16]$$

Denique ex $(\delta\mathfrak{G}' - \mathfrak{G}\delta')\,([3] - [4]) + (\alpha\delta' - \gamma\mathfrak{G}')\,[5] + (\delta\alpha' - \mathfrak{G}\gamma')\,[6]$ prodit:

$$(e + e')\, c' = (\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')\, c \;\ldots\; [17]$$

Substituendo hos valores (15, 16, 17) in 13 fit:

$$(e + e')\, T = (\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')\,(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c), \text{ siue } 2eT = (\alpha\delta' - \mathfrak{G}\gamma' - \gamma\mathfrak{G}' + \delta\alpha')m \;\ldots\; [18]$$

vnde T multo facilius deduci potest, quam ex [13]. — Combinando hanc aequationem cum 15, 16, 17 obtinetur $ma' = Ta$, $2mb' = 2Tb$, $mc' = Tc$. Quos valores ipsorum $a', 2b', c'$ in aequ. 7—12 substituendo et loco ipsius TT scribendo $mm + DUU$, transeunt illae post mutationes debitas in has:

$$(\alpha\gamma' - \gamma\alpha')^2 mm = aaUU$$
$$(\alpha\gamma' - \gamma\alpha')\,(\alpha\delta' + \mathfrak{G}\gamma' - \gamma\mathfrak{G}' - \delta\alpha')mm = 2abUU$$
$$(\alpha\delta' + \mathfrak{G}\gamma' - \gamma\mathfrak{G}' - \delta\alpha')^2 mm = 4bbUU$$
$$(\alpha\gamma' - \gamma\alpha')\,(\mathfrak{G}\delta' - \delta\mathfrak{G}')mm = acUU$$
$$(\alpha\delta' + \mathfrak{G}\gamma' - \gamma\mathfrak{G}' - \delta\alpha')\,(\mathfrak{G}\delta' - \delta\mathfrak{G}')mm = 2bcUU$$
$$(\mathfrak{G}\delta' - \delta\mathfrak{G}')^2 mm = ccUU$$

Hinc adiumento aequationis [14] et huius $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, facile deducitur (multiplicando primam, secundam, quartam; secundam, tertiam, quintam; quartam, quintam, sextam, resp. per $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ addendoque producta): $(\alpha\gamma' - \gamma\alpha')Umm = maUU$, $(\alpha\delta' + \epsilon\gamma' - \gamma\epsilon' - \delta\alpha')Umm = 2mbUU$, $(\epsilon\delta' - \delta\epsilon')Umm = mcUU$ atque hinc, diuidendo per mU*), $aU = (\alpha\gamma' - \gamma\alpha')m$... [19]; $2bU = (\alpha\delta' + \epsilon\gamma' - \gamma\epsilon' - \delta\alpha')m$ ...[20]; $cU = (\epsilon\delta' - \delta\epsilon')m$... [21], ex quarum aequationum aliqua U multo facilius quam ex [14] deduci potest. — Simul hinc colligitur, quomodocunque $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ determinentur (quod infinitis modis diuersis fieri potest), tum T tum U eundem valorem adipisci.

Iam si aequatio 18 multiplicatur per α, 19 per 2ϵ, 20 per $-\alpha$, fit per additionem $2\alpha eT + 2(\epsilon a - \alpha b)U = 2(\alpha\delta - \epsilon\gamma)\alpha' m = 2e\alpha' m$.

Simili modo fit ex ϵ[18] + ϵ[20] − 2α[21], $2\epsilon eT + 2(\epsilon b - \alpha c)U = 2(\alpha\delta - \epsilon\gamma)\epsilon' m = 2e\epsilon' m$.

Porro ex γ[18] + 2δ[19] − γ[20] fit $2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \epsilon\gamma)\gamma' m = 2e\gamma' m$.

Tandem ex δ[18] + δ[20] − 2γ[21] prodit $2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \epsilon\gamma)\delta' m = 2e\delta m$.

*) Hoc non liceret, si esset $U = 0$: tunc vero aequationum 19, 20, 21 veritas statim ex prima, tertia et sexta praecedentium sequeretur.

In quibus formulis, si pro a, b, c valores ex 1, 3, 5 substituuntur, fit

$$\alpha' m = \alpha T - (\alpha B + \gamma C) U$$
$$\mathfrak{C}' m = \mathfrak{C} T - (\mathfrak{C} B + \delta C) U$$
$$\gamma' m = \gamma T + (\alpha A + \gamma B) U$$
$$\delta' m = \delta T + (\mathfrak{C} A + \delta B) U$$

Ex analysi praec. sequitur, nullam transformationem formae F in f propositae similem dari, quae non sit contenta sub formula $X = \frac{1}{m}(\alpha t - (\alpha B + \gamma C) u) x + \frac{1}{m}(\mathfrak{C} t - (\mathfrak{C} B + \delta C) u) y$, $Y = \frac{1}{m}(\gamma t + (\alpha A + \gamma B) u) x + \frac{1}{m}(\delta t + (\mathfrak{C} A + \delta B) u) x) \ldots$ (I), designantibus t, u indefinite omnes numeros integros aequationi $tt - Duu = mm$ satisfacientes. Hinc vero concludere nondum possumus, omnes valores ipsorum t, u, aequationi illi satisfacientes, in formula (I) substitutos, transformationes idoneas praebere. At

1. Formam F per substitutionem, e quibusuis ipsorum t, u valoribus ortam, semper in formam f transmutari, per euolutionem confirmari facile potest adiumento aequationem 1, 3, 5 et huius $tt - Duu = mm$. Calculum prolixiorem quam difficiliorem breuitatis gratia supprimimus.

2. Quaeuis transformatio ex formula deducta propositae erit similis. Namque $\frac{1}{m}(\alpha t - (\alpha B + \gamma C) u) \times \frac{1}{m}(\delta t + (\mathfrak{C} A + \delta B) u) - \frac{1}{m}(\mathfrak{C} t - (\mathfrak{C} B + \delta C) u) \times \frac{1}{m}(\gamma t + (\alpha A + \gamma B) u) = \frac{1}{mm}(\alpha\delta - \mathfrak{C}\gamma)(tt - Duu) = \alpha\delta - \mathfrak{C}\gamma$.

3. Si formae F, f determinantes inaequales habent, fieri potest, vt formula (I) pro quibusdam valoribus ipsorum t, u praebeat substitutiones, quae *fractiones* implicent, adeoque reiici debeant, Omnes vero reliquae erunt transformationes idoneae, aliaeque praeter ipsas non dabuntur.

4. Si vero formae F, f eundem determinantem habent adeoque sunt *aequiualentes*, formula (I) nullas transformationes quae fractiones implicent praebebit, adeoque in hoc casu solutionem completam problematis exhibebit. Illud vero ita demonstramus.

Ex theoremate art. praec. sequitur in hocce casu, m simul fore diuisorem communem numerorum A, $2B$, C. Quoniam $tt - Duu = mm$, fit $tt - BBuu = mm - ACuu$, quare $tt - BBuu$ per mm diuisibilis erit: hinc etiam a potiori $4tt - 4BBuu$ adeoque (quia $2B$ per m diuisibilis) etiam $4tt$ per mm et proin $2t$ per m. Hinc $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ erunt integri, et quidem, quoniam differentia inter ipsos, $\frac{4}{m}Bu$ est par), aut vterque par, aut vterque impar. Si vterque impar esset, etiam productum impar foret, quod tamquam quadruplum numeri $\frac{1}{mm}(tt - BBuu)$, quem integrum esse modo ostendimus, necessario par: quare hic casus est impossibilis, adeoque $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$ semper pares, vnde $\frac{1}{m}(t + Bu)$, $\frac{1}{m}(t - Bu)$ erunt integri. Hinc vero nullo negotio deducitur, omnes quatuor coefficientes in (I) semper esse integros. *Q. E. D.*

Ex praecedentibus colligitur, si omnes solutiones aequationis $tt - Duu = mm$ habeantur, omnes transformationes formae (A, B, C) in (a, b, c) transf. datae similes inde deriuari. Illas vero in sequentibus inuenire docebimus. Hic tantummodo obseruamus multitudinem solutionum semper esse finitam quando D sit negatiuus, aut positiuus simulque quadratus: quando vero D positiuus non quadratus, infinitam. Quando hic casus locum habet, simulque D non $= d$ (supra 3°), disquiri insuper deberet, quomodo ii valores ipsorum t, u, qui substitutiones a fractionibus liberas, ab iis, qui fractas producunt, a priori dignosci possint. Sed pro hocce casu infra aliam methodum ab hoc incommodo liberam exponemus (art. 214).

Ex. Forma $xx + 2yy$ per substitutionem propriam $x = 2x' + 7y'$, $y = x' + 5y'$ transit in formam (6, 24, 99): desiderantur *omnes* transformationes propriae formae illius in hanc. Hic $D = -2$, $m = 3$, adeoque aequatio soluenda haec: $tt + 2uu = 9$. Huic sex modis diuersis satisfit ponendo scilicet $t = 3, -3, 1, -1, 1, -1$; $u = 0, 0, 2, 2, -2, -2$, resp. Solutio tertia et sexta dant substitutiones in fractis, adeoque sunt reiiciendae; ex reliquis sequuntur quatuor substitutiones:

$$x = \begin{cases} 2x' + 7y' \\ -2x' + 7y' \\ 2x' + 9y' \\ -2x' + 9y' \end{cases} \quad y = \begin{cases} x' + 5y' \\ -x' + 5y' \\ x' + 3y' \\ -x' + 3y' \end{cases}$$

(quarum prima est proposita).

163. Iam supra obiter diximus fieri posse vt forma aliqua, F, aliam, F', tam proprie quam improprie implicet. Perspicuum est hoc euenire, si inter formas F, F' alia G interponi possit, ita vt F ipsam G, G ipsam F' implicet, formaque G ita sit comparata, vt sibi ipsa sit improprie aequiualens. Si enim F ipsam G proprie vel improprie implicare supponitur: quum G ipsam G improprie implicet, F ipsam G improprie vel proprie (resp.) implicabit, adeoque, in vtroque casu, tam proprie quam improprie. (art. 159). Eodem modo hinc deducitur, quomodocunque G ipsam F' implicare supponatur, F semper ipsam F' tum proprie tum improprie implicare debere. — Tales vero formas dari, quae sibi ipsae sint improprie aequiualentes, videtur in casu maxime obuio, vbi formae terminus medius $= 0$. Talis enim forma sibi ipsa erit opposita (art. 159) adeoque improprie aequiualens. Generalius quaeuis forma, (a, b, c), hac proprietate est praedita, in qua $2b$ per a est diuisibilis. Huic enim forma (c, b, a) a parte prima erit contigua (art. 160) adeoque proprie aequiualens: sed (c, b, a) per art. 159 formae (a, b, c') improprie aequiualet: quare (a, b, c) sibi ipsa improprie aequiualebit. Tales formas (a, b, c) in quibus $2b$ per a est diuisibilis, *ancipites* vocabimus. Habebimus itaque theorema hoc:

Forma F, aliam formam F' tum proprie tum improprie implicabit, si forma anceps inuenire potest sub F contenta ipsam F vero implicans. Sed haec propositio etiam conuerti potest: scilicet

164. THEOREMA. *Si forma* $Axx + 2Bxy + Cyy \ldots (F)$ *formam* $A'x'x' + 2B'x'y' + C'x'y' \ldots (F')$ *tum proprie tum improprie implicat: forma anceps inueniri potest, sub F contenta formamque F' implicans.*

Ponamus, formam F transire in formam F' tum per substitionem $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, tum per hanc illi dissimilem, $x = \alpha' x' + \beta' x'$, $y = \gamma' x' + \delta' y'$. Tum designatis numeris $\alpha\delta - \beta\gamma$, $\alpha'\delta' - \beta'\gamma'$ per e, e', erit $B'B' - A'C' = ee(BB - AC) = e'e'(BB - AC)$; hinc $ee = e'e'$, et, quia per hyp. e, e' signa opposita habent, $e = -e'$ siue $e + e' = 0$. Iam patet si in F' pro x' substituatur $\delta' x'' - \beta' y''$, et pro y', $-\gamma' x'' + \alpha' y''$, eandem formam esse prodituram ac si in F scribatur *aut* 1) pro x, $\alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'')$ i. e. $(\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y''$, et pro y, $\gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'')$ i. e. $(\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y''$; *aut* 2) pro x, $\alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'')$ i. e. $e'x''$, et pro y, $\gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'')$ i. e. $e'y''$. Designatis itaque numeris $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$ $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$ per a, b, c, d: forma F per duas substitutiones $x = ax'' + by''$, $y = cx'' + dy''$; $x = e'x''$, $y = e'y''$ in eandem formam transmutabitur, vnde obtinemus tres aequationes sequentes:

$$Aaa + 2Bac + Ccc = Ae'e' \ldots\ldots\ldots [1]$$
$$Aab + B(ad + bc) + Ccd = Be'e' \ldots\ldots [2]$$
$$Abb + 2Bbd + Cdd = Ce'e' \ldots\ldots\ldots [3]$$

Ex valoribus ipsorum a, b, c, d autem inuenitur

$$ad - bc = ee' = -ee = -e'e' \ldots\ldots [4]$$

Hinc fit ex $d[1] - c[2]$, $(Aa + Bc)(ad - bc) = (Ad - Bc)e'e'$, adeoque $A(a + d) = 0$. Porro ex $(a + d)[2] - b[1] - c[3]$ fit $(Ab + B(a + d) + Cc)(ad + bc) = (-Ab + B(a+d) - Cc)e'e'$, adeoque $B(a + d) = 0$. Denique ex $a[3] - b[2]$ fit $(Bb + Cd)(ad - bc) = (-Bb + Ca)e'e'$ adeoque $C(a + d) = 0$. Quare quum omnes A, B, C nequeant esse $= 0$, necessario erit $a + d = 0$ siue $a = -d$.

Ex $a[2] - b[1]$ fit $(Ba + Cc)(ad - bc) = (Ba - Ab)e'e'$, vnde $Ab - 2Ba - Cc = 0$ [5]

Ex aequationibus $e + e' = 0$, $a + d = 0$ siue $\alpha\gamma - \gamma\gamma + \alpha'\delta' - \gamma'\gamma' = 0$, $\alpha\delta' - \gamma\gamma' - \gamma\gamma' + \delta\alpha' = 0$ sequitur $(\alpha + \alpha')(\gamma + \gamma') = (\gamma + \gamma')(\gamma + \gamma')$ siue $(\alpha + \alpha') : (\gamma + \gamma') = (\gamma + \gamma') : (\delta + \delta')$. Sit rationi huic *) in numeris minimis aequalis ratio $m : n$, ita vt m, n inter se primi sint, accipianturque μ, ν ita vt fiat $\mu m + \nu n = 1$. Porro sit r diu. comm. max. numerorum a, b, c; cuius quadratum propterea metietur ipsum $aa + bc$ siue $bc - ad$ siue ee; quare r etiam ipsum e metietur. His ita factis, si forma F per substitutionem $= mt + \frac{\nu e}{r} u$, $y = nt - \frac{\mu e}{r} u$ in formam $Mtt + 2Ntu + Puu$ (G) transire supponitur, haec anceps erit formamque F' implicabit.

*) Si omnes $\alpha + \alpha'$, $\gamma + \gamma'$, $\gamma + \gamma'$, $\delta + \delta'$ essent $= 0$, ratio indeterminata foret, adeoque methodus non applicabilis. Sed exigua attentio docet, hoc cum suppositionibus nostris consistere non posse. Foret enim $\alpha\delta - \gamma\gamma = \alpha'\delta' - \gamma'\gamma'$ i. e. $e = e'$ adeoque, quia $e = -e'$, $e = e' = 0$. Hinc vero etiam $B'B' - A'C'$ i. e. determinans formae F' fieret $= 0$, quales formas omnino exclusimus.

Dem. I. Quo pateat, formam G esse ancipitem, ostendemus esse $M(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu}) = 2N_r$ vnde quia r ipsos a, b, c metitur, $\frac{1}{r}(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu})$ integer erit, adeoque $2N$ multiplum ipsius M. Erit autem $M = Amm + 2Bmn + Cnn$, $N_r = (Am_\nu - B(m_\mu - n_\nu) - Cn_\mu)e$. Porro per euolutionem facile confirmatur esse $2e + 2a = e - e' + a - d = (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma')$, $2b = (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta')$ Hinc quoniam $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$, erit $m(2e + 2a) = -2nb$ siue $me + ma + nb = 0$ . . . [7]. Eodem modo erit $2e - 2a = e - e' - a + d = (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma')$, $2c = (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta')$, atque hinc $n(2e - 2a) = -2mc$, siue $ne - na + mc = 0$. . [8]

Iam si ad $mm(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu})$ additur $(1 - m_\mu - n_\nu)(m_\nu(e - a) + (m_\mu + 1)b)$ $+ (me + ma + nb)(m_{\mu\nu} + \nu) + (ne - na + mc)m_{\nu\nu}$ quod manifesto $= 0$, propter $1 - \mu m - \nu u = 0$, $me + ma + nb = 0$, $ne - na + mc = 0$: prodit productis rite euolutis partibusque se destruentibus deletis, $2m_\nu e + b$. Quare erit $mm(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu}) = 2m_\nu e + b$. . . . . [9]

Eodem modo addendo ad $mn(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu})$ haec:

$(1 - m_\mu - n_\nu)((n_\nu - m_\mu)e - (1 + m_\mu + n_\nu)a)$ $- (me + ma + nb)m_{\mu\mu} + (ne - na + mc)n_\nu$

inuenitur

$mn(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu}) = (n_\nu - m_\mu)e - a$. . . [10]

Denique addendo ad $nn(b_{\mu\mu} - 2a_{\mu\nu} - c_{\nu\nu})$ haec: $(m_\mu + n_\nu - 1)(n_\mu(e + a) + (n_\nu + 1)c)$

$-(me + ma + nb)\,n\mu\mu - (ne - na + mc)\,(n\mu\nu + \mu)$

fit

$nn(b\mu\mu - 2a\mu\nu - c\nu\nu) = -2n\mu e - c. \ldots . [11]$

Iam ex 9, 10, 11, deducitur

$(Amm + 2Bmn + Cnn)\,(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2e\,(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc$, siue propter [6],

$M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr.$ *Q. E. D.*

II. Vt probetur, formam G implicare formam F' demonstrabimus, *primo* G transire in F' ponendo $t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'$, $u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y' \ldots (S)$; *secundo* $\frac{r}{e}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ esse integros.

1. Quoniam F transit in G ponendo $x = mt + \frac{\nu e}{r}u$, $y = nt - \frac{\mu e}{r}u$: forma G per substitutionem (S) transmutabitur in eandem formam in quam F transformatur ponendo $x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') + \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$ i. e. $= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y'$ siue $= \alpha x' + \beta y'$; et $y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$ i. e. $= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y'$ siue $= \gamma x' + \delta y'$. Per hanc vero substitutionem F transit in F': quare per substitutionem (S) etiam G transibit in F'.

2. Ex valoribus ipsorum e, b, d inuenitur $\alpha'e + \gamma b - \alpha d = 0$, siue propter $d = -a$, $n\alpha'e + n\alpha a + n\gamma b = 0$; hinc ex [8], $n\alpha'e + n\alpha a = m\gamma e + m\gamma a$ siue $(n\alpha - m\gamma)a = (m\gamma - n\alpha')e$ [12]

Porro fit $\alpha nb = -\alpha m(e + a)$, $\gamma nb = -m(\alpha' e + \alpha a)$ adeoque $(n\alpha - m\gamma)b = (\alpha' - \alpha)me$ [13]

Denique fit $\gamma' e - \gamma a + \alpha c = 0$: hinc multiplicando per n, et pro na substituendo valorem ex [8] fit $(n\alpha - m\gamma)c = (\gamma - \gamma', ne$. . . [14]

Simili modo eruitur $\epsilon' e + \delta b - \epsilon d = 0$, siue $n\epsilon' e + n\delta b + n\epsilon a = 0$, adeoque per [7] $n\epsilon' e + n\epsilon a = m\delta e + m\delta a$, siue $(n\epsilon - m\delta)a = (m\delta - n\epsilon')e$ [15]

Porro fit $\epsilon nb = -\epsilon m(e + a)$, $\delta mb = -m(\epsilon e' + \epsilon a)$ adeoque $(n\epsilon - m\delta)b = (\epsilon' - \epsilon)me$ [16]

Tandem $\delta' e - \delta a + \epsilon c = 0$: hinc multiplicando per n et substituendo pro na valorem ex [8] fit $(n\epsilon - m\delta)c = (\delta - \delta')ne$ . . . . . [17]

Iam quum diuisor communis maximus numerorum a, b, c sit r, integri $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ ita accipi possunt vt fiat $\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$. Quo facto erit ex 12, 13, 14; 15, 16, 17

$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \frac{r}{e}(n\alpha - m\gamma)$
$\mathfrak{A}(m\delta - n\epsilon') + \mathfrak{B}(\epsilon' - \epsilon)m + \mathfrak{C}(\delta - \delta')n = \frac{r}{e}(n\epsilon - m\delta)$
adeoque $\frac{r}{e}(n\alpha - n\gamma)$, $\frac{r}{e}(n\epsilon - m\delta)$ integri. *Q. E. D.*

165. *Ex.* Forma $3xx + 14xy - 4yy$ in formam $-12x'x' - 18x'y' + 39y'y'$ transmutatur, tum proprie, ponendo $x = 4x' + 11y'$, $y = -x' - 2y$, tum improprie, ponendo $x = -74x' + 89y'$, $y = 15x' - 18y'$. Hic igitur $\alpha + \alpha'$, $\epsilon + \epsilon'$, $\gamma + \gamma'$, $\delta + \delta'$ sunt -70, 100, 14, -20; est autem $-70 : 14 = 100 : -20 = 5 : -1$. Faciemus itaque $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Numeri autem a, b, c inueniun-

tur $= 237$, $= 1170$, 48, quorum diuisor communis maximus $= 3 = r$; denique fit $e = 3$. Hinc transformatio (S) haec erit: $x = 5t - u$, $y = -t$. Per quam forma $(3, 7, -4)$ transit in formam ancipitem $tt - 16tu + 3uu$.

Si formae F, F' sunt aequiualentes: forma G, sub F contenta, etiam sub F' contenta erit. Sed quoniam eanden formam etiam implicat, ipsi aequiualens erit, et proin etiam formae F. In hoc igitur casu theorema ita enunciabitur:

Si F, F' tam proprie, quam improprie sunt aequiualentes: forma anceps vtrique aequiualens inueniri poterit. — Ceterum in hoc casu $e = \pm 1$, adeoque etiam r, ipsum e metiens, $= 1$ erit.

Haec de formarum transformatione in genere sufficiant: transimus itaque ad considerationem *repraesentationum.*

166. *Si forma F formam F' implicat: quicunque numerus per F' repraesentari potest etiam per F poterit.*

Sint indeterminatae formarum F, F' respectiue x, y; x', y', ponamusque numerum M per F' repraesentari faciendo $x' = m$, $y' = n$, formam F vero in F' transire per substitutionem $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Tum manifestum est si ponatur $x = \alpha m + \beta n$, $y = \gamma m + \delta n$, F transire in M.

Si M pluribus modis per formam F' repraesentari potest, e. g. etiam faciendo $x' = m'$,

$y' = n'$: plures repraesentationes ipsius M per F inde sequentur. Si enim esset tum $\alpha m + \gamma n = \alpha m' + \gamma n'$ tum $\beta m + \delta n = \beta m' + \delta n'$, foret aut $\alpha\delta - \beta\gamma = 0$, adeoque etiam determinans formae $F' = 0$ contra hyp., aut $m = m'$, $n = n'$. Hinc sequitur M ad minimum totidem modis diuersis per F repraesentari posse quot per F'.

Si igitur tum F ipsam F', tum F' ipsam F implicat i. e. si F, F' sunt aequiualentes, numerusque M per alterutram repraesentari potest: etiam per alteram repraesentari poterit, et quidem totidem modis diuersis per alteram, quot per alteram.

Denique obseruamus, in hocce casu diuisorem communem maximum numerorum m, n aequalem esse diuisori comm. max. nnmerorum $\alpha m + \gamma n$, $\beta m + \delta n$. Sit ille $= \Delta$, nnmerique μ, ν ita accepti vt fiat $\mu m + \nu n = \Delta$. Tum erit $(\delta\mu - \beta\nu)(\alpha m + \gamma n) - (\gamma\mu - \alpha\nu)(\beta m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm \Delta$. Hinc diu. comm. max. numerorum $\alpha m + \gamma n$, $\beta m + \delta n$ metietur ipsum Δ, Δ vero etiam illum metietur, quia manifesto ipsos $\alpha m + \gamma n$, $\beta m + \delta n$ metitur. Quare necessario ille erit $= \Delta$. — Quando igitur m, n inter se primi sunt, etiam $\alpha m + \gamma n$, $\beta m + \delta n$ inter se primi erunt.

167. Theorema. *Si formae* $axx + 2bxy + cyy \ldots (F)$, $a'x'x' + 2b'x'y' + c'y'y' \ldots (F')$ *sunt aequiualentes, ipsarum determinans* $= D$, *posteriorque in priorem transit ponendo* $x' = \alpha x + \gamma y$, $y' = \beta x + \delta y$;

porro numerus M per F repraesentatur, faciendo $x = m$, $y = n$, *adeoque per F' faciendo* $x' = \alpha m + \gamma n = m'$, $y' = \beta m + \delta n = n'$ *et quidem ita vt m ad n eoque ipso etiam m' ad n' sit primus: ambae repraesentationes aut ad eundem valorem expressionis* $\sqrt{D}$ *(mod. M) pertinebunt, aut ad oppositos, prout transformatio formae F' in F propria est vel impropria.*

Dem. Determinentur numeri μ, ν ita vt fiat $\mu m + \nu n = 1$, ponaturque $\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu'$, $\frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$ (qui erunt integri propter $\alpha\delta - \beta\gamma = \pm 1$). Tum erit $\mu m' + \nu' n' = 1$. (Cf. art. praec. fin.). Porro sit $\mu(bm + cn) - \nu(am + bn) = V$, $\mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$, eruntque V, V' valores expr. $\sqrt{M}$ (mod. D) ad quos repraesentatio prima et secunda pertinent. Si in V' pro μ, ν, m, n valores ipsorum substituuntur; in V vero pro a, $a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma$ pro b, $a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$; pro c, $a'\beta\beta + 2b'\beta\delta + c'\delta\delta$: inuenietur euolutione facta $V = V'(\alpha\delta - \beta\gamma)$. Quare erit aut $V = V'$, aut $V = -V'$, prout $\alpha\delta - \beta\gamma = +1$ aut $= -1$, i. e. repraesentationes pertinebunt ad eundem valorem expr. $\sqrt{M}$ (mod. D) vel ad oppositos, prout transformatio formae F' in F est propria vel impropria. *Q. E. D.*

Si itaque plures repraesentationes numeri M per formam (a, b, c), ope valorum inter se primorum indeterminatarum x, y, habentur ad valores *diuersos* expr. $\sqrt{D}$ (mod. M) pertinentes: repraesentationes respondentes per formam (a', b', c') ad eosdem resp., valores pertinebunt, et si nulla repraesentatio numeri M per

formam aliquam ad valorem quendam determinatum pertinens datur, nulla quoque dabitur ad hunc valorem pertinens per formam illi aequiualentem.

168. Theorema. *Si numerus M per formam $axx + 2bxy + cyy$ repraesentatur tribuendo ipsis x, y valores inter se primos m, n, valorque expressionis $\sqrt{D}$ (mod. M), ad quem haec repraesentatio pertinet, est N: formae (a, b, c), $\left(M, N, \frac{NN-D}{M}\right)$ proprie aequiualentes erunt.*

Demonstr. Ex art. 155 patet, numeros integros μ, ν inueniri posse ita vt sit $m\mu + n\nu = 1$, $\mu(bm + cn) - \nu(am + bn) = N$. Quo facto forma (a, b, c) per substitutionem $x = mx' - \nu y'$, $y = nx' + \mu y'$, quae manifesto est propria, transit in formam cuius determinans $= D(m\mu + n\nu)^2$ i. e. $= D$, siue in formam aequiualentem: quae forma si ponitur $= \left(M', N', \frac{N'N'-D}{M'}\right)$, erit $M' = amm + 2bmn + cnn = M$; $N' = -ma + (m\mu - n\nu)b + nc = N$. Quare forma in quam (a, b, c) per transformationem illam mutatur erit $\left(M, N, \frac{NN-D}{M}\right)$. *Q. E. D.*

Ceterum ex aequationibus $m + n\nu = 1$, $\mu(mb + nc) - \nu(ma + nb) = N$ deducitur $\mu = \frac{nN + ma + nb}{amm + 2bmn + cnn} = \frac{nN + ma + nb}{M}$; $\nu = \frac{mb + nc - mN}{M}$, qui numeri itaque erunt integri.

Porro obseruandum, hanc propositionem locum non habere, si $M = 0$; tum enim terminus $\frac{NN - D}{M}$ fit *indeterminatus* *).

169. Si plures repraesentationes numeri M, per (a, b, c) habentur, ad eundem valorem expr. $\sqrt{D}$ (mod. M), N, pertinentes (vbi valores ipsorum x, y semper inter se primos supponimus): plures etiam transformationes propriae formae (a, b, c), (F), in $(M, N, \frac{NN - D}{M})$, (G) inde deducentur. Scilicet si etiam per hos valores $x = m'$, $y = n'$ talis repraesentatio prouenit, (F) etiam per substitutionem $x = m'x' + \frac{m'N - n'b - n'c}{M} y'$, $y = n'x' + \frac{n'N + m'a + m'b}{M} y'$ in (G) transit. Vice versa, ex quauis transformatione propria formae (F) in (G) sequetur repraesentatio numeri M per formam (F), ad valorem N pertinens. Scilicet si (F) transit in (G) positis $x = mx' - \nu y'$, $y = nx' + \nu y'$, M repraesentatur per (F) ponendo $x = m$, $y = n$, et quoniam hic $m\mu + n\nu = 1$, valor expr. $\sqrt{D}$ (mod. M) ad quem repraesentatio pertinet erit $\mu(bm + cn) - \nu(am + bn)$ i. e. N. Ex pluribus vero transformationibus propriis diuersis, sequentur totidem repraesentationes diuersae ad N pertinentes **). — Hinc

*) In hoc enim casu, si ad ipsum phrasin extendere volumus, haec: N esse valorem expr. $\sqrt{D}$ (mod. M), siue $NN \equiv D$ (mod. M) significabit, $NN - D$ esse multiplum ipsius M, adeoque $= 0$.

**) Si ex duabus transformationibus propriis diuersis eadem repraesentatio defluere supponitur, illae ita se habere debebunt: 1) $x = mx' - \nu y'$, $y = nx' + \mu y'$; 2) $x = mx' - \nu' y'$, $y = nx'$

facile colligitur, si omnes transformationes propriae formae (F) in (G) habeantur, ex his omnes repraesentationes ipsius M per (F) ad valorem N pertinentes sequi. Vnde quaestio de repraesentationibus numeri dati per formam datam (in quibus indeterminatae valores inter se primos nanciscuntur) inuestigandis, reducta est ad quaestionem de inueniendis omnibus transformationibus propriis formae illius in datam aequiualentem.

Applicanda iam ad haec, ea quae in art. 162 docuimus, facile concluditur: Si repraesentatio aliqua numeri M per formam (F) ad valorem N pertinens sit haec: $x = \alpha$, $y = \gamma$: formulam generalem omnes repraesentationes eiusdem numeri per formam (F), ad valorem N pertinentes, comprehendentem fore hanc: $x = \frac{\alpha t - (ab + \gamma c)u}{m}$, $y = \frac{\gamma t + (\alpha a + \gamma b)u}{m}$, vbi m diuisor communis maximus numerorum a, $2b$, c; et t, u omnes numeri, indefinite, aequationi $tt - Duu = mm$ satisfacientes.

170. Si forma (a, b, c) ancipiti alicui aequiualens, adeoque formae $(M, N, \frac{NN - D}{M})$ tam proprie, quam improprie, siue tam formae $(M, N, \frac{NN - D}{M})$, quam huic $(M, -N, \frac{NN - D}{M})$

$+ \mu' x'$. Sed ex duabus aequationibus $m\mu + n\nu = m\mu' + n\nu'$, $\mu(mb + nc) - \nu(ma + mb) = \mu'(mb + nc) - \nu'(ma + nc)$, facile deducitur esse aut $M = 0$ aut $\mu = \mu'$, $\nu = \nu'$. At $M = 0$ iam exclusimus.

proprie: repraesentationes numeri M habebuntur per formam (F), tam ad valorem N, quam ad valorem $-N$, pertinentes. Et vice versa si plures repraesentationes numeri M per eandem formam (F), ad valores *oppositos* expr. $\sqrt{D}$ (mod. M), N, $-N$, pertinentes habentur: forma (F) formae (G) tam proprie quam improprie aequiualens erit, formaque anceps assignari poterit, cui (F) aequiualeat.

Haec generalia de repraesentationibus hic sufficiant: de repraesentationibus, in quibus indeterminatae valores inter se non primos habent, infra dicemus. Respectu aliarum proprietatum, formae quarum determinans est negatiuus prorsus alio modo sunt tractandae, quam formae determinantis positiui: quare iam vtrasque seorsim considerabimus. Ab illis tamquam facilioribus initium facimus.

171. Problema. *Proposita forma quacunque* (a, b, a') *cuius determinans negatiuus,* $= -D$, *designante* D *numerum positiuum, inuenire formam huic proprie aequiualentem,* (A, B, C), *in qua* A *non* $> \sqrt{\frac{4}{3}D}$, B *non* $> \frac{1}{2}A$, C *non* $< A$.

Solutio. Supponimus in forma proposita non omnes tres conditones simul locum habere: alioquin enim aliam formam quaerere opus non esset. Sit b' residuum abs. min. numeri $-b$ secundum modulum a'*), atque $a'' = \frac{b'b' + D}{a'}$,

*) Obseruare conuenit, si formae alicuius (a, b, a') terminus primus vel vltimus a vel a' sit $= 0$, ipsius determinantem esse quadratum positiuum: quare illud in casu praesenti euenire nequit. — Ex simili ratione termini exteri a, a' formae determinantis negatiui, signa opposita habere non possunt.

qui erit integer quia $b'b' \equiv bb$, $b'b' + D \equiv bb + D \equiv aa' \equiv 0 \pmod{a'}$. Iam si $a'' \prec a'$, fiat denuo b'' resid. abs. min. ipsius $-b'$ secundum mod. a'', atque $a''' = \frac{b''b'' + D}{a''}$. Si hic iterum $a''' \prec a''$, sit rursus b''' res. abs. min. ipsius b'' secundum mod. a''' atque $a^{IV} = \frac{b'''b''' + D}{a'''}$. Haec operatio continuetur donec in progressione a', a'', a''', a^{IV} etc. ad terminum a^{m+1} peruenietur, qui praecedente suo a^m non sit minor, quod tandem euenire debet, quia alias progressio infinita numerorum integrorum continuo decrescentium haberetur. Tum forma (a^m, b^m, a^{m+1}) omnibus conditionibus satisfaciet.

Dem. I. In progressione formarum (a, b, a'), (a', b', a''), (a'', b'', a''') etc, quaeuis praecedenti est contigua, quare vltima primae proprie aequiualens erit (artt. 159, 160).

II. Quum b^m sit residuum absolute minimum ipsius $-b^{m-1}$ secundum mod. a^m, maior quam $\frac{1}{2}a^m$ non erit (art. 4).

III. Quia $a^m a^{m+1} = D + b^m b^m$, atque a^{m+1} non $\prec a^m$, $a^m a^m$ non erit $\succ D + b^m b^m$, et quum b^m non $\succ \frac{1}{2}a^m$, $a^m a^m$ non erit $\succ D + \frac{1}{4}a^m a^m$ et $\frac{3}{4}a^m a^m$ non $\succ D$, tandemque a^m non $\succ \sqrt{\frac{4D}{3}}$.

Exempl. Proposita sit forma (304, 217, 155) cuius determinans $= -31$. Hic inuenitur progressio formarum: (304, 217, 155), (155, —

62, 25), (25, 12, 7), (7, 2, 5), (5, — 2, 7). Vltima est quaesita. — Eodem modo formae (121, 49, 20), cuius determinans = — 19, aequiualentes inueniuntur: (20, — 9, 5), (5, — 1, 4), (4, 1, 5): quare (4, 1, 5) erit forma quaesita.

Tales formas (A, B, C), quarum determinans est negatiuus et in quibus A non $> \sqrt{\frac{4}{3}D}$, B non $> \frac{1}{2}A$, A non $> C$, *formas reductas* vocabimus. Quare cuiuis formae determinantis negatiui, forma reducta proprie aequiualens inueniri poterit.

172. Problema. *Inuenire conditiones, sub quibus duae formae reductae non identicae, eiusdem determinantis, — D, (a, b, c), (a', b', c') proprie aequiualentes esse possint.*

Sol. Supponamus, id quod licet, a' esse non $> a$, formamque $axx + 2bxy + cyy$ transire in $a'x'x' + 2b'x'y' + c'y'y'$ per substitutionem propriam $x = \alpha x' + \epsilon y'$, $y = \gamma x' + \delta y'$. Tum habebuntur aequationes

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a' \quad [1]$$
$$a\alpha\epsilon + b(\alpha\delta + \epsilon\gamma) + c\gamma\delta = b' \quad [2]$$
$$\alpha\delta - \epsilon\gamma = 1 \quad [3]$$

Ex [1] sequitur $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$; quare aa' erit positiuus; et quum $ac = D + bb$, $a'c' = D + b'b'$, etiam ac, $a'c'$ positiui erunt: quare a, a', c, c' omnes eadem signa habebunt. Sed tum a tum a' non $> \sqrt{\frac{4D}{3}}$, adeoque aa' non $> \frac{4D}{3}$; quare

multo minus $D\gamma\gamma$ ($= aa' - (a\alpha + b\gamma)^2$) maior quam $\frac{4}{3}D$ esse poterit. Hinc γ erit aut $= 0$, aut $= \pm 1$.

I. Si $\gamma = 0$, ex [3] sequitur esse aut $\alpha = 1, \delta = 1$, aut $\alpha = -1, \delta = -1$. In vtroque casu fit ex [1] $a' = a$, et ex [2] $b' - b = \pm \mathfrak{C}a$. Sed b non $> \frac{1}{2}a$, et b' non $> \frac{1}{2}a'$ proin etiam non $> \frac{1}{2}a$. Quare aequatio $b' - b = \pm \mathfrak{C}a$, consistere nequit nisi fuerit

aut $b = b'$, vnde sequeretur $c' = \frac{b'b' + D}{a'} = \frac{bb + D}{a} = c$, quare formae (a, b, c), (a', b', c') identicae essent contra hyp.

aut $b = -b' = \pm \frac{1}{2}a$. In hoc etiam casu erit $c' = c$ formaque (a', b', c') erit $(a, -b, c)$ i. e. formae $(a, b, c,)$ opposita. Simul patet formas has esse ancipites propter $2b = +a$.

II. Si $\gamma = \pm 1$, fit ex [1] $a\alpha\alpha + c - a' = \pm 2b\alpha$. Sed c non minor quam a, adeoque non minor quam a': hinc $a\alpha\alpha + c - a'$ siue $2b\alpha$ certo non minor quam $a\alpha\alpha$. Quare quum $2b$ non sit maior quam a, erit α non minor quam $\alpha\alpha$; vnde necessario aut $\alpha = 0$, aut $= \pm 1$.

1) Si $\alpha = 0$, fit ex [1], $a' = c$, et quoniam a neque maior quam c, neque minor quam a', erit necessario $a' = a = c$. Porro ex [3] fit $\mathfrak{C}\gamma = -1$, vnde ex [2] $b + b' = \pm \delta c = \pm \delta a$. Hinc simili modo vt in (I) sequitur esse

aut $b = b'$, in quo casu formae (a, b, c) $(a' b', c')$ forent identicae, contra hyp.

aut $b = -b'$, in quo casu formae (a, b, c), (a', b', c') erunt oppositae.

2) Si $\alpha = \pm 1$, ex [1] sequitur $\mp 2b = a + c - a'$. Quare quum neque a, neque $c < a'$, erit $2b$ non $< a$, et non $< c$. Sed $2b$ etiam non $> a$, neque $> c$, vnde necessario $\pm 2b = a = c$, et hinc ex aequ. $\mp 2b = a + c - a'$, etiam $= a'$. Fit igitur ex [2] $b' = a(\alpha\zeta + \gamma\delta) + b(\alpha\delta + \zeta\gamma)$, siue, propter $\alpha\delta - \zeta\gamma = 1$, $b' - b = a(\alpha\zeta + \gamma\delta) + 2b\gamma = a(\alpha\zeta + \gamma\delta \pm \zeta\gamma)$, quare necessario, vt ante

aut $b = b'$, vnde formae (a, b, c), (a', b', c') identicae, contra hyp.

aut $b = -b'$, adeoque formae illae oppositae. Simul in hoc casu propter $a = \pm 2b$, formae erunt ancipites.

Ex his omnibus colligitur, formas (a, b, c) (a', b', c') proprie aequiualentes esse non posse nisi fuerint oppositae, simulque *aut* ancipites, *aut* $a = c = a' = c'$. In hisce casibus formas (a, b, c), (a', b', c') proprie aequiualere, vel a priori facile praeuideri potuit; si enim formae sunt oppositae, improprie, et si insuper ancipites, etiam poprie aequiualentes esse debent; si vero $a = c$, forma $\left(\frac{D + (a-b)^2}{a}, a - b, a\right)$ formae (a, b, c) contigua et proin aequiualens erit; sed propter $D + bb = ac = aa$ fit $\frac{D+(a-b)^2}{a}$

$= 2a - 2b$, forma vero $(2a - 2b, a - b, a)$ est anceps; quare (a, b, c) oppositae suae etiam proprie aequiualebit.

Aeque facile iam diiudicari potest quando duae formae reductae (a, b, c), (a', b', c') non oppositae improprie aequiualentes esse possint. Erunt enim impr. aequiualentes, si (a, b, c) $(a', -b', c')$, quae non identicae erunt, proprie sunt aequiualentes, et contra. Hinc patet, conditionem, sub qua *illae* improprie sint aequiualentes, esse, vt sint identicae, insuperque aut ancipites aut $a = c$. — Formae vero reductae quae neque identicae sunt neque oppositae, neque proprie neque improprie aequiualentes esse possunt.

173. Problema. *Propositis duabus formis eiusdem determinantis negatiui, F et F', inuestigare vtrum sint aequalentes.*

Solutio. Quaerantur duae formae reductae f, f' formis F, F' resp., proprie aequiualentes: si formae f, f' sunt proprie, vel improprie vel vtroque modo aequiualentes, etiam F, F' erunt; si vero f, f' nullo modo aequiualentes sunt, etiam F, F' non erunt.

Ex art. praec. dari possunt quatuor casus:

1) Si f, f' neque identicae neque oppositae, F, F' nullo modo aequiualentes erunt.

2) Si f, f' sunt *primo* vel identicae vel oppositae, et *secundo* vel ancipites, vel terminos

suos extremos aequales habent: F, F' tum proprie, tum improprie aequiualentes erunt.

3) Si f, f' sunt identicae, neque vero ancipites neque terminos extremos aequales habent: F, F' proprie tantum aequiualebunt.

4) Si f, f' sunt oppositae, neque vero ancipites, neque terminos extremos aequales habent: F, F' proprie tantum aequiualentes erunt.

Ex. Formis (41, 35, 30), (7, 18, 47) quarum determinans $= -5$, reductae (1, 0, 5), (2, 1, 3) aequiualentes inueniuntur, quare illae nullo modo aequiualentes erunt. — Formis vero (23, 38, 63), (15, 20, 27) aequiualet eadem reducta (2, 1, 3), quae quum simul sit anceps, formae (23, 38, 63), (15, 20, 27) tum proprie tum improprie aequiualebunt. — Formis (37, 53, 78), (53, 73, 102), aequiualent reductae (9, 2, 9), (9, — 2, 9) quae quum sint oppositae, ipsarumque termini extremi aequales: formae propositae tam proprie quam improprie erunt aequiualentes.

174. Multitudo omnium formarum reductarum, determinantem datum $= D$ habentium, semper est finita, et, respectu numeri D, satis modica: formae hae ipsae vero duplici modo inueniri possunt. Designemus formas reductas determinantis $= D$ indefinite per (a, b, c), vbi

itaque omnes valores ipsorum a, b, c determinari debent.

Methodus prima. Accipiantur pro a omnes numeri, tum positiui tum negatiui non maiores quam $\sqrt{\frac{4}{3}D}$, quorum residuum quadraticum $= D$, et pro singulis a, fiat b successiue aequalis omnibus valoribus expr. $\sqrt{} = D$ (mod. a), non maioribus quam $\frac{1}{2}a$, tum positiue tum negatiue acceptis; c vero pro singulis valoribus determinatis ipsorum a, b, ponatur $= \frac{D + bb}{a}$. Si quae formae hoc modo oriuntur in quibus $c < a$, hae erunt reiiciendae, reliquae autem manifesto erunt reductae.

Methodus secunda. Accipiantur pro b omnes numeri, tum positiui tum negatiui, non maiores quam $\frac{1}{2}\sqrt{\frac{4}{3}D}$, siue $\sqrt{\frac{1}{3}D}$; pro singulis b resoluatur $bb + D$ omnibus quibus fieri potest modis in binos factores (etiam signorum diuersitatis ratione habita) ambos ipso $2b$ non minores ponaturque alter factor, et quidem, quando factores sunt inaequales, minor, $= a$, alter $= c$. Si quae formae hoc modo prodeunt, in quibus $a \geqslant \sqrt{\frac{4}{3}D}$, erunt reiiciendae, reliquae vero omnes manifesto erunt reductae. — Denique patet, nullam formam reductam dari posse quae non per vtramque methodum inueniatur.

Ex. Sit $D = 85$. Hic limes valorum ipsius a est $\sqrt{\frac{340}{3}}$ qui iacet inter 10 et 11. Numeri vero inter 1 et 10 (incl.) quorum residuum $= 85$, sunt 1, 2, 5, 10. Vnde habentur formae duodecim: (1, 0, 85), (2, 1, 43), (2, — 1, 43), (5, 0, 17), (10, 5, 11); (10 — 5, 11); (—

1, 0, — 85) (— 2, 1, — 43), (— 2, — 1, — 43) (— 5, 0, — 17), (— 10, 5, — 11), (— 10, — 5, — 11).

Per methodum alteram limes valorum ipsius b habetur $\sqrt{\frac{85}{3}}$, qui situs est inter 5 et 6. Pro $b = 0$, prodeunt formae (1, 0, 75), (— 1, 0, — 85), (5, 0, 17), (— 5, 0, — 17), pro $b = \pm 1$ hae: (2, $\pm$ 1, 43) (— 2, $\pm$ 1, — 43). Pro $b = \pm 2$ nullae habentur, quia 89 in duos factores, qui ambo non > 4, resolui nequit. Idem valet de $\pm$ 3, $\pm$ 4. Tandem pro $b = \pm 5$, proueniunt (10, $\pm$ 5, 11), (— 10, $\pm$ 5, — 11).

175. Si ex omnibus formis reductis determinantis dati, formarum binarum, quae, licet non identicae, tamen proprie sunt aequiualentes, alterutra reiicitur: formae remanentes hac insigni proprietate erunt praeditae, vt, quaeuis forma eiusdem determinantis alicui ex ipsis proprie sit aequiualens, et quidem vnicae tantum (alias enim inter ipsas aliquae proprie aequiualentes forent). Vnde patet, *omnes formas eiusdem determinantis in totidem classes distribui posse quot formae remanserint*, referendo scilicet formas eidem reductae proprie aequiualentes in eandem classem. Ita pro $D = 85$, remanent formae (1, 0, 85), (2, 1, 43), (5, 0, 17), (10, 5, 11), (— 1, 0, — 84), (— 2, 1, — 43), (— 5, 0, — 17), (— 10, 5 — 11); quare omnes formae determinantis — 85 in octo classes distribui poterunt, prout formae primae, aut secundae etc. proprie aequiualent. Perspicuum vero est, formas in eadem

classe locatas proprie aequiualentes fore, formas ex diuersis classibus proprie aequiualentes esse non posse. Sed hoc argumentum de classificatione formarum infra multo fusius exsequemur. Hic vnicam obseruationem adiicimus. Iam supra ostendimus, si determinans formae (a, b, c) fuerit negatiuus $= -D$, a et c eadem signa habere (quia scilicet $ac = bb + D$ adeoque positiuus); eadem ratione facile perspicitur, si formae (a, b, c), (a', b', c') sint aequiualentes, omnes a, c, a', c' eadem signa habituros. Si enim prior in posteriorem per substitut: $x = \alpha x' + \epsilon y'$, $y = \gamma x' + \delta y'$ transit: erit $a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a'$, hinc $aa' = (a\alpha + b\epsilon)^2 + D\gamma\gamma$, adeoque certo non negatiuus; quoniam vero neque a, neque $a' = 0$ esse potest, erit aa' positiuus et proin signa ipsorum a, a' eadem. Hinc manifestum est, formas quarum termini exteri sint positiui, ab iis quarum termini exteri sint negatiui, prorsus esse separatas, sufficitque ex formis reductis eas tantum considerare quae terminos suos exteros positiuos habent, nam reliquae totidem sunt multitudine, et ex illis oriuntur, tribuendo terminis exteris signa opposita; idemque valet de formis ex reductis reiiciendis et remanentibus.

176. Ecce itaque pro determinantibus quibusdam negatiuis tabulam formarum, secundum quas omnes reliquae eiusdem determinantis in classes distingui possunt; apponimus autem, ad annotat. art. praec., semissem tantum, scilicet eas quarum termini exteri positiui.

D	
1	(1, 0, 1).
2	(1, 0, 2).
3	(1, 0, 3), (2, 1, 2).
4	(1, 0, 4), (2, 0, 2).
5	(1, 0, 5), (2, 1, 3).
6	(1, 0, 6), (2, 0, 3).
7	(1, 0, 7), (2, 1, 4).
8	(1, 0, 8), (2, 0, 4), (3, 1, 3).
9	(1, 0, 9), (2, 1, 5), (3, 0, 3).
10	(1, 0, 10), (2, 0, 5).
11	(1, 0, 11), (2, 1, 6), (3, 1, 4), (3 — 1, 4).
12	(1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4).

Superfluum foret hanc tabulam hic vlterius continuare, quippe quam infra multo aptius disponere docebimus.

Patet itaque, quamuis formam determinantis — 1, formae $xx + yy$ proprie aequiualere, si ipsius termini exteri sint positiui, vel huic $— xx — yy$, si sint negatiui; quamuis formam determinantis — 2, cuius termini exteri positiui, formae $xx + 2yy$ etc.; quamuis formam determinantis — 11, cuius termini exteri positiui, alicui ex his $xx + 11yy$, $2xx + 2xy + 6yy$, $3xx + 2xy + 4yy$, $3xx — 2xy + 4yy$ etc.

177. Problema. *Habetur series formarum, quarum quaeuis praecedenti a parte posteriori contigua: desideratur transformatio aliqua propria primae in formam quamcunque seriei.*

Solutio. Sint formae $(a,b,a') = F$; $(a', b', a'') = F'$; $(a'', b'', a''') = F''$; $(a''', b''', a^{IV}) = F'''$

etc. Designentur $\frac{b+b'}{a}$, $\frac{b'+b''}{a'}$, $\frac{b''+b'''}{a''}$ etc. respectiue per h', h'', h''' etc. Sint indeterminatae formarum F, F', F'' etc. x, y; x', y'; x'', y'' etc. Ponatur F transmutari

in F' positis $x = \alpha' x' + \gamma' y'$, $y = \beta' x + \delta' y'$
F'' . . . $x = \alpha'' x'' + \gamma'' y''$, $y = \beta'' x'' + \delta'' y''$
F''' . . . $x = \alpha''' x''' + \gamma''' y'''$, $y = \beta''' x''' + \delta''' y'''$
etc.

Tum quia F transit in F' positis $x = -y'$, $y = x' + h' y'$; F' in F'' positis $x' = -y''$, $y' = x'' + h'' y''$; F'' in F''' positis $x'' = -y'''$, $y'' = x''' + h''' y'''$ etc. (art. 160), facile eruetur sequens algorithmus (art. 159):

$$\begin{array}{|l|l|l|l|}
\alpha' = 0 & \gamma' = -1 & \beta' = 1 & \delta' = h' \\
\alpha'' = \gamma' & \gamma'' = h'' \gamma' - \alpha' & \beta'' = \delta' & \delta'' = h'' \delta' - \beta' \\
\alpha''' = \gamma'' & \gamma''' = h''' \gamma'' - \alpha'' & \beta''' = \delta'' & \delta''' = h''' \delta'' - \beta'' \\
\alpha^{IV} = \gamma''' & \gamma_{IV} = h^{IV} \gamma''' - \alpha''' & \beta_{IV} = \delta''' & \delta_{IV} = h^{IV} \delta''' - \beta'''
\end{array}$$

etc.

siue

$$\begin{array}{|l|l|l|l|}
\alpha' = 0 & \gamma' = -1 & \beta' = 1 & \delta' = h' \\
\alpha'' = \gamma' & \gamma'' = h'' \gamma' & \beta'' = \delta' & \delta'' = h'' \delta' - 1 \\
\alpha''' = \gamma'' & \gamma''' = h''' \gamma'' - \gamma' & \beta''' = \delta'' & \delta''' = h''' \delta'' - \delta' \\
\alpha^{IV} = \gamma''' & \gamma_{IV} = h^{IV} \gamma''' - \gamma'' & \beta_{IV} = \delta''' & \delta_{IV} = h^{IV} \delta''' - \delta''
\end{array}$$

etc.

Omnes has transformationes esse proprias tum ex ipsarum formatione tum ex art, 159 nullo negotio deduci potest.

Algorithmus hic perquam simplex et ad calculum expeditus, algorithmo in art. 27 exposito est analogus, ad quem etiam reduci potest *). Ceterum solutio haec ad formas determinantis negatiui non est restricta, sed ad omnes casus patet, si modo nullus numerorum a', a'', a''' etc. $= 0$.

178. Problema. *Propositis duabus formis F, f, eiusdem determinantis negatiui, proprie aequiualentibus: inuenire transformationem aliquam propriam alterius in alteram.*

Sol. Supponamus formam F esse (A, B, A') et per methodum art. 171 inuentam esse progressionem formarum (A', B', A''), (A'', B'', A''') etc. vsque ad (A^m, B^m, A^{m+1}) quae sit reducta: similiterqun f esse (a, b, a') et per eandem methodum inuentam seriem (a', b', a''), (a'', b'', a''') vsque ad (a_n, b_n, a^{n+1}), quae sit reducta. Tum duo casus locum habere possunt.

I. Si formae (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) sunt aut identicae, aut oppositae simulque ancipites. Tum formae (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$ erunt contiguae (designante A^{m-1} terminum progressionis $A, A', A'' \ldots A^m$ penultimum, similiaque $B^{m-1}, a^{n-1}, b^{n-1}$). Nam

*) Erit scilicet in signis art. 27, $\zeta^n = \pm [- h'', h''' - h^{IV} \ldots \pm h^n]$, vbi signa ambigue posita, esse debent $- -$; $- +$; $+ -$; $+ +$; prout n formae $4k + 0$; 1; 2; 3 — et $\delta^n = \pm [h' - h'', h''' \ldots \pm h^n]$, vbi signa ambigua esse debent $+ -$; $+ +$; $- -$; $- +$ prout n formae $4k + 0$; 1; 2; 3. Sed hoc, quod quiuis facile ipse confirmare poterit, fusius exsequi, nobis breuitas non permittit.

$A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ siue } A^m}$, vnde $B^{m-1} - b^{n-1} \equiv b^n - B^m$ adeoque $\equiv 0$, si formae (A^m, B^m, A^{m+1}), (a_n, b_n, a^{n+1}) sunt identicae et $\equiv 2b^n$ adeoque $\equiv 0$, si sunt oppositae et ancipites. Quare in progressione formarum (A, B, A'), (A', B', A'') .... (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$, $(a^{n-1}, -b^{n-2}, a^{n-2})$ ... $(a', -b, a)$, (a, b, a') quaeuis forma praecedenti contigua erit, adeoque per art. praec. transformatio propria primae F in vltimam f inueniri poterit.

II. Si formae (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) non identicae, sed oppositae simulque $A^m = A^{m+1} = a^n = a^{n+1}$. Tum progressio formarum (A, B, A'), (A', B', A'') .... (A^m, B^m, A^{m+1}), $(a^n, -b^{n-1}, a^{n-1})$, $(a^{n-1}, -b^{n-2}, a^{n-2})$ .... $(a', -b, a)$, (a, b, a') eadem proprietate erit praedita. Nam $A^{m+1} = a^n$, et $B^m - b^{n-1} = -(b^n + b^{n-1})$ per a^n diuisibilis. Vnde per art. praec. inuenietur transformatio propria formae primae F in vltimam f.

Ex. Ita pro formis (23, 38, 63), (15, 20, 27) habetur progressio (23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, — 7, 27) (27, — 20, 15), (15, 20, 27), quare $h' = 1$, $h'' = 3$, $h''' = 2$, $h^{IV} = -3$, $h^V = -1$, $h^{VI} = 0$. Hinc deducitur transformatio formae $23xx + 76xy + 63yy$ in $15tt + 40tu + 27uu$ haec: $x = -13t - 18u$, $y = 8t + 11u$.

Ex solutione hac nullo negotio sequitur solutio problematis: *Si formae F, f improprie sunt aequiualentes, inuenire transformationem impropriam formae F in f.* Sit enim $f = att + 2btu + a'uu$ eritque forma opposita $app - 2bpq + a'qq$ formae F proprie aequiualens. Quaeratur transformatio propria formae F in illam, $x = \alpha p + \varepsilon q$, $y = \gamma p + \delta q$, patetque F transire in f positis $x = \alpha t - \varepsilon q$, $y = \gamma t - \delta q$, hancque transformationem fore impropriam.

Quodsi igitur formae F, f tam proprie quam improprie sunt aequiualentes: inueniri poterit tam transformatio propria aliqua quam impropria.

179. Problema. *Si forma F, f sunt aequiualentes: inuenire omnes transformationes formae F in f.*

Sol. Si formae F, f vnico tantum modo sunt aequiualentes i. e. proprie tantum vel improprie tantum: quaeratur per art. praec. transformatio vna formae F in f, patetque alias quam quae huic sint similes dari non posse. Si vero formae F, f tam proprie quam improprie aequiualent, quaerantur duae transformationes, altera propria, altera impropria. Iam sit forma $F = (A, B, C)$, $BB - AC = -D$, numerorumque A, $2B$, C diuisor communis maximus $= m$. Tum ex art. 162 patet, in priori casu omnes transformationes formae F in f ex vna transformatione, in posteriori omnes proprias ex propria omnesque improprias ex impropria deduci posse, si modo omnes solutio-

nes aequationist $tt + Duu = mm$ habeantur. His igitur inuentis problema erit solutum.

Habetur autem $D = AC - BB$, $4D = 4AC - 4BB$, quare $\frac{4D}{mm} = 4\frac{A}{m}\frac{C}{m} - (\frac{2B}{m})^2$ erit integer. Iam si

1) $\frac{4D}{mm} > 4$, erit $D > mm$: quare in $tt + Duu = mm$, u necessario debebit esse $= 0$, adeoque t alios valores quam $+ m$, et $- m$ habere nequit. Hinc si F, f vnico tantum modo aequiualentes sunt et transformatio aliqua $x = \alpha x' + \xi y'$, $y = \gamma x' + \delta y'$: praeter hanc ipsam quae prodit ex $t = m$ (art. 162), et hanc $x = \alpha x' - \xi y'$, $y = -\gamma x' - \delta y'$ aliae locum habere non possunt. Si vero F, f tum proprie tum improprie aequiualent, atque propria aliqua transformatio habetur $x = \alpha x' + \xi y'$, $= \gamma x' + \delta y'$, impropriaque $x = \alpha' x' + \xi y'$, $y = \gamma' x' + \delta' y'$, praeter illam (ex $t = m$) et hancce $x = -\alpha' x' - \xi' y'$, $y = -\gamma' x' - \delta y'$ (ex $t = -m$) alia propria non dabitur; similiterque nulla impropria praeter $x = \alpha' x' + \delta' y'$, $y = \gamma' x' + \delta' y'$ et $x = -\alpha' x' - \xi' y'$, $y' = -\gamma x' - \delta' y'$.

2) Si $\frac{4D}{mm} = 4$, siue $D = mm$, aequatio $tt + Duu = mm$ quatuor solutiones admittet t, $u = m, 0; -m, 0; 0, 1; 0, -1$. Hinc si F, f vnico tantum modo sunt aequiualentes et transformatio aliqua $x = \alpha x' + \xi y'$, $y = \gamma x' + \delta y'$: *quatuor* omnino transformationes dabuntur, $x = \pm \alpha x' + \xi y'$, $y = \pm \gamma x' \pm \delta y'$; $x = \mp \frac{\alpha B + \gamma C}{m} x' \mp \frac{\xi B + \delta C}{m} y'$, $y = \pm \frac{\alpha A + \gamma B}{m} x' \pm \frac{\xi A + \delta B}{m} y'$. Siue

ro F, f duobus modis aequiualent, siue praeter transformationem illam datam alia ipsi dissimilis habetur: haec quoque suppeditabit quatuor illis dissimiles, ita vt *octo* transformationes habeantur. — Ceterum facile demonstrari potest in hoc casu F, f semper reuera duobus modis aequiualere. Nam quum $D = mm = AC - BB$, m etiam ipsum B metietur. Formae $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ determinans erit $= -1$, quare formae $(1, 0, 1)$ vel huic $(-1, 0, -1)$ erit aequialens. Facile vero perspicitur, per eandem transformationem per quam $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ transeat in $(\pm 1, 0, \pm 1)$ formam (A, B, C) transire in $(\pm m, 0, \pm m)$, ancipitem. Quare forma (A, B, C), ancipiti aequialens, cuiuis formae, cui aequialet, tum proprie tum improprie aequialebit.

3) Si $\frac{4D}{mm} = 3$, siue $4D = 3mm$. Tum m erit par omnesque solutiones aequationis $tt + Duu = mm$ erunt sex, $t, u = m, 0$; $-m, 0$; $\frac{1}{2}m, 1$; $-\frac{1}{2}m, -1$; $\frac{1}{2}m, -1$; $-\frac{1}{2}m, 1$, Si itaque duae transformationes dissimiles formae F in f habentur, $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; $x = {}'x' + \beta' y'$, $y = \gamma' x' + \delta' y'$: habebuntur duodecim transformationes, scilicet sex priori similes

$$x = \pm \alpha x' \pm \beta y', \quad y = \pm \gamma x' \pm \delta y';$$

$$x = \pm (\tfrac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta - \frac{\beta B + \delta C}{m}) y',$$
$$y = \pm (\tfrac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m}) x' \pm (\tfrac{1}{2}\delta + \frac{\beta A + \delta B}{m}) y';$$

$$x = \pm (\tfrac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m}) x' \pm (\tfrac{1}{2}\beta + \beta \frac{B + \delta C}{m}) y'$$
$$y = \pm (\tfrac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m} x' \pm (\tfrac{1}{2}\delta - \frac{\beta A + \delta B}{m}) y'$$

et sex posteriori similes, quae ex his nascuntur ponendo pro α, β, γ, δ hos α', β', γ', δ'.

Quod vero in hoc casu semper F, f vtroque modo aequiualent, ita demonstramus. Formae $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ determinans erit $= -\frac{4D}{mm} = -3$, adeoque (art. 176) aut formae $(\pm 1, 0, \pm 3)$ aut huic $(2, 1, 2)$ aequiualens. Vnde facile perspicitur, formam (A, B, C) aut formae $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ aut huic $(\pm m, \frac{1}{2}m, \pm m)$*) quae ambae sunt ancipites, aequiualere adeoque, cuiuis aequiualenti, vtroque modo.

4) Si supponitur $\frac{4D}{mm} = 1$, fit $(\frac{2B}{mm})^2 = 4\frac{AC}{mm} - 2$, adeoque $\equiv 2 (\mathrm{mod.}\ 4)$. Sed quum nullum quadratum esse possit $\equiv 2 (\mathrm{mod.}\ 4)$ hic casus locum habere nequit.

5) Supponendo $\frac{4D}{mm} = 1$, fit $(\frac{2B}{m})^2 = 4\frac{AC}{mm} - 1 \equiv -1 (\mathrm{mod.}\ 4)$. Quod quum impossibile sit, etiam hic casus nequit locum habere.

Ceterum quum D neque $= 0$, neque negatiuus sit, alii casus praeter enumeratos dari non possunt.

180. Problema. *Inuenire omnes repraesentationes numeri dati M per formam $axx + 2bxy + cyy$ ... F, determinantis negatiui $-D$, in quibus x, y valores inter se primos nanciscuntur.*

*) Demonstrari potest, formam (A, B, C) necessario posteriori aequialere: sed hoc hic non necessarium.

Sol. Ex art. 154 patet, M eo quo requiritur modo repraesentari non posse, nisi $-D$ sit resid. quadr. ipsius M. Inuestigentur itaque primo omnes valores diuersi (*i. e.* incongrui) expr. $\sqrt{} - D \pmod{M}$, qui sint N, $-N$, N' N', N'', $-N''$ etc.; quo simplicior euadat calculus, omnes N, N' etc. ita determinari possunt, vt non sint $> \frac{1}{2}M$. Iam quoniam quaeuis repraesentatio ad aliquem horum valorum pertinere debet singuli seorsim considerentur.

Si formae F, $(M, N, \frac{D+NN}{M})$ non sunt proprie aequiualentes, nulla repraesentatio ipsius M ad valorem N pertinens dari potest (art. 168). Si vero sunt, inuestigetur transformatio propria formae F in $Mx'x' + 2Nx'y' + \frac{D+NN}{M}y'y'$ quae sit $x = \alpha x' + \epsilon y'$, $y = \gamma x' + \delta y'$, eritque $x = \alpha$, $y = \gamma$ repraesentatio numeri M per F ad N pertinens. Sit diu. comm. max. numerorum A, $2B$, C, $= m$ distinguanturque tres casus (art. praec.):

1) Si $\frac{4D}{mm} > 4$, aliae repraesentationes ad N pertinentes quam hae *duae* $x = \alpha$, $y = \gamma$; $x = -\alpha$, $y = -\gamma$ non dabuntur (artt. 169, 180).

2) Si $\frac{4D}{mm} = 4$, habebuntur *quatuor* repraesentationes $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\frac{\alpha B + \gamma C}{m}$, $y = \pm\frac{\alpha A + \gamma B}{m}$.

3) Si $\frac{4D}{mm} = 3$, habebuntur *sex* repraesentationes, $x = \pm\alpha$, $y = \pm\gamma$; $x = \pm(\frac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m})$, $y = \pm(\frac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m})$; $x = \pm(\frac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m})$, $y = \pm(\frac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m})$.

Eodem modo quaerendae sunt repraesensentationes ad valores $-N$, N', $-N'$ etc. pertinentes.

181. Inuestigatio repraesentationum numeri M per formam F in quibus x, y valores inter se non primos habent, ad casum iam consideratum facile reduci potest. Fiat talis repraesentatio ponendo $x = \mu e$, $y = \mu f$, ita vt μ sit diu. comm. max. ipsorum μe, μf, siue e, f inter se primi. Tum erit $M = \mu\mu(Aee + 2Bef + Cff)$ adeoque per $\mu\mu$ diuisibilis; substitutio vero $x = e$, $y = f$ erit repraesentatio numeri $\frac{M}{\mu\mu}$ per formam F, in qua x, y valores inter se primos habent. Si itaque M per nullum quadratum (praeter 1) diuisibilis est, *e. g.* si est numerus primus: tales repraesentationes ipsius M non dabuntur. Si vero A diuisores quadraticos implicat, sint hi $\mu\mu$, $\nu\nu$, $\pi\pi$ etc. Quaerantur primo omnes repraesentationes numeri $\frac{M}{\mu\mu}$ per formam (A, B, C), in quibus x, y valores inter se primos habent, qui valores si per μ multiplicantur praebebunt omnes repraesentationes ipsius M, in quibus diu. comm. max. numerorum x, y est μ. Simili modo omnes repraesentationes ipsius $\frac{M}{\nu\nu}$ in quibus valores

ipsorum x, y inter se primi sunt, praebebunt omnes repraesentationes ipsius M in quibus diu. comm. max. valorum ipsorum x, y est ϑ etc.

Palam igitur est, per praecepta praecedentia omnes repraesentationes numeri dati per formam datam determinantis negatiui inueniri posse.

182. Descendimus ad quosdam casus particulares, tum propter insignem ipsorum elegantiam, tum propter assiduam operam ab ill. Eulero ipsis impensam, vnde classicam quasi dignitatem sunt nacti.

I. Per formam $xx + yy$ ita repraesentari vt x ad y sit primus, (siue in duo quadrata inter se prima discerpi), nullus numerus potest nisi cuius residuum quadraticum est $= -1$, tales vero numeri, positiue accepti, omnes poterunt. Sit M talis numerus, omnesque valores expr. $\sqrt{} -1 \pmod{M}$ hi: N, $-N$, N', $-N'$, N'', $-N''$ etc. Tum per art. 176 forma $(M, N, \frac{NN+1}{M})$ formae $(1, 0, 1)$ proprie aequiualens erit. Sit transformatio aliqua propria huius in illam, $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, eruntque repraesentationes numeri M per formam $xx + yy$ ad N pertinentes hi quatuor *): $x = \pm \alpha$, $y = \pm \gamma$; $x = \mp \gamma$, $y = \pm \alpha$.

*) Patet enim, hunc casum sub (2) art. 180 contentum esse.

Quum forma (1, 0, 1) sit anceps, patet, etiam formam (M, — N, $\frac{NN \mp 1}{M}$) ipsi proprie aequiualentem fore, illamque proprie in hanc transmutari positis $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. Hinc deriuantur quatuor repraesentationes ipsius M ad — N pertinentes, $x = \pm \alpha$, $y = \mp \gamma$; $x = \pm \gamma$, $y = \mp \alpha$. Manifestum itaque est, octo repraesentationes ipsius M dari, quarum semissis altera ad N, altera ad — N pertineat; sed hae omnes *vnicam* tantummodo discerptionem numeri M in duo quadrata exhibent, $M = \alpha\alpha + \gamma\gamma$, siquidem ad quadrata ipsa tantum, neque vero ad ordinem radicumue signa spectamus.

Quodsi itaque alii valores expr. $\sqrt{} - 1$ (mod. M) praeter N et — N non dantur, quod *e. g.* euenit, quando M est numerus primus, M vnico tantum modo in duo quadrata inter se prima resolui poterit. Iam quum — 1 sit residuum quadraticum cuiusuis numeri primi formae $4n + 1$ (art. 108), manifestoque numerus primus in duo quadrata inter se non prima discerpi nequeat, habemus theorema:

Quiuis numerus primus formae $4n + 1$ *in duo quadrata decomponi potest, et quidem vnico tantum modo.* $1 = 0 + 1$, $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, $29 = 4 + 25$, $37 = 1 + 36$, $41 = 16 + 25$, $53 = 4 + 49$, $61 = 25 + 36$, $73 = 9 + 64$, $89 = 25 + 64$, $97 = 16 + 81$ etc.

Theorema hoc elegantissimum iam Fermatio notum fuit, sed ab ill. Eulero primo demonstratum est, *Comm. nou. Petr. T. V, ad annos* 1754, 1755, *p.* 3 *sqq.* In *T. IV*, diss. exstat ad idem argumentum pertinens, p 3 sqq., sed tum rem penitus nondum absoluerat, vid. imprimis art. 27.

Si igitur numerus aliquis formae $4n + 1$ aut pluribus modis aut nullo modo in duo quadrata resolui potest, certo non erit primus.

Vice versa autem, si expr. $\sqrt{\ } - 1$ (mod. M) praeter N et $-N$ alios adhuc valores habet, aliae adhuc repraesentationes ipsius M dabuntur, ad hos pertinentes. In hoc itaque casu M pluribus modis in duo quadrata resolui poterit e. g. $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Repraesentationes reliquae, in quibus x, y valores obtinent non primos inter se, per methodum nostram generalem facile inueniri possunt. Obseruamus tantummodo, si numerus aliquis factores formae $4n + 3$ inuoluens, per nullam diuisionem per quadratum ab his liberari possit (quod fiet, si aliquis aut plures talium factorum *dimensionem imparem* habet), hunc nullo modo in duo quadrata resolui posse *).

*) Si numerus $M = 2^{\mu} Sa^{\alpha} b^{\beta} c^{\gamma} \ldots$ ita vt a, b, c etc. sint numeri primi inaequales formae $4n + 1$, atque S productum ex omnibus factoribus primis ipsius M formae $4n + 3$ (ad quam formam

II. Per formam $xx + 2yy$ nullus numerus, cuius non residuum -2, ita repraesentari potest vt x ad y sit primus, reliqui omnes poterunt. Sit -2 residuum numeri M, atque N valor aliquis expr. $\sqrt{\ } -2 \pmod{M}$. Tum per art. 176 formae $(1, 0, 2)$, $(M, N, \frac{NN+2}{M})$ proprie aequiualentes erunt. Transeat illa proprie in hanc ponendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, eritque $x = \alpha$, $y = \gamma$ repraesentatio numeri M ad N pertinens. Praeter quam et hanc $x = -\alpha$, $y = -\gamma$ aliae ad N non pertinebunt (art. 180).

Simili modo, vt supra, perspicitur, repraesentationes $x = \pm\alpha$, $y = \mp\gamma$ ad valorem $-N$ pertinere. Omnes vero hae quatuor repraesentationes vnicam tantum discerptionem ipsius M in quadratum et quadratum duplex exhibent, et si praeter N et $-N$ alii valores expr. $\sqrt{\ } -2 \pmod{M}$ non dantur, aliae discerptiones non dabuntur. Hinc adiumento proposs. art. 116 facile deducitur theorema:

quiuis numerus positiuus reduci potest, faciendo $\mu = 0$ quando M est impar, et $S = 1$ quando M nullos factores formae $4n+3$ implicat): *M nullo modo* in duo quadrata resolui poterit, si S est non-quadratus; si vero S est quadratus, dabuntur $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ etc discerptiones ipsius M, quando aliquis numerorum α, β, γ etc. est impar, aut $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$ etc. $+\frac{1}{2}$, quando omnes α, β, γ etc. sunt pares (siquidem ad quadrata ipsa tantum respicitur). Qui in calculo combinationum aliquantum sunt versati, demonstrationem huius theorematis (cui, perinde vt aliis *particularibus*, immorari nobis non licet) ex theoria nostra generali haud difficulter eruere poterunt. Cf. art. 105.

Quiuis numerus primus formae $8n + 1$ *vel* $8n + 3$ *in quadratum et quadratum duplex decomponi potest et quidem vnico tantum modo.* $1 = 1 + 0$, $3 = 1 + 2$, $11 = 9 + 2$, $17 = 9 + 8$, $19 = 1 + 18$, $41 = 9 + 32$, $43 = 25 + 18$, $59 = 9 + 50$, $67 = 49 + 18$, $73 = 1 + 72$, $83 = 81 + 2$, $89 = 81 + 8$, $97 = 25 + 72$ etc.

Etiam hoc theorema, vti plura similia, Fermatio innotuit: sed ill. La Grange primus demonstrationem dedit, *Suite des recherches d'Arithmetique, Nouv. Mem. de l'Ac. de Berlin* 1775, *p.* 323 *sqq.* Multa ad idem argumentum pertinentia iam ill. Euler absoluerat, *Specimen de vsu obseruationum in mathesi pura Comm. nou. Petr. T. VI p.* 185 *sqq.* Sed demonstratio completa theorematis semper ipsius industriam elusit, p. 220. Conf. etiam diss. in T. VIII (ad annos 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, sub fin.

III. Per methodum similem demonstratur, quemuis numerum cuius residuum quadr. sit -3 repraesentari posse aut per formam $xx + 3yy$, aut per hanc $2xx + 2xy + 2yy$, ita vt valor ipsius x ad valorem ipsius y sit primus. Quare quum -3 sit residuum omnium numerorum primorum formae $3n + 1$ (art. 119) manifestoque per formam $2xx + 2xy + 2yy$ numeri *pares* tantum repraesentari possint: eodem modo vt supra habetur theorema:

Quiuis numerus primus formae $3n + 1$ *in quadratum et quadratum triplex decomponi potest, et quidem vnico tantum modo.* $1 = 1 + 0$, $7 = 4 + 3$, $13 = 1 + 12$, $19 = 16 + 3$, $31 = 4 + 27$, $37 = 25 + 12$, $43 = 16 + 27$, $61 = 49 + 12$, $67 = 64 + 3$, $73 = 1 + 72$ etc.

Demonstrationem huius theorematis ill. Euler primus tradidit in commentatione modo laudata, *Comm. nou. Petr. T. VIII, p.* 105 *sqq.*

Simili modo vlterius progredi et *e. g.* ostendere possemus, quemuis numerum primum formae $20n + 1$, vel $20n + 3$, vel $20n + 7$, vel $20n + 9$ (quippe quorum residuum — 5) per alterutram formam $xx + 5yy$, $2xx + 2xy + 3yy$ repraesentari posse, et quidem numeros primos formae $20n + 1$ et $20n + 9$ per priorem, primos formae $20n + 3$, $20n + 7$, per posteriorem, nec non dupla primorum formae $20n + 1$, $20n + 9$ per formam $2xx + 2xy + 3yy$, dupla primorum formae $20n + 3$, $20n + 7$, per formam $xx + 5yy$: sed hanc propositionem infinitasque alias particulares quiuis proprio marte ex praecedentibus et infra tradendis deriuare poterit. — Transimus itaque ad *formas determinantis positiui*, et quum harum indoles prorsus alia sit, quando determinans est quadratus, alia, quando non-quadratus: formas determinantis quadrati hic primo excludimus posteaque seorsim considerabimus.

183. Problema. *Proposita forma quacunque* (a, b, a'), *cuius determinans positiuus non-quadratus* $= D$: *inuenire formam huic proprie aequiualentem,* $(A,$

B, C), in qua B sit positiuus et $< \sqrt{D}$; *A vero si est positiuus, vel* $-A$, *si A negatiuus, inter* $\sqrt{D}$ *et* $\sqrt{D} - B$ *situs.*

Sol. Supponimus in forma proposita vtramque conditionem nondum locum habere; alioquin enim aliam formam quaerere opus non esset. Porro obseruamus, in forma determinantis *non-quadrati* terminum primum vel vltimum $= o$ esse non posse (art. 171 ann.). Sit $b' \equiv -b \pmod{a'}$ atque intra limites $\sqrt{D}$ et $\sqrt{D} \mp a$ situs (accepto signo superiori, quando a' positiuus, inferiori, quando est negatiuus) quod fieri posse simili ratione vt art. 3, facile demonstratur, ponaturque $\frac{b'b' - D}{a'} = a''$, qui erit integer, quia $b'b' - D \equiv bb - D \equiv aa' \equiv o \pmod{a'}$. Iam si $a'' < a'$, fiat denuo $b'' \equiv -b' \pmod{a''}$ et inter $\sqrt{D}$ et $\sqrt{D} \mp a''$ situs (prout a'' positiuus vel negatiuus) et $\frac{b''b'' - D}{a''} = a'''$. Si hic iterum $a''' < a''$, sit rursus $b''' \equiv -b'' \pmod{a'''}$, et inter $\sqrt{D}$ et $\sqrt{D} \mp a'''$ situs atque $\frac{b'''b''' - D}{a'''} = a^{IV}$. Haec operatio continuetur, donec in progressione a', a'', a''', a^{IV} etc. ad terminum a^{m+1} perueniatur, praecedente a^m non minorem, quod tandem euenire debet, quia alioquin progressio infinita numerorum integrorum continuo decrescentium haberetur. Tum positis $a^m = A$, $b^m = B$, $a^{m+1} = C$, forma (A, B, C) omnibus conditionibus satisfaciet.

Dem. I. Quoniam in progressione formarum (a, b, a'), (a', b', a''), (a'', b'', a''') etc. quaeuis praecedenti est contigua: vltima (A, B, C) primae (a, b, a') proprie aequiualens erit.

II. Quia B inter $\sqrt{D}$ et $\sqrt{D} \mp A$ situs est (accipiendo semper signum superius quando A est positiuus, inferius quando A est negatiuus): patet, si ponatur $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$, hos p, q fore positiuos. Iam facile confirmatur, fore $qq + 2pq + 2p\sqrt{D} = D + AA - BB$; quare $D + AA - BB$ erit numerus positiuus, quem ponemus $= r$. Hinc propter $D = BB - AC$, fit $r = AA - AC$, adeoque $AA - AC$ numerus positius: quia vero per hyp. A non est maior quam C, manifesto illud aliter fieri nequit, quam si AC est negatiuus, adeoque signa ipsorum A, C opposita. Hinc $BB = D + AC < D$ adeoque $B < \sqrt{D}$.

III. Porro quia $-AC = D - BB$, erit $AC < D$, et hinc (quia A non $< C$), $A < \sqrt{D}$. Quare $\sqrt{D} \mp A$ erit positiuus, adeoque etiam B, qui inter limites $\sqrt{D}$ et $\sqrt{D} \mp A$, est situs.

IV. Hinc a potiori $\sqrt{D} + B \mp A$ positiuus, et quia $\sqrt{D} - B \pm A = -q$, est negatiuus, $\pm A$ situs erit inter $\sqrt{D} + B$ et $\sqrt{D} - B$. *Q. E. D.*

Ex. Proposita sit forma (67, 97, 140), cuius determinans $= 29$. Hic inuenitur pro-

gressio formarum (67, 97, 140), (140, — 97, 67) (67, — 37, 20) (20, — 3, — 1), (— 1, 5, 4). Vltima erit quaesita.

Tales formas (A, B, C) determinantis positiui non-quadrati D, in quibus A positiue acceptus iacet inter $\sqrt{D} + B$ et $\sqrt{D} - B$, B vero positiuus est atque $< \sqrt{D}$, *formas reductas* vocabimus. Formae itaque reductae determinantis positiui non-quadrati aliquantum differunt a formis reductis determinantis negatiui; sed propter magnam analogiam inter has et illas, denominationes diuersas introducere noluimus.

184. Si aequiualentia duarum formarum *reductarum* determinantis positiui aeque facile dignosci posset, vt in formis determinantis negatiui (art. 172), aequiualentiam duarum formarum *quarumcunque* eiusdem determinantis positiui nullo negotio diiudicare possemus. Sed hic res longe aliter se habet, fierique potest vt permultae formae reductae inter se aequiualentes sint. Antequam itaque problema hoc aggrediamur, profundius in naturam formarum reductarum (determinantis positiui non-quadrati, quod semper hic subintelligendum) inquirere necesse erit.

1) Si (a, b, c) est forma reducta, a et c signa opposita habebunt. Nam posito determinante formae $= D$, erit $ac = bb - D$, adeoque, propter $b < \sqrt{D}$, negatiuus.

2) Numerus c perinde vt a, positiue acceptus, inter $\sqrt{D} + b$ et $\sqrt{D} - b$ situs erit. Nam $-c = \frac{D - bb}{a}$; quare, abstractione facta a signo, c iacebit inter $\frac{D - bb}{\sqrt{D} + b}$ et $\frac{D - bb}{\sqrt{D} - b}$ i. e. inter $\sqrt{D} - b$ et $D + b$.

3) Hinc patet, etiam (c, b, a) fore formam reductam.

4) Tum a tum c erunt $< 2\sqrt{D}$. Vterque enim est $< \sqrt{D} + B$, adeoque a potiori $< 2\sqrt{D}$.

5) Numerus b situs erit inter $\sqrt{D}$ et $\sqrt{D} \mp a$ (accepto signo superiori quando a positiuus, inferiori quando est negatiuus). Quia enim $\pm a$ iacet inter $\sqrt{D} + b$ et $\sqrt{D} - b$, erit $\pm a - (\sqrt{D} - b)$, siue $b - (\sqrt{D} \mp a)$ positiuus; $b - \sqrt{D}$ autem est negatiuus; quamobrem b inter $\sqrt{D}$ et $\sqrt{D} \mp a$ erit situs. — Prorsus eodem modo demonstratur, b inter $\sqrt{D}$ et $\sqrt{D} \mp c$ iacere (prout c pos. vel neg.).

6) *Cuiuis formae reductae* (a, b, c) *ab vtraque parte contigua est reducta vna, et non plures.*

Fiat $a' \equiv c$, $b' \equiv -b \pmod{a'}$ et inter $\sqrt{D}$ et $\sqrt{D} \mp a'$ situs *), $c' = \frac{b'b' - D}{a'}$, eritque forma (a', b', c') formae (a, b, c) ab vltima

*) Vbi signa ambigua sunt, superiora semper valent quando a' est positiuus, inferiora quando a' negatiuus.

parte contigua, simulque manifestam est, si vlla forma reducta formae (a, b, c) ab vltima parte contigua detur, eam ab hac $(a' b', c')$ diuersam esse non posse. Hanc vero reuera esse reductam, ita demonstramus.

A) Si ponitur $\sqrt{D} + b \mp a' = p$, $\pm a' - (\sqrt{D} - b) = q$, $\sqrt{D} - b = r$, hi p, q, r ex (2) supra et defin. formae reductae erunt positiui. Porro ponatur $b' - (\sqrt{D} \mp a') = q'$, $\sqrt{D} - b' = r'$ eruntque q', r' positiui, quia b' iacet inter $\sqrt{D}$ et $\sqrt{D} \mp a'$. Denique sit $b + b' = \pm ma'$ eritque m integer. Iam patet esse $p + q' = b + b'$, adeoque $b + b'$ siue $\pm ma'$ positiuum, et proin etiam m; vnde sequitur $m - 1$ certe non esse negatiuum. Porro fit $r + q' \pm ma' = 2b' \pm a'$, siue $2b' = r + q' \pm (m - 1)a'$, vnde $2b'$ et b' necessario erunt positiui. Et quoniam $b' + r' = \sqrt{D}$, erit $b' < \sqrt{D}$.

B) Porro fit $r \pm ma' = \sqrt{D} + b'$, siue $r \pm (m - 1)a' = \sqrt{D} + b' \mp a'$; quare $\sqrt{D} + b' \mp a'$ erit positiuus. Hinc et quoniam $\pm a' - (\sqrt{\ } - b') = q'$, adeoque positiuus, $\mp a'$ iacebit inter $\sqrt{D} + b'$ et $\sqrt{D} - b'$. — Quocirca (a', b', c') erit forma reducta.

Eodem modo demonstratur, si fiat $'c = a$, $'b \equiv -b \pmod{'c}$ et inter $\sqrt{D}$ et $\sqrt{D} \pm {}'c$ situs, $'a = \frac{'b'b - D}{'c}$, formam $('a, 'b, 'c)$ fore reductam. Manifesto autem forma haec formae (a, b, c) a parte prima est contigua, aliaque

reducta praeter $('a, 'b, 'c)$ hac proprietate praedita esse non poterit.

Ex. Formae reductae (5, 11 — 14), cuius determinans = 191, a parte vltima contigua reducta (— 14, 3, 13), a parte prima vero haec (— 22, 9, 5).

7) Si formae reductae (a, b, c) a parte vltima contigua est reducta (a', b', c'): reductae (c, b, a) contigua erit a prima parte forma (c', b', a'); et si reductae (a, b, c) a prima parte contigua est forma $('a, 'b, 'c)$; reductae (c, b, a) reducta $('c, 'b, 'a)$ contigua erit ab vltima parte. Porro etiam formae $(— 'a, 'b, — 'c)$, $(— a, b, — c)$, $(— a', b', — c')$ reductae erunt, et secunda primae, tertia secundae ab vltima parte contiguae, siue prima secundae, secundaque tertiae a parte prima; similiterque tres formae $(— c', b' — a')$, $(— c, b, a)$, $(— 'c, 'b, — 'a)$. Haec tam obuia sunt vt explicatione non egeant.

185. Multitudo omnium formarum reductarum determinantis dati D semper est finita, ipsae vero duplici modo inueniri possunt. Designemus indefinite omnes formas reductas determinantis D per (a, b, c), ita vt omnes valores ipsorum a, b, c determinare oporteat.

Methodus prima. Accipiantur pro a omnes numeri (tum positiue, tum negatiue) minores quam $2\sqrt{D}$ quorum residuum quadraticum D, et pro singulis a, ponatur b aequalis omni-

bus valoribus positiuis expr. $\sqrt{D}$ (mod. a) inter $\sqrt{D}$ et $\sqrt{D} \mp a$ iacentibus, c vero pro singulis valoribus determinatis ipsorum a, b, ponatur $= \frac{bb - D}{a}$. Si quae formae hoc modo oriuntur, in quibus $\pm a$ extra $\sqrt{D} + b$ et $\sqrt{D} - b$ situs est, reiiciendae sunt.

Methodus secunda. Accipiantur pro b omnes numeri positiui minores quam $\sqrt{D}$, pro singulis b resoluatur $bb - D$ omnibus quibus fieri potest modis in binos factores qui neglecto signo inter $\sqrt{D} + b$ et $\sqrt{D} - b$ iaceant, ponaturque alter $= a$, alter $= c$. Manifestum est, singulas resolutiones in factores praebere binas formas, quia vterque factor tum $= a$, tum $= c$ poni debet.

Ex. Sit $D = 79$ eruntque valores ipsius a viginti duo $\mp$ 1, 2, 3, 5, 6, 7, 9, 10, 13, 10, 15. Vnde inueniuntur formae vndeuiginti: (1, 8, — 15), (2, 7, — 15), (3, 8, — 5), (3, 7, — 10), (5, 8, — 3), (5, 7, — 6), (6, 7, — 5), (6, 5, — 9), (7, 4, — 9), (7, 3, — 10), (9, 5, — 6), (9, 4, — 7), (10, 7, — 3), (10, 3, — 7), (13, 1, — 6), (14, 3, — 5), (15, 8, — 1), (15, 7, — 2), (15, 2, — 5), totidemque aliae quae fiunt ex his si terminorum exterorum signa commutantur, puta (— 1, 8, 25), (— 2, 7, 15) etc. ita vt omnes triginta octo sint. Sed ex his reiiciendae sex ($\pm$ 13, 1, $\mp$ 6), ($\pm$ 14, 3, $\pm$ 5), ($\mp$ 15, 2, $\pm$ 5); reliquae triginta duae omnes reductas amplectuntur. Per methodum secundam eae-

dem forma prodeunt sequenti ordine*): $(\pm 7, 3, \mp 10)$, $(\pm 10, 3, \mp 7)$, $(\pm 7, 4, \mp 9)$, $(\pm 9, 4, \mp 7)$, $(\pm 6, 5, \mp 9)$, $(\pm 9, 5, \mp 6)$, $(\pm 2, 7, \mp 15)$, $(\pm 3, 7, \mp 10)$, $(\pm 5, 7, \mp 6)$, $(\pm 6, 7, \mp 5)$, $(\pm 10, 7, \mp 3)$ $(\pm 15, 7, \mp 2)$, $(\pm 1, 8, \mp 15)$, $(\pm 3, 8, \mp 5)$, $(\pm 5, 8, \mp 3)$, $(\pm 15, 8, \mp 1)$.

186. Sit F forma reducta determinantis D, ipsique ab vltimo parte contigua forma reducta F'; huic iterum ab vltima parte contigua reducta F''; reducta F''' ipsi F'' contigua ab vltima parte etc. Tum patet, omnes formas F', F'', F''' etc. esse prorsus determinatas, et tum inter se tum formae F proprie aequiualentes. Quoniam vero multitudo omnium formarum reductarum determinantis dati est finita, manifestum est, omnes formas in progressione infinita F, F', F'' etc. diuersas esse non posse. Ponamns F^m et F^{m+n} esse identicas, eruntque F^{m-1}, F^{m+n-1} reductae, eidem formae reductae a parte prima contiguae, adeoque identicae; hinc eodem modo F^{m-2} et F^{m+n-2} etc. tandemque F et F^n identicae erunt. Quare in progressione F, F', F'' etc., si modo satis longe continuatur, necessario tandem forma prima F recurret; et si supponimus F^n esse primam identicam cum F, siue omnes F', F''... F^{n-1} a forma F diuersas; facile perspicitur, omnes formas F, F', F''.... F^{n-1} diuersas fore.

*) Pro $b = 1$, — 78 in duos factores qui neglecto signo inter $\sqrt{79} + 1$ et $\sqrt{79} - 1$ iaceant, resolui nequit; quare hic valor est praetereundus, ex eademque ratione valores 2 et 6.

Complexum harum formarum vocabimus *periodum formae F*. Si igitur progressio vltra vltimam periodi formam producitur, eaedem formae F, F', F'' etc. iterum prodibunt, progressioque tota infinita F, F', F'' etc. constituta erit ex hac periodo formae F infinities repetita.

Progressio F, F', F'' etc. etiam retro continuari potest, praeponendo formae F reductam $'F$, quae ipsi a parte prima est contigua; huic iterum reductam $''F$, quae ipsi a prima parte contigua etc. Hoc modo habebitur progressio formarum *vtrimque* infinita

$$\ldots,\ '''F,\ ''F,\ 'F,\ F,\ F',\ F'',\ F''',\ldots$$

perspicieturque facile, $'F$ identicam fore cum F^{n-1}, $''F$ cum F^{n-2} etc. adeoque progressionem etiam a laeua parte e periodo formae F, infinities repetita, esse constitutam.

Si formis F, F', F'', etc. $'F$, $''F$ etc. tribuuntur indices 0, 1, 2 etc., — 1, — 2 etc. generaliterque formae F^m index m, formae ${}^mF$ index $-m$, patet, *formas quascunque seriei identicas fore vel diuersas, prout ipsarum indices congrui sint vel incongrui secundum modulum n.*

Ex. Periodus formae (3, 8, — 5) cuius determinans = 79, inuenitur haec: (3, 8 — 5) (— 5, 7, 6), (6, 5, — 9), (— 9, 4, 7), (7, 3, — 10), (— 10, 7, 3). Post vltimam iterum prodit (3, 8, — 5). Hic itaque $n = 6$.

187. Ecce quasdam obseruationes generales circa has periodos.

1) Si formae F, F', F'' etc.; $'F$, $''F$, $'''F$ etc. ita exhibetur: $(a, b, -a')$, $(-a', b', a'')$, $(a'', b'', -a''')$ etc.; $(-'a, 'b, a)$, $(''a, ''b, -'a)$, $(-'''a, '''b, ''a)$ etc: omnes a, a', a'', a''' etc. $'a$, $''a$, $'''a$ etc. *eadem signa* habebunt (art. 184, 1), omnes vero b, b', b'' etc. $'b$, $''b$, etc. erunt positiui.

2) Hinc manifestum est, numerum n (multitudinem formarum ex quibus periodus formae F constat) semper esse *parem*. Etenim terminus primus formae cuiusuis F^m ex hac periodo manifesto idem signum habebit vti terminus primus a formae F, si m est par, oppositum, si m est impar. Quare quum F^n et F identicae sint, n necessario erit par.

3) Algorithmus per quem numeri b', b'', b''' etc., a'', a''' etc. inueniuntur, ex art. 184, 6 est hic:

inter limites $\sqrt{D}$ et

$b' \equiv -b \pmod{a'}$	$\sqrt{D} \mp a'$	$a'' = \frac{D - b'b'}{a'}$
$b'' \equiv -b' \pmod{a''}$	$\sqrt{D} \mp a''$	$a''' = \frac{D - b''b''}{a''}$
$b''' \equiv -b'' \pmod{a'''}$	$\sqrt{D} \mp a'''$	$a^{IV} = \frac{D - b'''b'''}{a'''}$

etc.

vbi in columna secunda signa superiora vel inferiora sunt accipienda, prout a, a', a'' etc. sunt positiui vel negatiui. Loco formularum in co-

lumna tertia etiam sequentes adhiberi possunt, quae commodiores euadunt, quando D est numerus magnus:

$$a'' = \frac{b + b'}{a'}(b - b') + a$$
$$a''' = \frac{b' + b''}{a''}(b' - b'') + a'$$
$$a^{IV} = \frac{b + b''}{a'''}(b'' - b''') + a'' \text{ etc.}$$

4) Forma quaecunque F^m, in periodo formae F contenta, proprie eandem periodum habet vt F. Scilicet periodus illa erit F^m, F^{m+1} .... F^{n-1}, F, F'.... F^{m-1}, in qua eaedem formae eodemque ordine occurrunt, vt in periodo formae F, et quae ab hac tantummodo respectu initii et finis discrepat.

5) Hinc patet, omnes formas reductas eiusdem determinantis D in periodos *distribui* posse. Accipiatur aliqua harum formarum, F, ad libitum inuestigeturque ipsius periodus, F, F', F'' .... F^{n-1}, quam designemus per P. Si haec omnes formas reductas determinantis D nondum amplectitur, sit aliqua in ipsa non contenta G huiusque periodus Q. Tum patet P et Q nullam formam communem habere posse; alioquin enim etiam G in P contenta esse deberet periodique omnino coinciderent. Si P et Q omnes formas reductas nondum exhauriunt, aliqua ex deficientibus, H, periodum tertiam, R, suppeditabit, quae neque cum P neque cum Q formam communem habebit. Hoc modo continuare possumus, vsquedum omnes formae re-

ductae sint exhaustae. Ita *e. g.* omnes formae reductae determinantis 79 in sex periodos distribuuntur:

I. (1, 7, −15), (−15, 7, 2), (2, 7, −15), (−15, 8, 1).

II. (−1, 8, 15), (15, 7, −2), (−2, 7, 15), (15, 8, −1).

III. (3, 8, −5), (−5, 7, 6), (6, 5, −9), (−9, 4, 7), (7, 3, −10), (−10, 7, 3).

IV. (−3, 8, 5), (5, 7, −6), (−6, 5, 9), (9, 4, −7), (−7, 3, 10), (−10, 7, −3).

V. (5, 8, −3), (−3, 7, 10), (10, 3, −7), (−7, 4, 9), (9, 5, −6), (−6, 7, 5).

VI. (−5, 8, 3), (3, 7, −10), (−10, 3, 7), (7, 4, −9), (−9, 5, 6), (6, 7, −5).

6) Vocemus *formas socias*, quae ex iisdem terminis constant, sed ordine inuerso positis, vt $(a, b, -a')$, $(-a', b, a)$. Tum facile perspicitur ex art. 184, 7, si periodus formae reductae F sit $F, F', F'' \ldots F^{2n-1}$, formae F socia f formisque $F^{2n-1}, F^{2n-2} \ldots F'', F'$ resp. sociae sint formae $f', f'' \ldots f^{n-2}, f^{n-1}$: periodum formae f fore $f, f', f'' \ldots f^{n-2}, f^{n-1}$, adeoque ex totidem formis constare, vt periodum formae F. Periodos formarum sociarum vocabimus *periodos socias*. Ita in exemplo nostro sociae sunt periodi III et VI; IV et V.

7) Sed fieri etiam potest, vt forma f ipsa in periodo sociae suae F occurrat, vti in ex. nostro in periodo I et II, adeoque periodus

formae F cum periodo formae f conueniat, siue vt *periodus formae F sibi ipsi sit socia*. Quoties hoc euenit, in hac periodo duae formae ancipites inuenientur. Ponamus enim periodum formae F constare e $2n$ formis siue F et F^{2n} esse identicas; porro sit $2m+1$ index formae f in periodo formae F *), siue F^{2m+1} et F sociae. Tum patet etiam F' et F^{2m} fore socias nec non F'' et F^{2m-1} etc., adeoque etiam F^m et F^{m+1}. Sit $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Tum erit $b^m + b^{m+1} \equiv 0$, (mod. a^{m+1}); ex defin. formarum sociarum vero erit $b^m = b^{m+1}$ atque hinc $2b^{m+1} \equiv 0$ (mod. a^{m+1}), siue formae F^{m+1} anceps. — Eodem modo F^{2m+1} et F^{2n} erunt sociae; hinc F^{2m+2} et F^{2n-1}; F^{2m+3} et F^{2n-2} etc. tandemque F^{m+n} et F^{m+n+1}, quarum posterior erit anceps, vti per simile ratiocinium facile probatur. Quia vero $m+1$ et $m+n+1$ secundum mod. $2n$ sunt incongrui, formae F^{m+1} et F^{m+n+1} identicae non erunt (art. 186, vbi n idem denotat, quod hic $2n$). Ita in I sunt formae ancipites (1, 8, — 15), (2, 7, — 15), in II vero (— 1, 8, 15), (— 2, 7, 15).

8) Vice versa, *quaeuis periodus, in qua forma anceps occurrit, sibi ipsi socia est.* Facile enim perspicitur, si F^m sit forma reducta anceps: formam ipsi sociam, (quae etiam est reducta), simul ipsi a parte prima contiguam esse, i. e. F^{m-1} et F^m socias. Tum vero to-

*) Index hic necessario erit impar, quia manifesto termini primi formarum F, f signa opposita habent (*vid. supra*, 2).

ta periodus sibi ipsi socia erit. — Hinc patet, *fieri non posse, vt vnica tantum forma anceps in periodo aliqua contenta sit.*

9) Sed etiam *plures quam duae in eadem periodo esse nequeunt.* Ponamus enim in periodo formae F, ex $2n$ formis constante, tres formas ancipites dari F^λ, F^μ, F^ν, ad indices λ, μ, ν respectiue pertinentes, ita vt λ, μ, ν sint numeri inaequales inter limites 0 et $2n - 1$ (incl.) siti. Tum formae $F^{\lambda-1}$ et F^λ erunt sociae; similiterque $F^{\lambda-2}$ et $F^{\lambda+1}$ etc. tandemque F et $F^{2\lambda-1}$. Ex eadem ratione F et $F^{2\mu-1}$ sociae erunt, nec non F et $F^{2\nu-1}$; quare $F^{2\lambda-1}$, $F^{2\mu-1}$, $F^{2\nu-1}$ identicae, indicesque $2\lambda - 1$, $2\mu - 1$, $2\nu - 1$ secundum modulum $2n$ congrui erunt, et proin etiam $\lambda \equiv \mu \equiv \nu \pmod{n}$. *Q. E. A.* quia manifesto inter limites 0 et $2n - 1$ tres numeri diuersi secundum modulum n congrui iacere nequeunt.

188. Quum omnes formae ex eadem periodo proprie sint aequiualentes: quaestio oritur, annon etiam formae e periodis diuersis proprie aequiualentes esse possint. Sed antequam ostendamus, *hoc esse impossibile*, quaedam de transformatione formarum reductarum sunt exponenda.

Quoniam in sequentibus de formarum transformationibus persaepe agendum erit; vt prolixitatem quantum fieri potest euitemus, sequenti scribendi compendio abhinc semper vtemur. Si forma aliqua $LXX + 2MXY +$

NTT per substitutionem $X = \alpha x + \xi y$, $Y = \gamma x + \delta y$ in formam $lxx + 2mxy + nyy$ transformatur; simpliciter dicemus, (L, M, N) transformari in (l, m, n) per substitutionem $\alpha, \xi, \gamma, \delta$. Hoc modo opus non erit, indeterminatas formarum singularum, de quibus agitur, per signa propria denotare. — Palam vero est, indeterminatam *primam* a *secunda* in quauis forma probe distingui debere.

Proposita sit forma reducta $(a, b, -a')\ldots f$, determinantis D. Formetur simili modo vt in art. 186 progressio formarum reductarum vtrimque infinita, $\ldots\ {}''f, {}'f, f, f', f''\ldots$, et quidem sit $f' = (-a', b', a'')$, $f'' = (a'', b'', -a''')$ etc.; ${}'f = (-{}'a, {}'b, a)$, ${}''f = ({}''a, {}''b, -{}'a)$ etc. Ponatur $\frac{b+b'}{-a'} = h'$, $\frac{b'+b''}{a''} = h''$, $\frac{b''+b'''}{-a'''} = h'''$ etc.; $\frac{{}'b+b}{a} = h$, $\frac{{}''b+{}'b}{-{}'a} = {}'h$, $\frac{{}'''b+{}''b}{{}''a} = {}''h$ etc. Tum patet, si (vt in art. 177) numeri $\alpha', \alpha'', \alpha'''$ etc. ξ', ξ'', ξ''' etc. etc. formentur secundum algorithmum sequentem

$$\begin{array}{llll|llll}
\alpha' = 0 & \xi' = -1 & \gamma' = 1 & \delta' = h' \\
\alpha'' = \xi' & \xi'' = h''\xi' & \gamma'' = \delta' & \delta'' = h''\delta' - 1 \\
\alpha''' = \xi'' & \xi''' = h'''\xi'' - \xi' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\
\alpha^{IV} = \xi''' & \xi^{IV} = h^{IV}\xi''' - \xi'' & \gamma^{IV} = \delta''' & \delta^{IV} = h^{IV}\delta''' - \delta''
\end{array}$$

etc.

f transformatum iri

in	per substitutionem
f'	$\alpha', \xi', \gamma', \delta'$
f''	$\alpha'', \xi'', \gamma'', \delta''$
f'''	$\alpha''', \xi''', \gamma''', \delta'''$ etc.

omnesque has transformationes fore proprias.

Quum $'f$ transeat in f per substitutionem propriam 0, 1, 1, h (art. 161): f transibit in $'f$ per subst. propr. h, 1, — 1, 0. Ex simili ratione $'f$ transibit in $''f$ per subst. propr. $'h$, 1, — 1, 0; $''f$ in $'''f$ per subst. pr. $''h$, 1, — 1, 0 etc. Hinc per art. 159 eodem modo vt art. 177 colligitur, si numeri $'\alpha$, $''\alpha$, $'''\alpha$ etc. $'\mathfrak{C}$, $''\mathfrak{C}$, $'''\mathfrak{C}$ etc. etc. formentur secundum algorithmum sequentem

$'\alpha = h$	$'\mathfrak{C} = 1$	$'\gamma = -1$	$'\delta = 0$
$''\alpha = {}'h\,{}'\alpha - 1$	$''\mathfrak{C} = {}'\alpha$	$''\gamma = {}'h\,{}'\gamma$	$''\delta = {}'\gamma$
$'''\alpha = {}''h\,{}''\alpha - {}''\alpha$	$'''\mathfrak{C} = {}''\alpha$	$'''\gamma = {}''h\,{}''\gamma - {}'\gamma$	$'''\delta = {}''\gamma$
$^{\text{iv}}\alpha = {}'''h\,{}'''\alpha - {}'''\alpha$	$^{\text{iv}}\mathfrak{C} = {}'''\alpha$	$^{\text{iv}}\gamma = {}'''h\,{}'''\gamma - {}''\gamma$	$^{\text{iv}}\delta = {}'''\gamma$

etc.

f transformatum in

in	per substitutionem
$'f$	$'\alpha$, $'\mathfrak{C}$, $'\gamma$, $'\delta$
$''f$	$''\alpha$, $''\mathfrak{C}$, $''\gamma$, $''\delta$
$'''f$	$'''\alpha$, $'''\mathfrak{C}$, $'''\gamma$, $'''\delta$ etc.

omnesque has transformationes fore proprias.

Si ponitur $\alpha = 1$, $\mathfrak{C} = 0$, $\gamma = 0$, $\delta = 1$: hi numeri eandem relationem habebunt ad formam f, quam habent α', $\mathfrak{C}'$, γ', δ' ad f'; α'', $\mathfrak{C}''$, γ'', δ'' ad f'' etc.; $'\alpha$, $'\mathfrak{C}$, $'\gamma$, $'\delta$ ad $'f$ etc. Scilicet per substitutionem α, $\mathfrak{C}$, γ, δ forma f transibit in f. Tum vero progressiones infinitae α', α'', α''' etc., $'\alpha$, $''\alpha$, $'''\alpha$ etc., per intercalationem termini α, concinne iungentur ita vt vnam continuam vtrimque infinitam constituere concipi possint secundum eandem legem vbique pro-

gredientem ... $'''\alpha, ''\alpha, '\alpha, \alpha, \alpha', \alpha'', \alpha'''$ ... Lex progressionis haec est: $'''\alpha + '\alpha = ''h''\alpha$, $''\alpha + \alpha = 'h'\alpha$, $'\alpha + \alpha' = h\alpha$, $\alpha + \alpha'' = h'\alpha'$, $\alpha' + \alpha''' = h''\alpha''$ etc., siue generaliter (si indicem negatiuum a dextra scriptum idem designare supponimus, vt positiuum a laeua) $\alpha^{m-1} + \alpha^{m+1} = h^m \alpha^m$. Simili modo progressio ... $''\mathfrak{C}, '\mathfrak{C}, \mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ ... continua erit, cuius lex $\mathfrak{C}^{m-1} + \mathfrak{C}^{m+1} = h^{m+1}\mathfrak{C}^m$; et proprie cum praecedente identica, omnibus terminis vno loco promotis, $\mathfrak{C}'' = '\alpha$, $'\mathfrak{C} = \alpha$, $\mathfrak{C} = \alpha'$ etc. Lex progressionis continuae .... $''\gamma, '\gamma, \gamma, \gamma', \gamma''$ ..... erit haec $\gamma^{m-1} + \gamma^{m+1} = h^m\gamma^m$, et lex huius ... $''\delta, '\delta, \delta, \delta', \delta''$ ... erit $\delta^{m-1} + \delta^{m+1} = h^{m+1}\delta^m$ insuperque generaliter $\delta^m = \gamma^{m+1}$.

Ex. Sit forma proposita f haec (3, 8, — 5) quae transformabitur

	in formam	per substitutionem
^{VII}f	(— 10, 7, 3)	— 805, — 152, + 143, + 27
^{VI}f	(3, 8, — 5)	— 152, + 45, + 27, — 8
^{V}f	(— 5, 7, 6)	+ 45, + 17, — 8, — 3
^{IV}f	(6, 5, — 9)	+ 17, — 11, — 3, + 2
$''f$	(— 9, 4, 7)	— 11, — 6, + 2, + 1
$''f$	(7, 3, — 10)	— 6, + 5, + 1, — 1
$'f$	(— 10, 7, 3)	+ 5, + 1, — 1, 0
f	(3, 8, — 5)	+ 1, 0, 0, + 1
f'	(— 5, 7, 6)	0, — 1, + 1, — 3
f''	(6, 5, — 9)	— 1, — 2, — 3, — 7
f'''	(— 9, 4, 7)	— 2, + 3, — 7, + 10
f^{IV}	(7, 3, — 10)	+ 3, + 5, + 10, + 17
f^{V}	(— 10, 7, 3)	+ 5, — 8, + 17, — 27
f^{VI}	(3, 8, — 5)	— 8, — 45, — 27, — 152
f^{VII}	(— 5, 7, 6)	— 45, + 143, — 152, + 483

etc.

189. Circa hunc algorithmum sequentia sunt annotanda.

1) Omnes a, a' a'' etc., $'a$, $''a$ etc. eadem signa habebunt; omnes b, b', b'' etc. $'b$, $''b$ etc. erunt positiui; in progressione .... $''h$, $'h$, h, h', h'' ... signa alternabunt, scilicet si omnes a, a' etc. sunt positiui, h^m vel ${}^m h$ erit positiuus quando m est par, negatiuus quando m impar; si vero a, a' etc. sunt negatiui, h^m vel ${}^m h$ pro m pari erit negatiuus, pro impari positiuus.

2) Si a est positiuus adeoque h' negatiuus, h'' positiuus etc., erit $\alpha'' = -1$ neg., $\alpha''' = h''\alpha''$ neg. et $> \alpha''$ (vel $= \alpha''$ si $h'' = 1$); $\alpha^{IV} = h'''\alpha'''$ — " pos. et $> \alpha'''$ (quia $h'''\alpha'''$ pos., α'' neg); $\alpha^V = h^{IV}\alpha^{IV}$ — α''' pos. et $> \alpha^{IV}$ (quia $h^{IV}\alpha^{IV}$ pos.) etc. Hinc facile concluditur, progressionem α', α'', α''' etc. in infinitum crescere duoque signa positiua semper duo negatiua excipere ita vt α^m habeat signum $+$, $+$, $-$, $-$ prout $m \equiv 0, 1, 2, 3 \pmod 4$. — Si a est negatiuus, per simile ratiocinium inuenitur α'' neg., α''' pos. et vel $>$ vel $= \alpha''$; α^{IV} pos. $> \alpha'''$; α^V neg. $> \alpha^{IV}$ etc., ita vt progressio α', α'', α''' etc. continuo crescat, signumque termini α^m sit $+$, $-$, $-$, $+$ prout $m \equiv 0, 1, 2, 3 \pmod 4$

3) Hoc modo inuenitur, omnes quatuor progressiones infinitas α', α'', α''' etc. γ, γ', γ'' etc.; α', α, $'\alpha$, $''\alpha$ etc.; γ, $'\gamma$, $''\gamma$ etc. continuo crescere, adeoque etiam sequentes cum illis identicas: ε, ε', ε'' etc.; $'\delta$, δ, δ', δ'' etc.; ζ, $'\zeta$, $''\zeta$ etc.; $'\delta$, $''\delta$ etc.; et, prout $m \equiv 0, 1, 2, 3 \pmod 4$,

signum ipsius α^m $+ \pm - \mp$; ipsius $\mathfrak{C}^m$, $\pm \mp$, $- \mp +$; ipsius γ^m, $\pm + \mp -$; ipsius δ^m, $+ \mp - \pm$; ipsius ${}^m\alpha$, $+ \pm - \mp$; ipsius ${}^m\mathfrak{C}$, $\mp + \pm -$; ipsius ${}^m\gamma$, $\mp - \pm +$; ipsius ${}^m\delta$ $+ \mp - \pm$, valentibus superioribus quando a est positiuus, inferioribus quando a negatiuus. Teneatur imprimis haec proprietas: Designante m indicem quemcunque positiuum, α^m et γ^m habebunt eadem signa quando a positiuus, opposita quando a negatiuus, similiterque $\mathfrak{C}^m$ et δ^m contra; ${}^m\alpha$ et ${}^m\gamma$, vel ${}^m\mathfrak{C}$ et ${}^m\delta$ habebunt eadem signa quando a negatiuus, opposita quando a positiuus.

4) In signis art. 32 magnitudo ipsorum α^m etc. concinne ita exhiberi potest, ponendo $\mp h' = k'$, $\pm h'' = k''$, $\mp h''' = k'''$ etc. $\pm h = k$, $\mp {}'h = {}'k$, $\pm {}''h = {}''k$ etc. ita vt omnes k', k'' etc. k, ${}'k$ etc. sint numeri positiui: $\alpha^m = \pm [k'', k''', k^{IV} \ldots k^{m-1}]$; $\mathfrak{C}^m = \pm [k'', k''' k^{IV} \ldots k^m]$; $\gamma^m = \pm [k', k'', k''' \ldots k^{m-1}]$; $\delta^m = \pm [k', k'', k''' \ldots k^m]$; ${}^m\alpha = \mp [k, {}'k, {}''k \ldots {}^{m-1}k]$; ${}^m\mathfrak{C} = \pm [k, {}'k, {}''k \ldots {}^{m-2}k]$; ${}^m\gamma = \pm [{}'k, {}''k \ldots {}^{m-1}k]$; ${}^m\delta = \pm [{}'k, {}''k \ldots {}^{m-2}k]$; *signa* vero ad praecepta modo tradita determinari debent. Secundum has formulas, quarum demonstrationem propter facilitatem omittimus, calculus semper expeditissime absolui poterit.

190. Lemma. *Designantibus m, μ, m', n, ν, n' numeros integros quoscunque, ita tamen vt trium posteriorum nullus sit $= 0$: dico, si $\frac{\mu}{\nu}$ iaceat inter limites $\frac{m}{n}$ et $\frac{m'}{n'}$ exclusiue, atque sit $mn' - nm' = \mp 1$, denominatorem ν fore maiorem quam n et n'.*

Dem. Manifesto $\mu nn'$ iacebit inter $\nu mn'$ et $\nu nm'$, adeoque ab vtroque limite minus differet quam limes alter ab altero, i. e. erit $\nu mn' - \nu nm > \mu nn' - \nu mn'$ et $> \mu nn' - \nu nm'$, siue $\nu > n'(\mu n - \nu m)$ et $> n(\mu n' - \nu m')$. Hinc sequitur, quoniam $\mu n - \nu m$ certe non $= 0$ (alioquin enim foret $\frac{\mu}{\nu} = \frac{m}{n}$ contra hyp.), neque $\mu n' - \nu m' = 0$ (ex simili ratione), sed vterque ad minimum $= 1$, fore $\nu > n'$ et $> n$. *Q. E. D.*

Perspicuum itaque est, ν non posse esse $= 1$, i. e. si fuerit $mn' - nm' = \pm 1$, inter fractiones $\frac{m}{n}, \frac{m'}{n'}$ nullum numerum integrum iacere posse. Quare etiam cifra inter ipsas iacere nequit, i. e. fractiones istae signa oppositа habere nequeunt.

191. Theorema. *Si forma reducta* $(a, b, -a')$ *determinantis* D *per substitutionem* $\alpha, \beta, \gamma, \delta$ *transit in reductam* $(A, B, -A')$ *eiusdem determinantis: iacebit*, primo, $\frac{\pm\sqrt{D}-b}{a}$ *inter* $\frac{\alpha}{\gamma}$ *et* $\frac{\beta}{\delta}$ *(siquidem neque* γ *neque* $\delta = 0$, *i. e. si vterque limes est finitus), accepto signo superiori, quando neuter horum limitum habet signum signo ipsius* a *oppositum (siue clarius, quando aut vterque idem habet, aut alter idem, alter est* $= 0$*), inferiori quando neuter habet idem vt* a; secundo $\frac{\pm\sqrt{D}+b}{a'}$ *inter* $\frac{\gamma}{\alpha}$ *et* $\frac{\delta}{\beta}$ *(siquidem neque* α *neque* $\beta = 0$*), signo superiori accepto quando limes neuter signum signo ipsius* a' *(vel* a*) oppositum habet, inferiori quando neuter habet idem vt* a' **).*

*) Manifestum est, alios casus locum habere non posse, quum ex art. praec. propter $\alpha\delta - \beta\gamma = \pm 1$, limites bini neque signa oppositа habere, neque simul $= 0$ esse possint.

Dem. Habentur aequationes $aαα + 2bαγ - a'γγ = A$.... [1]; $aγγ + 2bγδ - a'δδ = -A'$... [2]. Vnde deducitur

$$\frac{α}{γ} = \frac{\pm\sqrt{(D + \frac{aA}{γγ})} - b}{a} \quad \text{[3]}$$

$$\frac{γ}{δ} = \frac{\pm\sqrt{(D - \frac{aA'}{δδ})} - b}{a} \quad \text{[4]}$$

$$\frac{γ}{α} = \frac{\pm\sqrt{(D - \frac{aA'}{αα})} \mp b}{a'} \quad \text{[5]}$$

$$\frac{δ}{γ} = \frac{\pm\sqrt{(D + \frac{a'A}{γγ})} \mp b}{a'} \quad \text{[6]}.$$

Aequatio 3, 4, 5, 6 reiicienda erit, si $γ$, $δ$, $α$, $γ$ resp. $= 0$. — Sed dubium hic manet, quae *signa* quantitatibus radicalibus tribui debeant; hoc sequenti modo decidemus.

Statim patet in [3] et [4] necessario signa superiora accipi debere, quando neque $\frac{α}{γ}$ neque $\frac{γ}{δ}$ signum habeat signo ipsius a oppositum; quoniam accepto signo inferiori $\frac{aα}{γ}$ et $\frac{aγ}{δ}$ fierent quantitates negatiuae. Quia vero A et A' signa eadem habent, $\sqrt{D}$ cadet inter $\sqrt{(D + \frac{aA}{γγ})}$ et $\sqrt{(D - \frac{aA'}{δδ})}$ adeoque in hocce casu $\frac{\sqrt{D} - b}{a}$

inter $\frac{\alpha}{\gamma}$ et $\frac{\epsilon}{\delta}$. Quare pars prima theorematis pro casu priori est demonstrata.

Eodem modo perspicitur, in [5] et [6] necessario signa inferiora accipi debere, quando neque $\frac{\gamma}{\alpha}$ neque $\frac{\delta}{\epsilon}$ signum idem habeant vt a' siue a, quia accepto superiori $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\epsilon}$ necessario fierent quantitates positiuae. Vnde protinus sequitur $\frac{-\sqrt{D}+b}{a'}$ pro hocce casu iacere inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\epsilon}$. Demonstrata est itaque etiam pars secunda theorematis pro casu posteriori. Quodsi aeque facile ostendi posset, in [3] et [4] signa inferiora accipi debere, quando neutra quantitatum $\frac{\alpha}{\gamma}$, $\frac{\epsilon}{\delta}$ signum idem habeat vt a, et in [5] et [6] superiora, quando neque $\frac{\gamma}{\alpha}$ neque $\frac{\delta}{\epsilon}$ signum oppositum habeat: hinc simili modo sequeretur, pro illo casu $\frac{-\sqrt{D}-b}{a}$ iacere inter $\frac{\alpha}{\gamma}$ et $\frac{\epsilon}{\delta}$, pro hoc $\frac{\sqrt{D}+b}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\epsilon}$, siue pars prima theorematis etiam pro casu posteriori, et secunda pro casu priori demonstratae forent. Sed quum illud difficile quidem non sit, attamen sine quibusdam ambagibus fieri nequeat, methodum sequentem praeferimus.

Quando nullus numerorum α, ϵ, γ, $\delta = 0$, $\frac{\alpha}{\gamma}$ et $\frac{\epsilon}{\delta}$ eadem signa habebunt vt $\frac{\gamma}{\alpha}$, $\frac{\delta}{\epsilon}$. Quan-

do itaque neutra harum quantitatum signum idem habet vt a' siue a, adeoque $\frac{-\sqrt{D+b}}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\epsilon}$ cadit: neutra quantitatum $\frac{\alpha}{\gamma}$, $\frac{\epsilon}{\delta}$ signum idem vt a habebit, cadetque $\frac{a'}{-\sqrt{D+b}} = \frac{-\sqrt{D-b}}{a}$ (propter $aa' = D - bb$) inter $\frac{\alpha}{\gamma}$ et $\frac{\epsilon}{\delta}$. Quare pro eo casu vbi neque α neque $\epsilon = 0$, pars prima theor. etiam pro casu secundo est demonstrata (nam conditio vt neque γ neque $\delta = 0$, iam in theor. ipso est adiecta). Simili modo, quando nullus numerorum α, ϵ, γ, $\delta = 0$, et neque $\frac{\alpha}{\gamma}$ neque $\frac{\epsilon}{\delta}$ signum signo ipsius a vel a' oppositum habet, adeoque $\frac{\sqrt{D-b}}{a'}$ inter $\frac{\alpha}{\gamma}$ et $\frac{\epsilon}{\delta}$ iacet: etiam $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\epsilon}$ signum oppositum signo ipsius a' non habebit, cadetque $\frac{a}{\sqrt{D-b}} = \frac{\sqrt{D+b}}{a'}$ inter $\frac{\gamma}{\alpha}$ et $\frac{\delta}{\epsilon}$. In eo igitur casu vbi neque γ neque $\delta = 0$ pars secunda theor. etiam pro casu secundo est demonstrata.

Nihil itaque superesset quam vt demonstretur, partem primam theor. etiam pro casu secundo locumhabere si alteruter numerorum α, ϵ sit $= 0$, et partem secundam pro casu primo si aut γ aut $\delta = 0$; At *omnes hi casus sunt impossibiles.* Supponamus enim, pro parte *prima* theor., esse neque γ neque $\delta = 0$, $\frac{\alpha}{\gamma}, \frac{\epsilon}{\delta}$ non habere signum idem vt a atque esse 1) $\alpha = 0$. Tum ex aequ. $\alpha\delta - \epsilon\gamma = \pm 1$ fit $\epsilon =$

± 1, $\gamma = \pm 1$. Hinc ex [1] $A = -a'$, quare A et a', adeoque etiam a et A' signa opposita habent, vnde fit $\sqrt{(D - \frac{aA'}{\delta\delta})} > \sqrt{D} > b$. Hinc patet in [4] necessario signum inferius accipi debere, quia accepto superiori $\frac{\epsilon}{\delta}$ manifesto signum idem obtineret vt a. Fit itaque $\frac{\epsilon}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$ (propter $a < \sqrt{D} + b$ ex def. formae reductae), *Q. E. A.* quum $\epsilon = \pm 1$, et δ non $= 0$. — 2). Sit $\epsilon = 0$. Tum ex aequ. $\alpha\delta - \epsilon\gamma = \pm 1$ fit $\alpha = \pm 1$, $\delta = \pm 1$. Hinc ex [2] $-A' = -a'$, quare a et a et A signa eadem habebunt, vnde fit $\sqrt{(D + \frac{aA}{aa})} > \sqrt{D} > b$. Hinc patet in [3] signum inferius accipi debere, quia accepto superiori $\frac{\alpha}{\gamma}$ signum idem obtineret vt a. Fit itaque $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, *Q. E. A.* eadem ratione vt ante. — Pro parte *secunda* si supponimus neque α, neque $\epsilon = 0$; $\frac{\gamma}{\alpha}$, $\frac{\delta}{\epsilon}$ non habere signum signo ipsius a' oppositum atque 1) $\gamma = 0$: ex aequ. $\alpha\delta - \epsilon\gamma = \pm 1$ fit $\alpha = \pm 1$, $\delta = \pm 1$. Hinc ex [1] $A = a$, quare a' et A' signa eadem habebunt, vnde fit $\sqrt{(D + \frac{a'A'}{\epsilon\epsilon})} > \sqrt{D} > b$. Quocirca in [6] signum superius erit accipiendum, quia accepto inferiori, $\frac{\delta}{\epsilon}$ obtineret signum oppositum signo ipsius a'. Fit igitur $\frac{\delta}{\epsilon} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.*, quia $\delta = \pm 1$ et

γ non $= 0$. Tandem 2) si esset $\delta = 0$, ex $\alpha\delta - \beta\gamma = \pm 1$ fit $\beta = \pm 1$, $\gamma = \pm 1$, adeoque ex [2] $- A' = a$. Hinc $\sqrt{(D - \frac{a'A}{\alpha\alpha})} > \sqrt{D} > b$, quare in [5] signum superius accipiendum. Hinc $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.* — Quare theorema in omni sua extensione est demonstratum.

Quum differentia inter $\frac{\alpha}{\gamma}$ et $\frac{\beta}{\delta}$ sit $= \frac{1}{\gamma\delta}$: differentia inter $\frac{\pm\sqrt{D} - b}{a}$ et $\frac{\alpha}{\gamma}$ vel $\frac{\beta}{\delta}$ erit $< \frac{1}{\gamma\delta}$; inter $\frac{\pm\sqrt{D} - b}{a}$ autem et $\frac{\alpha}{\gamma}$, vel inter illam quantitatem et $\frac{\beta}{\delta}$ nulla fractio iacere poterit, cuius denominator non sit maior quam γ aut δ (*lemma praec.*). — Eodem modo differentia quantitatis $\frac{\pm\sqrt{D} + b}{a}$ a fractione $\frac{\gamma}{\alpha}$ vel hac $\frac{\delta}{\beta}$ erit minor quam $\frac{1}{\alpha\beta}$, et inter illam quantitatem et neutram harum fractionum iacere potest fractio cuius denominator non sit maior quam α et β.

192. Ex applicatione theor. praec. ad algorithmum art. 188 sequitur, quantitatem $\frac{\sqrt{D} - b}{a}$ quam per L designabimus, iacere inter $\frac{\alpha'}{\gamma'}$ et $\frac{\beta'}{\delta'}$; inter $\frac{\alpha''}{\gamma''}$ et $\frac{\beta''}{\delta''}$; inter $\frac{\alpha'''}{\gamma'''}$ et $\frac{\beta'''}{\delta'''}$ etc. (facile enim ex art. 189, 3 fin. deducitur, nullum horum limitum habere signum oppositum

signo ipsius a; quare quantitati radicali $\sqrt{D}$ signum positiuum tribui debet) siue inter $\frac{\alpha'}{\gamma'}$ et $\frac{\alpha''}{\gamma''}$; inter $\frac{\alpha''}{\gamma''}$ et $\frac{\alpha'''}{\gamma'''}$ etc. Omnes itaque fractiones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha^{V}}{\gamma^{V}}$ etc. ipsi L ab eadem parte iacebunt, omnesque $\frac{\alpha''}{\gamma''}$, $\frac{\alpha^{IV}}{\gamma^{IV}}$, $\frac{\alpha^{VI}}{\gamma^{VI}}$ etc. a parte altera. Quoniam vero $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ iacebit *extra* $\frac{\alpha'''}{\gamma'''}$ et L, similique ratione $\frac{\alpha''}{\gamma''}$ extra L et $\frac{\alpha^{IV}}{\alpha^{IV}}$; $\frac{\alpha'''}{\gamma'''}$ extra L et $\frac{\alpha^{V}}{\gamma^{V}}$ etc. Vnde manifestum est, has quantitates iacere sequenti ordine: $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha^{V}}{\gamma^{V}}$ ... L ... $\frac{\alpha^{VI}}{\gamma^{VI}}$, $\frac{\alpha^{IV}}{\gamma^{IV}}$, $\frac{\alpha''}{\gamma''}$. Differentia autem inter $\frac{\alpha'}{\gamma'}$ et L erit minor quam differentia inter $\frac{\alpha'}{\gamma'}$ et $\frac{\alpha''}{\gamma''}$ *i. e.* $< \frac{1}{\gamma'\gamma''}$, similique ratione differentia inter $\frac{\alpha''}{\gamma''}$ et L erit $< \frac{1}{\gamma''\gamma'''}$ etc. Quamobrem fractiones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$ etc. continuo proprius ad limitem L accedunt, et quoniam γ', γ'', γ''' continuo in infinitum crescunt, differentia fractionum a limite quauis quantitate data minor fieri potest.

Ex art. 189 nulla quantitatum $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$ etc. signum idem habebit vt a; hinc per ratiocinia praecedentibus omnino similia sequitur,

illas et hanc $\frac{-\sqrt{D}+b}{a'}$, quam per L designabimus, iacere sequenti ordine: $\frac{\gamma}{\alpha}$, $\frac{''\gamma}{''\alpha}$, $\frac{^{IV}\gamma}{^{IV}\alpha}$..... L'..... $\frac{^{V}\gamma}{^{V}\alpha}$, $\frac{'''\gamma}{'''\alpha}$, $\frac{'\gamma}{'\alpha}$. Differentia autem inter $\frac{\gamma}{\alpha}$ et L' minor erit quam $\frac{1}{'\alpha\alpha}$, differentia inter $\frac{'\gamma}{'\alpha}$ et L minor quam $\frac{1}{''\alpha'\alpha}$ etc. Quare fractiones $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$ etc. continuo proprius ad L' accedent, et differentia quauis quantitate data minor fieri poterit.

In ex. *art.* 188. fit $L = \frac{\sqrt{79}-8}{3} = 0{,}2960648$ et fractiones appropinquantes $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$ etc. Est autem $\frac{143}{483} = 0{,}2960662$. — Ibidem fit $L' = \frac{-\sqrt{79}+8}{5} = -0{,}1776388$. fractionesque approximantes $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$ $-\frac{8}{45}$, $-\frac{27}{152}$ $-\frac{143}{805}$ etc. Est vero $\frac{143}{805} = 0{,}1776397$.

193. Theorema. *Si formae reductae f, F proprie aequiualentes sunt: altera in alterius periodo contenta erit.*

Sit $f = (a, b, -a')$, $F = (A, B, -A')$, determinans harum formarum D, transeatque illa in hanc per substitutionem propriam $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$. Tum dico, si periodus formae f quaeratur progressioque vtrimque infinita formarum reductarum atque transformationum for-

mae f in ipsas eruatur, eodem modo vt art. 188: *vel* $+\mathfrak{A}$ fore aequalem termino alicui progressionis $\ldots {}''\alpha, {}'\alpha, \alpha, \alpha', \alpha'' \ldots$, hocque posito $= \alpha^m$, $+\mathfrak{B}$ fore $= \beta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$; *vel* $-\mathfrak{A}$ fore aequalem termino alicui α^m, et $-\mathfrak{B}, -\mathfrak{C}, -\mathfrak{D}$ resp. $= \varepsilon^m, \gamma^m, \delta^m$ (vbi m etiam indicem negatiuum designare potest). In vtroque casu F manifesto identica erit cum f^m.

Dem. I. Habentur quatuor aequationes, $a\mathfrak{A}\mathfrak{A} + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}\mathfrak{C} = A \ldots$ [1], $a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B \ldots$ [2], $a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D} = -A' \ldots$ [3]; $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1 \ldots$ [4]. Consideramus autem *primo* casum, vbi aliquis numerorum $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D} = 0$.

1° Si $\mathfrak{A} = 0$, fit ex [4] $\mathfrak{B}\mathfrak{C} = -1$, adeoque $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Hinc ex [1], $-a' = A$; ex [2], $-b \pm a'\mathfrak{D} = B$ siue $B \equiv -b$ (mod. a' vel A); vnde sequitur formam $(A, B, -A')$ formae $(a, b, -a')$ ab vltima parte contiguam esse. Quoniam vero illa est reducta, necessario cum f' identica erit. Ergo $B = b'$, adeoque ex [2] $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; hinc propter $\frac{b+b'}{-a'} = h'$, fit $\mathfrak{D} = \mp h'$. Vnde colligitur, $\mp\mathfrak{A}, \mp\mathfrak{B}, \mp\mathfrak{C}, \mp\mathfrak{D}$ esse resp. $= 0, -1, +1, h'$ siue $= \alpha', \beta', \gamma', \delta'$.

2° Si $\mathfrak{B} = 0$, fit ex [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; ex [3] $a' = A'$; ex [2] $b \mp a'\mathfrak{C} = B$, siue $b \equiv B$ (mod. a). Quoniam vero tum f tum F sunt formae reductae: tum b tum B ia-

cebunt inter $\sqrt{D}$ et $\sqrt{D} \pm a'$ (prout a' pos. vel neg., art. 185, 5). Quare erit necessario $b = B$, et $\mathfrak{C} = 0$. Hinc formae f, F sunt identicae atque $\pm \mathfrak{A}$, $\pm \mathfrak{B}$, $\pm \mathfrak{C}$, $\pm \mathfrak{D} = 1, 0, 0, 1 = \alpha, ^{\mathfrak{C}}, \gamma, ^{\delta}$ (resp.).

3° Si $\mathfrak{C} = 0$, fit ex [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; ex [1] $a = A$; ex [2] $\pm a\mathfrak{B} + b = B$ siue $b \equiv B \pmod{a}$. Quia vero tum b tum B iacent inter $\sqrt{D}$ et $\sqrt{D} \mp a$: erit necessario $B = b$ et $\mathfrak{B} = 0$. Quare casus hic a praecedente non differt.

4° Si $\mathfrak{D} = 0$, fit ex [4] $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; ex [3] $a = -A'$; ex [2] $\pm a\mathfrak{A} - b = B$ siue $B \equiv -b \pmod{a}$. Hinc forma F formae f a parte prima contigua erit, et proin cum forma $'f$ identica. Quare propter $\frac{'b+b}{a} = h$, et $B = 'b$, erit $\pm \mathfrak{A} = h$. Vnde colligitur $\pm \mathfrak{A}$, $\pm \mathfrak{B}$, $\pm \mathfrak{C}$, $\pm \mathfrak{D}$ resp. esse $= h$, 1, -1, 0, $= '\alpha, '\mathfrak{C}, '\gamma, '\delta$.

Superest itaque casus vbi nullus numerorum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D} = 0$. Hic per Lemma art. 190 quantitates $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$, $\frac{\mathfrak{D}}{\mathfrak{B}}$ idem signum habebunt, oriunturque inde duo casus, quum signum hoc vel cum signo ipsorum a, a' conuenire vel ipsi oppositum esse possit.

II. Si $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ idem signum habent vt a: quantitas $\frac{\sqrt{D}-b}{a}$ (quam designabimus per L)

inter has fractiones sita erit (art. 191). Demonstrabimus iam, $\frac{\mathfrak{A}}{\mathfrak{B}}$ aequalem fore alicui fractionum $\frac{\alpha''}{\gamma''}, \frac{\alpha'''}{\gamma'''}, \frac{\alpha^{IV}}{\gamma^{IV}}$ etc., atque $\frac{\mathfrak{B}}{\mathfrak{D}}$ proxime sequenti, scilicet si $\frac{\mathfrak{A}}{\mathfrak{C}}$ fuerit $= \frac{\alpha^m}{\gamma^m}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ fore $= \frac{\alpha^{m+1}}{\gamma^{m+1}}$. In art. praec. ostendimus, quantitates $\frac{\alpha'}{\gamma'}, \frac{\alpha''}{\gamma''}, \frac{\alpha'''}{\gamma'''}$ etc., (quas breuitatis gratia per (1), (2), (3) etc. denotabimus) atque L, hunc ordinem (I): obseruare (1), (3), (5)... L... (6), (4), (2); prima harum quantitatum est $= 0$ (propter $\alpha' = 0$), reliquae omnes idem signum habent vt L siue a. Quoniam vero per hyp. $\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{D}}$ (pro quibus scribemus $\mathfrak{M}$, $\mathfrak{N}$) idem signum habent: patet has quantitates ipsi (1) a dextra iacere (aut si mauis ab eadem parte a qua L), et quidem, quum L iaceat inter ipsas, alteram ipsi L a dextra, alteram a laeua. Facile vero ostendi potest, $\mathfrak{M}$ ipsi (2) a dextra iacere non posse alioquin enim $\mathfrak{N}$ iaceret inter (1) et L, vnde sequeretur *primo* (2) iacere inter $\mathfrak{M}$ et $\mathfrak{N}$, adeoque denominatorem fractionis (2) maiorem esse denominatore fractionis $\mathfrak{N}$ (art. 190), *secundo* $\mathfrak{M}$ iacere inter (1) et (2), adeoque denom. fractionis $\mathfrak{N}$ esse maiorem quam denom. fractionis (2), *Q. E. A.*

Supponamus $\mathfrak{M}$ nulli fractionum (2), (3), (4) etc. aequalem esse, vt, quid inde sequatur, videamus. Tum manifestum est, si fractio $\mathfrak{M}$ ips-

L a laeua iaceat, necessario eam sitam esse aut inter (1) et (3), aut inter (3) et (5), aut inter (5) et (7) etc. (quoniam L est irrationalis, adeoque ipsi $\mathfrak{M}$ certo inaequalis, fractionesque (1), (3), (5) etc. quauis quantitate data, ipsi L inaequali, propius ad L accedere possunt). Si vero $\mathfrak{M}$ ipsi L a dextra iacet: necessario iacebit aut inter (2) et (4), aut inter (4) et (6) aut inter (6) et (8) etc. Ponamus itaque $\mathfrak{M}$ iacere inter (m) et $(m+2)$, patetque quantitates $\mathfrak{M}$, (m), $(m+1)$, $(m+2)$, L iacere sequenti ordine, (II)*): (m), $(\mathfrak{M})$, $(m+2)$, L, $(m+1)$. Tum erit necessario $\mathfrak{N} = (m+1)$. Iacebit enim $\mathfrak{N}$ ipsi L a dextra; si vero etiam ipsi $(m+1)$ a dextra iaceret, $(m+1)$ iaceret inter $\mathfrak{M}$ et $\mathfrak{N}$, vnde $\gamma^{m+1} > \mathfrak{C}$, $\mathfrak{M}$ vero inter (m) et $(m+1)$ vnde $\mathfrak{C} > \gamma^{m+1}$ (art. 190), *Q. E. A.*; si vero $\mathfrak{N}$ ipsi $(m+1)$ a laeua iaceret, siue inter $(m+2)$ et $(m+1)$, foret $\mathfrak{D} > \gamma^{m+2}$, et quia $(m+2)$ inter $\mathfrak{M}$ et $\mathfrak{N}$, foret $\gamma^{m+2} > \mathfrak{D}$, *Q. E. A.* Erit itaque $\mathfrak{N} = (m+1)$, siue

$$\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}} = \frac{\mathfrak{E}^m}{\mathfrak{d}^m}$$

Quia $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, $\mathfrak{B}$ erit primus ad $\mathfrak{D}$ et ex simili ratione $\mathfrak{E}^m$ primus ad $\mathfrak{d}^m$. Vnde facile perspicitur aequationem $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\mathfrak{E}^m}{\mathfrak{d}^m}$ consistere non posse, nisi fuerit aut $\mathfrak{B} = \mathfrak{E}^m$, $\mathfrak{D} = \mathfrak{d}^m$, aut $\mathfrak{B} = -\mathfrak{E}^m$, $\mathfrak{D} = -\mathfrak{d}^m$. Iam

*) Nihil hic refert, siue ordo in (II) idem sit vt in (I), siue huic oppositus, *i. e.* siue (m) etiam in (I) ipsi L a laeua iaceat siue a dextra.

quum forma f per substitutionem propriam α^m, γ^m, δ^m in formam f^m transmutetur, quae est $(\pm a^m, b^m, \mp a^{m+1})$: habebuntur aequationes $a\alpha^m\alpha^m + 2b\alpha^m\gamma^m - a'\gamma^m\gamma^m = \mp a^m$ ... [5]; $a\alpha^m\gamma^m + b(\alpha^m\delta^m + \gamma^m\gamma^m) - a'\gamma^m\delta^m = b^m$ ... [6]; $a\gamma^m\gamma^m + 2b\gamma^m\delta^m - a'\delta^m\delta^m = \mp a^{m+1}$ ... [7]; $\alpha^m\delta^m - \gamma^m\gamma^m = 1$ ... [8]. Hinc fit: (ex aequ. 7 et 3), $\mp a^{m+1} = -A'$. Porro multiplicando aequationem [2] per $\alpha^m\delta^m - \gamma^m\gamma^m$, aequationem [6] per $\mathfrak{AD} - \mathfrak{BC}$ et subtrahendo facile per euolutionem confirmatur esse $B - b^m = (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\gamma^m + b(\mathfrak{D}\gamma^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m) + (\mathfrak{B}\delta^m - \mathfrak{D}\gamma^m)(a\mathfrak{A}\alpha^m + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m)$ ... [9] siue quoniam vel $\gamma^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$ vel $\gamma^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$), $B - b^m = \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D}) = \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A'$. Hinc $B \equiv b^m \pmod{A'}$; quia vero tum B tum b^m, inter $\sqrt{D}$ et $\sqrt{D} \mp A'$ iacent, necessario erit $B = b^m$ adeoque $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$, siue $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$, *i. e.* $\mathfrak{M} = (m)$.

Hoc modo itaque ex suppositione, $\mathfrak{M}$ nulli quantitatum (2), (3), (4) etc. aequalem esse, deduximus, eam reuera alicui aequalem esse. Quodsi vero ab initio supponimus, esse $\mathfrak{M} = (m)$, manifesto erit vel $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$, vel $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. In vtroque casu fit ex [1] et [5] $A = \pm a^m$, et ex [9] $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\gamma^m)A$, siue $B \equiv b^m \pmod{A}$. Hinc simili modo vt supra concluditur $B = b^m$, et hinc $\mathfrak{B}\delta^m = \mathfrak{D}\gamma^m$; quare

quum $\mathfrak{B}$ ad $\mathfrak{D}$ primus sit et $\mathfrak{C}^m$ ad $\mathfrak{d}^m$: erit aut $\mathfrak{B} = \mathfrak{C}^m$, $\mathfrak{D} = \mathfrak{d}^m$ aut $-\mathfrak{B} = \mathfrak{C}^m$, $-\mathfrak{D} = \mathfrak{d}^m$, et proin ex [7] $-A' = \mp a^{m+1}$. Quamobrem formae F, f^m identicae erunt. Adiumento aequationis $\mathfrak{AD} - \mathfrak{BC} = \alpha^m \mathfrak{d}^m - \mathfrak{C}^m \gamma^m$ autem nullo negotio probatur, poni debere $+\mathfrak{B} = \mathfrak{C}^m$, $+\mathfrak{D} = \mathfrak{d}^m$, quando $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$; contra $-\mathfrak{B} = \mathfrak{C}^m$, $-\mathfrak{D} = -\mathfrak{d}^m$, quando $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. *Q. E. D.*

III. Si signum quantitatum $\frac{\mathfrak{A}}{\mathfrak{C}}$ signo ipsius a oppositum: demonstratio praecedenti tam similis est, vt praecipua tantum momenta addigitauisse sufficiat. Iacebit $\frac{-\sqrt{D}+b}{a'}$ inter $\frac{\mathfrak{C}}{\mathfrak{A}}$ et $\frac{\mathfrak{D}}{\mathfrak{B}}$. Fractio $\frac{\mathfrak{D}}{\mathfrak{B}}$ alicui fractionum $\frac{'\mathfrak{d}}{'\mathfrak{C}}, \frac{''\mathfrak{d}}{''\mathfrak{C}}$ $\frac{'''\mathfrak{d}}{'''\mathfrak{C}}$ etc. aequalis erit.... (I), qua posita $= \frac{m\mathfrak{d}}{m\mathfrak{C}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$ erit $= \frac{m\gamma}{m\alpha}$... (II). Demonstratur autem (I) ita: Si $\frac{\mathfrak{D}}{\mathfrak{B}}$ nulli illarum fractionum aequalis esse supponitur: inter duas tales $\frac{m\mathfrak{d}}{m\mathfrak{C}}$ et $\frac{m+2\mathfrak{d}}{m+2\mathfrak{C}}$ iacere debebit. Hinc vero eodem modo vt supra deducitur, necessario esse $\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{m+1\mathfrak{d}}{m+1\mathfrak{C}} = \frac{m\gamma}{m\alpha}$, atque vel $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$, vel $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. Quoniam vero f per substitutionem propriam ${}^m\alpha$, ${}^m\mathfrak{C}$, ${}^m\gamma$, ${}^m\mathfrak{d}$ in formam ${}^mf = (\pm {}^m a, {}^m b, \pm {}^{m-1}a)$ transit: hinc emergunt tres aequa-

tiones, ex quibus coniunctis cum aequ. 1, 2, 3, 4 atque hac, $^{m}\alpha^{m}\delta - {}^{m}\mathfrak{C}^{m}\gamma = 1$ deducitur eodem modo vt supra, terminum primum A, formae F, termino primo formae ^{m}f aequalem esse, illiusque terminum medium medio huius congruum secundum modulum A, vnde sequitur, quia vtraque forma est reducta, adeoque vtriusque terminus medius inter $\sqrt{D}$ et $\sqrt{D} \pm A$ situs, hos terminos medios aequales esse: hinc vero deducitur $\frac{^{m}\delta}{^{m}\mathfrak{C}} = \frac{\mathfrak{D}}{\mathfrak{B}}$. Veritas itaque assertionis (I) deriuata hic est ex suppositione illam esse falsam.

Supponendo autem $\frac{^{m}\delta}{^{m}\mathfrak{C}} = \frac{\mathfrak{D}}{\mathfrak{B}}$, prorsus simili modo et per easdem aequationes demonstratur, esse etiam $\frac{^{m}\gamma}{^{m}\alpha} = \frac{\mathfrak{C}}{\mathfrak{A}}$, quod erat secundum (II). Hinc vero adiumento aequationum $\mathfrak{AD} - \mathfrak{BC} = 1$, $^{m}\alpha^{m}\delta - {}^{m}\mathfrak{C}^{m}\gamma = 1$ deducitur esse vel $\mathfrak{A} = {}^{m}\alpha$, $\mathfrak{B} = {}^{m}\mathfrak{C}$, $\mathfrak{C} = {}^{m}\gamma$, $\mathfrak{D} = {}^{m}\delta$, vel $-\mathfrak{A} = {}^{m}\alpha$, $-\mathfrak{B} = {}^{m}\mathfrak{C}$, $-\mathfrak{C} = {}^{m}\gamma$, $-\mathfrak{D} = {}^{m}\delta$, formasque F, ^{m}f identicas. *Q. E. D.*

194. Quum formae quas supra socias vocauimus (art. 187, 6) semper sint improprie aequiualentes (art. 160), perspicuum est, si formae reductae F, f improprie aequiualentes sint, formaeque F socia forma G, formas f, G proprie aequiualentes fore adeoque formam G in periodo formae f contentam. Quodsi itaque formae F, f tum proprie tum improprie aequiualentes sunt, patet, tum F tum G in pe-

riodo formae f reperiri debere. Quare periodus haec sibi ipsi socia erit, duasque formas ancipites continebit (art. 187, 7). Vnde theorema art. 165 egregie confirmatur ex quo iam poteramus esse certi, formam aliquam ancipitem dari formis F, f aequiualentem.

195. Problema. *Propositis duabus formis quibuscunque* Φ, ϕ *eiusdem determinantis: diiudicare vtrum aequiualentes sint, annon.*

Sol. Quaerantur duae formae reductae F, f, propositis Φ, ϕ resp. proprie aequiualentes (art. 183). Quae prout aut proprie tantum aequiualent, aut improprie tantum, aut vtroque modo, aut neutro; etiam propositae aut proprie tantum aequiualentes erunt, aut improprie tantum, aut vtroque aut neutro modo. Euoluatur periodus alterutrius formae reductae *e. g.* periodus formae f. Si forma F in hac periodo occurrit neque vero simul forma ipsi F socia, manifesto casus *primus* locum habebit; contra si socia haec adest neque vero F ipsa, *secundus*; si vtraque, *tertius*; si neutra, *quartus*.

Ex. Propositae sint formae (129, 92, 65), (42, 59, 81) determinantis 79. His proprie aequiualentes inueniuntur reductae (10, 7, — 3), (5, 8, — 3). Periodus formae prioris haec est: (10, 7, — 3), (— 3, 8, 5), (5, 7, — 6), (— 6, 5, 9), (9, 4, — 7) (— 7, 3, 10). In qua quum forma (5, 8, — 3) ipsa non reperiatur, sed tamen socia (— 3, 8, 5): formas propositas improprie tantum aequiualere concludimus.

Si omnes formae reductae determinantis dati eodem modo vt supra (art. 187, 5) in periodos P, Q, R etc. distribuuntur, atque e quauis periodo forma aliqua ad libitum eligitur, ex P, F; ex Q, G; ex R, H etc.: inter has formas F, G, H etc. duae quae proprie aequiualeant esse non poterunt. Quaeuis autem alia forma eiusdem determinantis alicui ex istis proprie aequiualens erit et quidem *vnicae* tantum. Hinc manifestum est, *omnes formas huius determinantis in totidem classes distribui posse, quot habeantur periodi*, scilicet referendo eas quae formae F proprie aequiualent in primam classem, eas quae formae G proprie aequiualent in secundam etc. Hoc modo omnes formae in eadem classe contentae proprie aequiualentes erunt, formae vero e classibus diuersis non poterunt proprie aequiualere. Sed hic huic argumento infra fusius explicando non immoramur.

196. Problema. *Propositis duabus formis proprie aequiualentibus* Φ, ϕ: *inuenire transformationem propriam alterius in alteram.*

Sol. Per methodum art. 183 inueniri poterunt duae series formarum $\Phi, \Phi', \Phi'' \ldots \Phi^{n}$ et $\phi, \phi', \phi'' \ldots \phi^{\nu}$ tales vt quaeuis forma sequens praecedenti proprie aequiualeat, vltimaeque Φ^{n}, ϕ^{ν} sint formae reductae; et quum Φ, ϕ proprie aequiualentes esse supponantur, necessario Φ^{μ} in periodo formae ϕ^{ν} contenta erit. Sit $\phi^{\nu} = f$ ipsiusque periodus vsque ad formam Φ^{n} haec $f, f', f'' \ldots f^{m-1}, \Phi^{n}$, ita vt in hac periodo index formae Φ^{μ} sit m; designenturque formae quae oppositae sunt sociis formarum

Φ, Φ', Φ'' ... Φ^n per Ψ, Ψ', Ψ'' ... Ψ^n resp. *). Tum in progressione Φ, Φ', Φ'' ... f, f', f'' ... f^{m-1}, Ψ^{n-1}, Ψ^{n-2} ... Ψ, Φ quaeuis forma praecedenti ab vltima parte contigua erit, vnde per art. 177 inueniri poterit transformatio propria primae Φ in vltimam Φ. Illud autem de formis reliquis progressionis nullo negotio perspicitur; de his f^{m-1}, Ψ^{n-1} sic probatur: Sit $f^{m-1} = (g, h, i)$; f^m siue $\Phi^n = (g', h', i')$; $\Phi^{n-1} = (g'', h'', i'')$. Forma (g', h', i') tum formae (g, h, i) tum formae (g'', h'', i'') ab vltima parte contigua erit; hinc $i = g' = i''$, et $-h \equiv h' \equiv -h''$ (mod. i vel g' vel i''). Vnde manifestum est formam $(i'', -h'', g'')$, i. e. formam Ψ^{n-1} formae (g, h, i), i. e. formae f^{m-1} ab vltima parte contiguam esse.

Si formae Φ, Φ impropriе aequiualentes sunt: forma Φ proprie aequiualebit formae cui opposita est Φ. Inueniri poterit itaque transformatio propria formae Φ in formam cui Φ est opposita; quae si supponitur fieri per substitutionem α, β, γ, δ, facile perspicitur, Φ improprie transformari in ipsam Φ per substitutionem α, $-\beta$, γ, $-\delta$.

Hinc etiam perspicuum est, si formae Φ, Φ tum proprie tum improprie aequiualentes sint, inueniri posse *duas* transformationes, propriam et impropriam.

Ex. Quaeritur transformatio impropria formae (129, 92, 65) in formam (42, 59, 81), quam

*) Ita vt Ψ oriatur ex Φ commutando terminum primum et vltimum tribuendoque medio signum oppositum, similiterque de reliquis.

illi improprie aequiualere in art. praec. inuenimus. Inuestiganda erit itaque primo transformatio propria formae (129, 92, 65) in formam (42, — 59, 81). Ad hunc finem euoluitur progressio formarum haec: (129, 92, 65), (65, — 27, 10), (10, 7, — 3), (— 3, 8, 5), (5, 22, 81), (81, 59, 42), (42, — 59, 81). Hinc deducitur transformatio propria — 47, 56, 73, — 87, per quam (129, 92, 65) transit in (42, — 59, 81); quare per impropriam — 47, — 56, 73, 87 transibit in (42, 59, 81).

197. Si transformatio vna formae alicuius $(a, b, c) \ldots \varphi$ in aequiualentem Φ habetur: ex hac *omnes* transformationes similes formae φ in Φ deduci poterunt, si modo omnes solutiones aequationis indeterminatae $tt - Duu = mm$ assignari possunt, designante D determinantem formarum Φ, φ; m diuisorem communem maximum numerorum $a, 2b, c$ (art. 162). Hoc igitur problema, quod pro valore negatiuo ipsius D iam supra soluimus, nunc pro positiuo aggrediemur. Quia vero manifesto quiuis valor ipsius t aequationi satisfaciens etiamnum mutato signo satisfacit, similiterque quiuis valor ipsius u: sufficiet si omnes valores *positiuos* ipsorum t, u assignare possimus, fungeturque quaelibet solutio per valores positiuos, quatuor solutionum vice. Hoc negotium ita absoluemus, vt *primo* valores *minimos* ipsorum t, u (praeter hos per se obuios $t = m$, $u = 0$) inuenire, *tum* ex his omnes reliquos deriuare doceamus.

198. Problema. *Inuenire numeros minimos t, u aequationi indeterminatae $tt - Duu = mm$ satisfacientes, siquidem forma aliqua (M, N, P) datur, cuius de-*

terminans est D, numerorumque M, 2N, P diuisor communis maximus m.

Sol. Accipiatur ad lubitum forma reducta $(a, b, -a') \ldots f$, determinantis D, vbi diuisor communis maximus numerorum a, $2b$, a' sit m, qualem dari vel inde manifestum est, quod forma reducta formae (M, N, P) aequiualens inueniri potest, quae per art. 161 hac proprietate erit praedita: sed ad propositum praesens quaeuis forma reducta in qua conditio haec locum habet poterit adhiberi. Euoluatur periodus formae f, quam ex n formis constare supponemus. Retentis omnibus signis quibus in art. 188 vsi sumus, f^n erit $(+a^n, b^n, -a^{n+1})$, quia n par, et in hanc formam transibit f per substitutionem propriam α^n, β^n, γ^n, δ^n. Quia vero f et f^n sunt identicae: f transibit in f^n etiam per substitutionem propriam 1, 0, 0, 1. Ex his duabus transformationibus similibus formae f in f^n per art. 162 deduci poterit solutio aequationis $tt - Duu = mm$ *in integris*, scilicet $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (aequ. 18 art. 162), $u = \frac{\gamma^n m}{a}$ (aequ. 19) *). Designentur hi valores positiue accepti si forte nondum sunt per T, U, eruntque hi T, U valores minimi ipsorum t, u, praeter hos $t = m$, $u = 0$ (a quibus necessario erunt diuersi, quia manifesto γ^n non poterit esse $= 0$).

Supponamus enim dari adhuc minores valores ipsorum t, u puta $\mathfrak{t}$, $\mathfrak{u}$ qui sint positiui et $\mathfrak{u}$

*) Quae in art. 162 erant $\alpha, \beta, \gamma, \delta$; $\alpha', \beta', \gamma', \delta'$; A, B, C; A', B', C'; e, hic sunt 1, 0, 0, 1; $\alpha^m, \beta^m, \gamma^m, \delta^m$; $a, b, -a'$; $a, b, -a'$; 1.

non $= o$. Tum per art. 162 forma f per substitutionem propriam $\frac{1}{m}(t - bu)$, $\frac{1}{m}a'u$, $\frac{1}{m}au$, $\frac{1}{m}(t + bu)$ transformabitur in formam cum ipsa identicam. Iam ex art. 193, II sequitur, *aut* $\frac{1}{m}(t - bu)$ *aut* $-\frac{1}{m}(t - bu)$ alicui numerorum α^{II}, α^{III}, α^{IV} etc. aequalem esse debere, puta $= \alpha^{\mu}$ (quia enim $tt = Duu + mm = bbuu + a'uu + mm$, erit $tt > bbuu$, adeoque $t - bu$ positiuus; hinc fractio $\frac{t - bu}{au}$, quae respondet fractioni $\frac{\mathfrak{A}}{\mathfrak{C}}$ in art. 193, idem signum habebit vt a vel a'); atque in casu priori $\frac{1}{m}a'u$, $\frac{1}{m}au$, $\frac{1}{m}(t + bu)$, in posteriori easdem quantitates mutatis signis, resp. $= \mathfrak{C}^{\mu}$, γ^{μ}, δ^{m}. Sed quum sit $u < U$ i. e. $u < \frac{\gamma^{n} m}{a}$ et $> o$: erit $\gamma^{\mu} < \gamma^{n}$ et $> o$; quocirca quum progressio γ, γ', γ'' etc. continuo crescat, necessario μ iacebit inter o et n excl. Forma vero respondens, f^{μ}, identica erit cum forma f, *Q.E.A*, quum omnes formae f, f', f'', etc. vsque ad f^{n-1} diuersae esse supponantur. Ex his colligitur, minimos valores ipsorum t, u (exceptis valoribus m, o) esse T, U.

Ex. Si $D = 79$, $m = 1$: adhiberi poterit forma $(3, 8, -5)$, pro qua $n = 6$, atque $\alpha^{n} = -8$, $\gamma^{n} = -27$, $\delta^{n} = -152$ (art. 188). Hinc $T = 80$, $U = 9$, qui sunt valores minimi numerorum t, u, aequationi $tt - 79uu = 1$ satisfacientes.

199. Ad praxin formulae adhuc commodiores erui possunt. Erit nimirum $2b\gamma^n = -a(\alpha^n - \delta^n)$, quod facile ex art. 162 deducitur, multiplicando aequ. [19] per $2b$, [20] per a et mutando characteres illic adhibitos in praesentes. Hinc fit $\alpha^n + \delta^n = 2\delta^n - \frac{2b}{a}\gamma^n$, adeoque

$$\pm T = m\,(\delta^n - \frac{b}{a}\gamma^n),\ \pm U = \frac{\gamma^n m}{a}.$$

Per similem methodum hos valores obtinemus

$$\pm T = m\,(\alpha^n + \frac{b}{a'}\varepsilon^n),\ \pm U = \frac{\varepsilon^n m}{a'}.$$

Tum hae tum illae formulae perquam commodae euadunt, propter $\gamma^n = \delta^n - 1$, $\alpha^n = \varepsilon^n - 1$, ita vt si hac vteris, solam progressionem $\varepsilon', \varepsilon'', \varepsilon''' \ldots \varepsilon^n$, si illa vti mauis, solam hanc $\delta', \delta'', \delta'''$ etc. supputauisse sufficiat. Praeterea ex art. 189, 3 facile deducitur, quum n necessario sit par, α^n et $\frac{b}{a'}\varepsilon^n$ eadem signa habere; neque minus δ^n et $\frac{b}{a}\gamma^n$, ita vt in formula priori pro T differentia absoluta, in posteriori summa absoluta accipi debeat, neque adeo ad signa respicere omnino opus sit. Receptis signis in art. 189, 4 adhibitis erit ex formula priori

$$T = m\,[k', k'', k''' \ldots k^n] - \frac{mb}{a}[k', k'', k''' \ldots k^n - 1];\ U = \frac{m}{a'}[k', k'', k''' \ldots k^n - 1];$$

ex posteriori

$$T = m\,[k'', k''' \ldots k^n - 1] + \frac{mb}{a'}[k'', k''' \ldots k^n];$$

$$U = \frac{m}{a}[k'', k''' \ldots k^n];$$

vbi pro valore ipsius T etiam $m\,[k'', k''' \ldots k^{n}, \frac{b}{a'}]$ scribi poterit.

Ex. Pro $D = 61$, $m = 2$ adhiberi potest forma $(2, 7, -6)$, pro qua eruitur $n = 6$; k^{I}, k^{II}, k^{III}, k^{IV}, k^{V}, k^{VI} resp. $= 2, 2, 7, 2, 2, 7$. Hinc fit $T = 2\,[2, 2, 7, 2, 2, 7] - 7\,[2, 2, 7, 2, 2] = 2888 - 1365 = 1523$, ex formula prima; idem prouenit ex secunda $T = 2\,[2, 7, 2, 2] + \frac{7}{3}\,[2, 7, 2, 2, 7]$. U vero fit $= \frac{1}{3}\,[2, 2, 7, 2, 2] = [2, 7, 2, 2, 7] = 195$.

Ceterum plura artificia adhuc dantur, per quae calculus contrahi potest, sed de his fusius hic loqui breuitas non permittit.

200. Vt ex valoribus minimis ipsorum t, u *omnes* obtineamus, aequationem $TT - DUU = mm$ ita exhibemus $(\frac{T}{m} + \frac{U}{m}\sqrt{D})(\frac{T}{m} - \frac{U}{m}\sqrt{D}) = 1$, vnde etiam erit $(\frac{T}{m} + \frac{U}{m}\sqrt{D})^{e}\ (\frac{T}{m} - \frac{U}{m}\sqrt{D})^{e} = 1 \ldots [1]$, denotante e numerum quemcunque. Iam designabimus breuitatis caussa valores quantitatum

$$\frac{m}{2}(\frac{T}{m} + \frac{U}{m}\sqrt{D})^{e} + \frac{m}{2}(\frac{T}{m} - \frac{U}{m}\sqrt{D})^{e},$$

$$\frac{m}{2\sqrt{D}}(\frac{T}{m} + \frac{U}{m}\sqrt{D})^{e} - \frac{m}{2\sqrt{D}}(T - \frac{U}{m}\sqrt{D})^{e}\ *)$$

generaliter per t^{e}, u^{e} resp. *i. e.* illarum valores pro

*) In his solis quatuor expressionibus et in aequ. [1] e denotat *exponentem* potestatis; in reliquis literae apici adscriptae semper *indicem* designant.

$e = 0$, per t^0, u^0 (qui erunt m, 0); pro $e = 1$ per t', u' (qui fiunt T, U); pro $e = 2$ per t'', u''; pro $t = 3$ per t''', u''' etc. — demonstrabimusque, si pro e accipiantur omnes numeri integri non negatiui i. e. 0, omnesque positiui ab 1 vsque ad ∞, expressiones illas exhibere omnes valores positiuos ipsorum t, u: scilicet I) omnes valores illarum expressionum esse reuera valores ipsorum t, u; II) omnes valores illos esse numeros integros; III) nullos valores positiuos ipsorum t, u dari qui sub formulis illis non contineantur.

I. Substitutis pro t^e, u^e valoribus suis nullo negotio aduimento aequ. [1] confirmatur, esse $(t^e + u^e \sqrt{D})\ (t^e - u^e \sqrt{D}) = mm$; i. e. $t^e\ t^e - D\ u^e\ u^e = mm$.

II. Eodem modo facile confirmatur, esse generaliter $t^{e+1} + t^{e-1} = \frac{2T}{m} t^e$, $u^{e+1} + u^{e-1} = \frac{2T}{m} u^e$. Hinc manifestum est duas progressiones t^0, t', t'', t''' etc., u^0, u', u'', u''' etc. esse recurrentes, et vtriusque scalam relationis $\frac{2T}{m}$, -1, scilicet $t'' = \frac{2T}{m} t' - t^0$, $t''' = \frac{2T}{m} t'' - t'$ etc. $u'' = \frac{2T}{m} u'$ etc.

Iam quoniam per hyp. forma aliqua datur, (M, N, P), determinantis D, in qua M, $2N$, P per m sunt diuisibiles: habebitur $TT = (NN - MP)\ UU + mm$, eritque adeo manifesto $4TT$ per mm diuisibilis. Hinc $\frac{2T}{m}$ erit numerus integer et

quidem positiuus. Quia vero $t^\circ = m$, $t' = T$, $u^\circ = o$, $u' = U$, adeoque integri: omnes t'', t''' etc. u'', u''' etc. etiam integri erunt. Porro perspicuum est, quia $TT > mm$, omnes t°, t', t'', t''' etc. positiuos et continuo in infinitum crescentes esse, nec non omnes u°, u', u'', u''' etc.

III. Supponamus, dari adhuc alios valores positiuos ipsorum t, u qui in progressione t°, t', t'' etc. u°, u', u'' etc. non contenti sint, puta $\mathfrak{T}$, $\mathfrak{U}$. Manifestum est, quum progressio u°, u' etc. a o in infinitum crescat, $\mathfrak{U}$ necessario inter duos terminos proximos, u^n et $u^n + 1$ situm fore, ita vt sit $\mathfrak{U} > u^n$ et $\mathfrak{U} < u^n + 1$. Vt absurditatem huius suppositionis demonstremus, obseruamus

1° Aequationi $tt - Duu = mm$ satisfactum iri etiam ponendo $t = \frac{1}{m}(\mathfrak{T} t^n - D\mathfrak{U} u^n)$, $u = \frac{1}{m}(\mathfrak{U} t^n - \mathfrak{T} u^n)$. Hoc quidem nullo negotio per substitutionem confirmatur: quod vero hi valores quos ponemus breuitatis gratia $= \tau$, ν, semper sunt numeri *integri* ita ostendimus. Si (M, N, P) est forma determinantis D, atque m diuisor communis numerorum M, $2N$, P: erit tum $\mathfrak{T} + N\mathfrak{U}$ tum $t^n + Nu^n$ per m diuisibilis adeoque etiam $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$ siue $\mathfrak{U} t^n - \mathfrak{T} u^n$. Quare ν erit integer et proin etiam τ, quia $\tau\tau = D\nu\nu + mm$.

2° Patet ν non posse esse $= o$; hinc enim sequeretur $\mathfrak{U}\mathfrak{U} t^n t^n = \mathfrak{T}\mathfrak{T} u^n u^n$ siue $\mathfrak{U}\mathfrak{U}(Du^n u^n + mm) = u^n u^n (D\mathfrak{U}\mathfrak{U} + mm)$ siue $\mathfrak{U}\mathfrak{U} =$

$u^n\,u^n$, contra hyp. ex qua $\mathfrak{U} > u^n$. Quum igitur praeter valorem o, minimus valor ipsius u sit U, erit v certe non minor quam U.

3° Facile ex valoribus ipsorum t^n, t^{n+1}, u^n, u^{n+1} confirmari potest esse $m\,U = u^{n+1}\,t^n - t^{n+1}\,u^n$. Quare $\mathfrak{U}\,t^n - \mathfrak{T}\,u^n$ certe non erit minor quam $u^{n+1}\,t^n - t^{n+1}\,u^n$.

4° Iam ex aequatione $\mathfrak{T}\,\mathfrak{T} - D\,\mathfrak{U}\,\mathfrak{U} = m\,m$ habetur $\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{(D + \frac{m\,m}{\mathfrak{U}\,\mathfrak{U}})}$ et similiter $\frac{t^{n+1}}{u^{n+1}} = \sqrt{(D + \frac{m\,m}{u^{n+1}\,u^{n+1}})}$, vnde facile deducitur esse $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{n+1}}{u^{n+1}}$. Hinc vero et ex conclusione in 3° sequitur $(\mathfrak{U}\,t^n - \mathfrak{T}\,u^n)\ (t^n + u^n\,\frac{\mathfrak{T}}{\mathfrak{U}}) > (u^{n+1}\,t^n - t^{n+1}\,u^n)\ (t^n + u^n\,\frac{t^{n+1}}{u^{n+1}})$, siue, euolutione facta, et loco ipsorum $\mathfrak{T}\,\mathfrak{T}$, $t^n\,t^n$, $t^{n+1}\,t^{n+1}$ substitutis valoribus suis $D\,\mathfrak{U}\,\mathfrak{U} + m\,m$, $D\,u^n\,u^n + m\,m$, $D\,u^{n+1}\,u^{n+1} + m\,m$,

$$\frac{1}{\mathfrak{U}}\,(\mathfrak{U}\,\mathfrak{U} - u^n\,u^n) > \frac{1}{u^{n+1}}\,(u^{n+1}\,u^{n+1} - u^n\,u^n),$$

vnde, quoniam vtraque quantitas manifesto positiua, fit transponendo $\mathfrak{U} + \frac{u^n\,u^n}{u^{n+1}} > u^{n+1} + \frac{u^n\,u^n}{\mathfrak{U}}$, *Q. E. A.*, quia quantitatis prioris pars prima *minor* est quam pars prima quantitatis secundae, nec non illius secunda minor quam secunda hu-

ius. Quamobrem suppositio consistere nequit et progressiones t, t', t'', etc. u, u', u'', etc. omnes valores positiuos ipsorum t, u exhibebunt.

Ex. Pro $D = 61$, $m = 2$ valores minimos positiuos ipsorum t, u inuenimus 1523, 195: quare *omnes* valores positiui exhibebuntur per has formulas $t = (\frac{1523}{2} + \frac{195}{2}\sqrt{61})^e + (\frac{1523}{2} - \frac{195}{2}\sqrt{61})^e$, $u = \frac{1}{\sqrt{61}}((\frac{1523}{2} + \frac{195}{2}\sqrt{61})^e - (\frac{1523}{2} - \frac{195}{2}\sqrt{61})^e)$. Inuenitur autem $t^\circ = 2$, $t' = 1523$, $t'' = 1523\,t' - t^\circ = 2319527$, $t''' = 1523\,t'' - t' = 3532618098$ etc.; $u^\circ = 0$, $u' = 195$, $u'' = 1523\,u' - u^\circ = 296985$, $u''' = 1523\,u'' - u' = 452307960$ etc.

201. Circa problema in artt. praecc. tractatum sequentes obseruationes adhuc adiicimus.

1) Quum aequationem $t\,t - D\,u\,u = m\,m$ pro omnibus casibus soluere docuerimus, vbi m est diuisor communis maximus trium numerorum M, 2 N, P, talium vt $N\,N - M\,P = D$: operae pretium est omnes numeros qui tales diuisores esse possunt siue omnes valores ipsius m pro valore dato ipsius D assignare. Ponatur $D = n\,n\,D'$, ita vt D' a factoribus quadraticis omnino sit liber, quod obtinetur si pro $n\,n$ assumitur maximum quadratum ipsum D metiens: sin vero D

iam per se nullum factorem quadraticum implicaret, fieri deberet $n = 1$. Tum dico

Primo, si D' fuerit formae $4k + 1$, quemuis diuisorem ipsius $2n$ fore valorem ipsius m, et vice versa. Si enim g est diuisor ipsius $2n$, habebitur forma $(g, n, \frac{nn(D'-1)}{g})$, cuius determinans est D, et in qua manifesto diuisor communis maximus numerorum g, $2n$, $\frac{nn(D'-1)}{g}$ erit g (patet enim $\frac{nn(D'-1)}{gg} = \frac{4nn}{gg} \cdot \frac{D'-1}{4}$ esse numerum integrum). Si vero, vice versa, g supponitur esse valor ipsius m, scilicet diuisor communis maximus numerorum M, $2N$, P, atque $NN - MP = D$: manifesto $4D$ siue $4nnD'$ diuisibilis erit per gg. Hinc vero sequitur, $2n$ necessario per g diuisibilem esse. Si enim g ipsum $2n$ non metiretur, g et $2n$ haberent diuisorem communem maximum minorem quam g, quo posito $= \delta$, atque $2n = \delta n'$, $g = \delta g'$, foret $n'n'D'$ per $g'g'$ diuisibilis, n' ad g' adeoque etiam $n'n'$ ad $g'g'$ primus et proin etiam D' per $g'g'$ diuisibilis, contra hyp. secundum quam D' ab omni factore quadratico est liberatus.

Secundo, si D' fuerit formae $4k + 2$ vel $4k + 3$, quemuis diuisorem ipsius n fore valorem ipsius m, et vice versa quemuis valorem ipsius m metiri ipsum n. Si enim g est diuisor ipsius n, habebitur forma $(g, 0, \frac{nnD'}{g})$, cuius

determinans $= D$, et vbi manifesto numerorum g, o, $\frac{nnD'}{g}$ diuisor communis maximus erit g. — Si vero g supponitur esse valor ipsius m, puta diuisor communis maximus numerorum M, 2 N, P, atque $NN - MP = D$: eodem modo vt supra g metietur ipsum 2 n, siue $\frac{2n}{g}$ erit integer. Si quotiens hic esset impar: quadratum $\frac{4nn}{gg}$ foret $\equiv 1 \pmod 4$, adeoque $\frac{4nnD'}{gg}$ aut $\equiv 2$ aut $\equiv 3 \pmod 4$. At $\frac{4nnD'}{gg} = \frac{4D}{gg} = \frac{4NN}{gg} - \frac{4MP}{gg} \equiv \frac{4NN}{gg} \pmod 4$, et proin $\frac{4NN}{gg}$ aut $\equiv 2$ aut $\equiv 3 \pmod 4$. *Q. E. A.*, quia omne quadratum aut cifrae aut vnitati secundum modulum 4 congruum esse debet. Quare quotiens $\frac{2n}{g}$ necessario erit par, adeoque $\frac{n}{g}$ integer, siue g diuisor ipsius n.

Patet itaque, 1 semper esse valorem ipsius m, siue aequationem $tt - Duu = 1$ pro quouis valore positiuo non quadrato ipsius D per praecedentia resolubilem esse; 2 tunc tantummodo esse valorem ipsius m, si D fuerit aut formae $4k$, aut formae $4k + 1$.

2) Si m est maior quam 2, attamen numerus idoneus, solutio aequationis $tt - Duu = mm$ reduci potest ad solutionem similis aequa-

tionis, vbi m est aut 1 aut 2. Scilicet posito vt ante $D = nn\ D'$, si m ipsum n metitur, metietur mm ipsum D. Tum si valores minimi ipsorum p, q in aequatione $pp - \frac{D}{mm}\ qq = 1$ supponuntur esse $p = P$, $q = Q$, valores minimi ipsorum t, u in aequatione $tt - D\ uu = mm$ erunt $t = m\ P$, $u = Q$. — Si vero m ipsum n non metitur, metietur saltem ipsum $2\ n$ eritque certo par; $\frac{4D}{mm}$ autem integer. Et si tunc valores minimi ipsorum p, q in aequatione $p\ p - \frac{4D}{mm}\ qq = 4$ inuenti sunt $p = P$, $q = Q$: valores minimi ipsorum t, u in aequatione $tt - Duu = mm$ erunt $t = \frac{m}{2}P$, $u = Q$. — In vtroque autem casu non solum ex valoribus minimis ipsorum p, q valores minimi ipsorum t, u, sed ex *omnibus* valoribus illorum *omnes* valores horum per hanc methodum manifesto deduci poterunt.

3) Designantibus t°, u°; t', u'; t'', u'' etc. omnes valores positiuos ipsorum t, u in aequatione $tt - Duu = mm$ (vt in art. praec.), si contingit vt valores quidam ex serie illa, valoribus primis in eadem secundum modulum quemcunque datum r, congrui sint, puta $t^\varrho \equiv t^\circ$ (siue $\equiv m$), $u^\varrho \equiv u^\circ$ siue $\equiv 0$ (mod. r); simulque valores proxime sequentes valoribus secundis, puta $t^{\varrho+1} \equiv t'$, $u^{\varrho+1} \equiv u'$ (mod. r): erit etiam $t^{\varrho+2} \equiv t''$, $u^{\varrho+2} \equiv u''$; $t^{\varrho+3} \equiv t'''$, $u^{\varrho+3} \equiv$

u''' etc. Hoc facile inde deducitur, quod vtraque series t°, t', t'' etc., u°, u', u'' etc. est ex recurrentium genere, scilicet quoniam $t'' = \frac{2T}{m} t' - t^\circ$, $t^{\varrho+2} = \frac{2T}{m} t^{\varrho+1} - t^\varrho$ erit $t'' \equiv t^{\varrho+2}$ similiterque de reliquis. — Hinc autem sequitur, fore generaliter $t^{h+\varrho} \equiv t^h$, $u^{h+\varrho} \equiv u^h$ (mod. r), denotante h numerum quemcunque, nec non adhuc generalius, si fuerit $\mu \equiv \nu$ (mod. ϱ), fore $t^\mu \equiv t^\nu$, $u^\mu \equiv u^\nu$ (mod. r).

4) Conditionibus autem in obseru. praec. requisitis semper satisfieri potest, scilicet semper inueniri potest index ϱ (pro modulo quocunque dato r) pro quo sit $t^\varrho \equiv t^\circ$, $t^{\varrho+1} \equiv t'$, $u^\varrho \equiv u^\circ$, $u^{\varrho+1} \equiv u'$. Ad quod demonstrandum obseruamus

primo, conditioni tertiae semper satisfieri posse. Nullo enim negotio per criteria in (1) tradita perspicietur, etiam aequationem $pp - rrDqq = mm$ solubilem fore; et si valores minimi positiui ipsorum p, q (praeter hos m, 0) supponuntur esse P, Q: inter valores ipsorum t, u manifesto erunt etiam $t = P$, $u = rQ$. Quare P, rQ in progressionibus t°, t' etc., u°, u' etc. contenti erunt, et si $P = t^\lambda$, $rQ = u^\lambda$, erit $u^\lambda \equiv 0 \equiv u^\circ$ (mod. r). Praeterea facile perspicietur, inter u° et u^λ nullum terminum fore ipsi u° secundum modulum r congruum.

Secundo patet, si hic insuper tres reliquae conditiones adimpletae sint, puta si etiam $u^{\lambda+1} \equiv u'$,

$t^\lambda \equiv t^\circ$, $t^{\lambda+1} \equiv t'$, poni tantummodo debere $\varrho = \lambda$. Si vero vna aut altera illarum conditionum locum non habet, dico certe statui posse $\varrho = 2\lambda$. Nam ex aequat. [1] formulisque generalibus pro t^e, u^e in art. praec. deducitur $t^{2\lambda} = \frac{1}{m}(t^\lambda t^\lambda + D u^\lambda u^\lambda) = \frac{1}{m}(mm + 2 D u^\lambda u^\lambda)$ adeoque $\frac{t^{2\lambda} - t^\circ}{r} = \frac{2 D u^\lambda u^\lambda}{m r}$, quae quantitas erit numerus integer, quia per hyp. r ipsum u^λ metititur, nec non mm ipsum $4D$, adeoque a potiori m ipsum $2D$. — Porro erit $u^{2\lambda} = \frac{2}{m} t^\lambda u^\lambda$, et quoniam $4 t^\lambda t^\lambda = 4 D u^\lambda u^\lambda + 4 mm$, adeoque per $m\,m$ diuisibilis, $2 t^\lambda$ erit diuisibilis per m, et proin $u^{2\lambda}$ per r, siue $u^{2\lambda} \equiv u^\circ$ (mod. r). — Tertio inuenitur $t^{2\lambda+1} = t' + \frac{2 D u^\lambda u^{\lambda+1}}{m}$, et quoniam ex simili ratione $\frac{2 D u^\lambda}{m r}$ est integer, erit $t^{2\lambda+1} \equiv t'$ (mod. r). — Tandem reperitur $u^{2\lambda+1} = u^\lambda + \frac{2 t^{\lambda+1} u^\lambda}{m}$, et quoniam $2t^{\lambda+1}$ per m diuisibilis est, u^λ per r: erit $u^{2\lambda+1} \equiv u'$ (mod. r). *Q. E. D.*

Ceterum vsus posteriorum duarum obseruationum in sequentibus apparebit.

202. Casus particularis problematis, nempe soluere aequationem $t\,t - D u u = 1$, iam a geometris seculi praecedentis fuit agitatus. Sagacissimus Fermatius problema hoc analystis Anglis

proposuit, Wallisiusque Brounkerum tamquam inuentorem solutionis quam in *Alg. Cap.* 98, *Opp. T. II p.* 418 *sqq.* tradit nominat; Ozanam Fermatium; denique ill. Euler qui de illo egit in *Comm. Petr. VI. p.* 175, *Comm. nou. XI, p.* 28*), *Algebra P. II. pag.* 226, *Opiusc. An. I. p.* 310, Pellium, vnde problema illud a quibusdam auctoribus *Pellianum* vocatum est. Omnes hae solutiones, si essentiam spectas, conueniunt cum ea quam obtinemus, si in art. 198 formam reductam eam adoptamus in qua $a = 1$; attamen operationem quam praescribunt tandem necessario *finiri*, siue problema semper *reuera solubile* esse, nemo ante ill. La Grange rigorose**) demonstrauit, *Melanges de la Soc. de Turin T. IV. p.* 19, et concinnius *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. Exstat haec disquisitio etiam in *supplementis ad Euleri Algebram* iam saepius laudatis. Ceterum methodus nostra (ex principiis omnino diuersis petita, neque ad casum $m = 1$ restricta) plerumque plures vias ad solutionem perueniendi suppeditat, quoniam in art. 198 a quauis alia forma reducta $(a, b, -a')$ proficisci possumus.

*) In hac comm. algorithmus quem art. 32 exposuimus, per similia signa exhibetur, quod nos illic annotare negleximus.

**) Quae Wallisius ad hunc finem protulit l. c. p. 427, 428 nihil ponderis habent. Paralogismus in eo consistit, quod p. 428 l. 4. supponit, proposita quantitate p inueniri posse numeros integros a, x tales vt $\frac{x}{a}$ minor sit quam p, defectus vero *assignato* minor. Hoc vtique verum est, quando defectus *assignatus* est *quantitas data*, neque vero, quando ab a et x pendet adeoque variabilis est, vti in casu praesenti euenit.

203. Problema. *Si formae* Φ, Φ *sunt aequiualentes, omnes transformationes alterius in alteram exhibere.*

Sol. Quando formae hae vnico tantum modo aequiualentes sunt (i. e. aut proprie tantum aut improprie tantum) quaeratur per art. 196 transformatio vna formae φ, in Φ, quae sit α, $\mathfrak{E}$, γ, δ, patetque alias quam quae huic sint similes, dari non posse. Quando vero φ, Φ tum proprie tum improprie aequiualent, quaerantur duae transformationes dissimiles, i. e. altera propria altera impropria, puta α, $\mathfrak{E}$, γ, δ et α', $\mathfrak{E}'$, γ', δ', eritque quaeuis alia transformatio aut huic aut illi similis. Si itaque forma Φ est (a, b, c) ipsius determinans $= D$, diuisor communis maximus numerorum a, $2b$, c (vti semper in praec.) m, atque t, u indefinite omnes numeri aequationi $tt - Duu = mm$ satisfacientes: in casu priori omnes transformationes formae φ in Φ contentae erunt sub prima formularum sequentium I, in posteriori vel sub prima I vel sub secunda II.

$$\text{I}.... \quad \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u), \ \frac{1}{m}(\mathfrak{E} t - (\mathfrak{E} b + \delta c)u),$$
$$\frac{1}{m}(\gamma t + (\alpha a + \gamma b)u), \ \frac{1}{m}(\delta t + (\mathfrak{E} a + \delta b)u)$$

$$\text{II}.... \quad \frac{1}{m}(\alpha' t - (\alpha' b + \gamma' c)u), \ \frac{1}{m}(\mathfrak{E}' t - (\mathfrak{E}' b + \delta' c)u),$$
$$\frac{1}{m}(\gamma' t + (\alpha' a + \gamma' b)u), \ \frac{1}{m}(\delta' t + (\mathfrak{E}' a + \delta' b)u).$$

Ex. Desiderantur omnes transformationes formae (129, 92, 65) in formam (42, 59,

81). Has improprie tantum aequiualentes esse in art. 195 inuenimus et in art. seq. transformationem impropriam illius in hanc eruimus — 47, — 56, 73, 87. Quamobrem omnes transformationes formae (129, 92, 65) in (42, 59, 81) exhibebuntur per formulam — (47 t + 421 u), — (56 t + 503 u), 73 t + 653 u, 87 t + 780 u, vbi t, u sunt indefinite omnes numeri aequationi $tt - 79\,uu = 1$ satisfacientes; hi vero exhibentur per formulas

$$\pm t = \tfrac{1}{2}((80+9\sqrt{79})^e + (80-9\sqrt{79})^e),$$

$$\pm u = \frac{1}{2\sqrt{79}}((80+9\sqrt{79})^e - (80-9\sqrt{79})^e)$$

vbi pro e omnes numeri integri non negatiui sunt accipiendi.

204. Perspicuum est, formulam generalem omnes transformationes exhibentem eo *simpliciorem* euadere, quo simplicior fuerit transformatio initialis ex qua formula est deducta. Iam quum arbitrarium sit, a qua transformatione proficiscamur, saepenumero formula generalis simplicior reddi potest, si ex formula primo inuenta transformatio simplicior deducitur tribuendo ipsis t, u valores determinatos, et tunc ex hac alia formula componitur. Ita *e. g.* positis in formula in ex. art. praec. inuenta, $t = 80$, $u = -9$, prodit transformatio simplicior quam ea a qua profecti eramus, scilicet 29, 47, — 37, — 60 vnde deducitur formula generalis 29 t — 263 u, 47 t — 424 u, — 37 t + 337 u, — 60 t + 543 u. Quando itaque per praecepta praecedentia formula generalis eruta

est, tentari poterit, annon, tribuendo ipsis t, u valores determinatos $\pm t'$, $\pm u'$; $\pm t''$, $\pm u''$ etc. transformatio obtineatur simplicior quam ea ex qua formula deducta fuit, in quo casu ex illa transformatione formula simplicior deriuari poterit. — Ceterum in diiudicanda simplicitate aliquid arbitrarii remanet, quod si operae pretium esset ad normam fixam reuocare, nec non in progressione t', u'; t'', u'' etc. *limites* assignare possemus, vltra quos transformationes continuo minus simplices prodeant, ita vt vltra progredi opus non sit sed intra illos tentamen instituisse sufficiat: attamen quum plerumque per methodos a nobis praescriptas transformatio simplicissima vel statim vel adhibitis pro t, u valoribus $\pm t'$, $\pm u'$ prodire soleat, hanc disquisitionem breuitatis gratia supprimimus.

205. Problema. *Inuenire omnes repraesentationes numeri dati M per formulam datam $axx + 2bxy + cyy$, cuius determinans positiuus non - quadratus $= D$.*

Sol. Primo obseruamus, inuestigationem repraesentationum per valores ipsorum x, y inter se non primos, hic prorsus eodem modo, vt supra (art. 181) pro formis determinantis negatiui, ad eum casum reduci posse, vbi repraesentationes per valores indeterminatarum inter se primos quaeruntur, quod igitur hic repetere superfluum foret. Ad possibilitatem repraesentationum per valores ipsorum x, y inter se primos autem requiritur, vt D sit residuum quadraticum ipsius M, et si omnes valores expressionis $\sqrt{D}$ (mod. M) sunt N,

$-N$, N', $-N'$, N'', $-N''$ etc. (quos ita accipere licet vt nullus sit $> \frac{1}{2}M$), quaeuis repraesentatio numeri M per formam propositam ad aliquem horum valorum pertinebit. Ante omnia itaque valores illi erui debebunt; tunc repraesentationes ad singulos pertinentes deinceps inuestigari. Repraesentationes ad valorem N pertinentes non dabuntur, nisi formae (a, b, c) et $(M, N, \frac{NN-D}{M})$ proprie aequiualentes sunt; si vero sunt, quaeratur transformatio aliqua propria prioris in posteriorem, quae sit $\alpha, \beta, \gamma, \delta$. Tum habebitur repraesentatio numeri M per formam (a, b, c) ad valorem N pertinens haec: $x = \alpha$, $y = \gamma$, omnesque repraesentationes ad hunc valorem pertinentes exhibebuntur per formulam $x = \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u)$, $y = \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u)$, designante m diuisorem communem maximum numerorum a, $2b$, c; et t, u indefinite omnes numeros aequationi $tt - Duu = mm$ satisfacientes. — Ceterum manifestum est, formulam hanc generalem eo simpliciorem euadere, quo simplicior sit transformatio $\alpha, \beta, \gamma, \delta$ ex qua deducta est; quare haud inutile erit, transformationem simplicissimam formae (a, b, c) in $(M, N, \frac{NN-D}{M})$ secundum art. praec. antea eruere, et ex hac formulam deducere. — Prorsus eodem modo repraesentationes ad valores reliquos $-N$, N', $-N'$ etc. pertinentes (si quae dantur) per formulas generales exhiberi possunt.

Ex. Quaeruntur omnes repraesentationes numeri 585 per formulam $42xx + 62xy + 21yy$.

Quod ad repraesentationes per valores ipsorum x, y inter se non primos pertinet, statim patet alias huius generis dari non posse, quam in quibus diuisor communis maximus ipsorum x, y sit 3: quum 585 per vnicum quadratum 9 diuisibilis sit. Quando itaque omnes repraesentationes numeri $\frac{585}{9}$ i. e. 65 per formam $42x'x' + 62x'y' + 21y'y'$ inuentae sunt, in quibus x' ad y' primus; omnes repraesentationes numeri 585 per formam $42xx + 62xy + 21yy$, in quibus x ad y primus, ex illis deriuabuntur ponendo $x = 3x'$, $y = 3y'$. Valores expressionis $\sqrt{79}$ (mod. 65) sunt ± 12, ± 27. Repraesentatio numeri 65 ad valorem + 12 pertinens inuenitur $x' = 2$, $y' = -1$; quocirca omnes repraesentationes ipsius 65 ad hunc valorem pertinentes exhibebuntur per formulam $x' = 2t - 41u$, $y' = -t + 53u$, adeoque omnes repraesentationes ipsius 585 *hinc* oriundae per formulam $x = 6t - 123u$, $y = -3t + 159u$. Simili modo inuenitur formula generalis omnes repraesentationes numeri 65 ad valorem — 12 pertinentes exhibens $x' = 22t - 199u$, $y' = -23t + 211u$; et formula omnes repraesentationes numeri 585 hinc oriundas complectens $x = 66t - 597u$, $y = -69t + 633u$. Ad valores + 27 et — 27 autem nulla repraesentatio numeri 65 pertinet. — Vt repraesentationes numeri 585 per valores ipsorum x, y inter se primos inueniantur, primo valores expressionis $\sqrt{79}$ (mod. 585) eruere oportet, qui sunt ± 77, ± 103, ± 157, ± 248. Ad valores ± 77, ± 103, ± 248 inuenitur nullam repraesentationem pertinere; ad valorem + 157 autem pertinet repraesenta-

tio $x = 3$, $y = 1$, vnde deducitur formula generalis omnes repraesentationes ad hunc valorem pertinentes exhibens $x = 3t - 114u$, $y = t + 157u$; similiterque inuenitur repraesentatio ad -157 pertinens $x = 83$, $y = -87$, et formula in qua omnes similes sunt contentae $x = 83t - 746u$, $y = -87t + 789u$. Habentur itaque quatuor formulae generales sub quibus omnes repraesentationes numeri 585 per formam $42xx + 62xy + 21yy$ contentae sunt

$$\begin{array}{ll} x = 6t - 123u & y = -3t + 159u \\ x = 66t - 597u & y = -69t + 633u \\ x = 3t - 114u & y = t + 157u \\ x = 83t - 746u & y = -87t + 789u \end{array}$$

vbi t, u indefinite omnes numeros integros denotant, qui aequationi $tt - 79uu = 1$ satisfaciunt.

Applicationibus specialibus disquisitionum praecedentium de formis determinantis positiui non-quadrati breuitatis gratia non immoramur, quippe quas simili modo vt artt. 176, 182 quisque, sine negotio, proprio marte instituere poterit statimque ad formas determinantis positiui quadrati, quae solae adhuc supersunt, properamus.

206. Problema. *Proposita forma* (a, b, c) *determinantis quadrati* hh, *designante* h *ipsius radicem positiuam, inuenire formam* (A, B, C) *illi proprie aequiualentem, in qua* A *iaceat inter limites* 0 *et* $2h - 1$ *incl.,* B *sit* $= h$, $C = 0$.

Sol. I. Quoniam $hh = bb - ac$, erit $(h - b) : a = c : -(h + b)$. Sit huic rationi aequalis ratio $\gamma : \delta$, ita vt γ ad δ sit primus, determinenturque α, β ita vt sit $\alpha\delta - \beta\gamma = 1$, quae

fieri poterunt. Per substitutionem $\alpha, \mathfrak{G}, \gamma, \mathfrak{d}$ transeat forma (a, b, c) in (a', b', c'), quae igitur illi proprie aequiualens erit. Habebitur autem $b' = a\alpha\mathfrak{G} + b(\alpha\mathfrak{d} + \mathfrak{G}\gamma) + c\gamma\mathfrak{d} = (h - b)\alpha\mathfrak{d} + b(\alpha\mathfrak{d} + \mathfrak{G}\gamma) - (h + b)\mathfrak{G}\gamma = h(\alpha\mathfrak{d} - \mathfrak{G}\gamma) = h$; $c' = a\mathfrak{G}\mathfrak{G} + 2b\mathfrak{G}\mathfrak{d} + c\mathfrak{d}\mathfrak{d} = (h - b)\mathfrak{G}\mathfrak{d} + 2b\mathfrak{G}\mathfrak{d} - (h + b)\mathfrak{G}\mathfrak{d} = 0$. Quodsi itaque insuper a' inter limites 0 et $2h - 1$ iam est situs, forma (a', b', c') omnibus conditionibus satisfaciet.

II. Si vero a' extra limites 0 et $2h - 1$ iacet, sit A residuum minimum positiuum ipsius a' secundum modulum $2h$, quod manifesto inter hos limites situm erit, ponaturque $A - a' = 2hk$. Tum forma (a', b', c') i. e. $(a', h, 0)$ per substitutionem $1, 0, k, 1$ transibit in formam $(A, h, 0)$, quae formis (a', b', c'), (a, b, c) proprie aequiualens erit omnibusque conditionibus satisfaciet. — Ceterum perspicuum est, formam (a, b, c) transire in formam $(A, h, 0)$ per substitutionem $\alpha + \mathfrak{G}k, \mathfrak{G}, \gamma + \mathfrak{d}k, \mathfrak{d}$.

Ex. Proposita sit forma $(27, 15, 8)$ cuius determinans $= 9$. Hic $h = r$; rationibus $-12 : 27 = 8 : -18$ in numeris minimis aequalis est ratio $4 : -9$. Positis itaque $\mathfrak{G} = 4$, $\mathfrak{d} = -9$, $\alpha = -1$, $\gamma = 2$, forma (a', b', c') fit $(-1, 3, 0)$, quae transit in formam $(5, 3, 0)$ per substitutionem $1, 0, 1, 1$. Haec igitur est forma quaesita, transitque in eam proposita per substitutionem propriam $3, 4, -7, -9$.

Tales formas (A, B, C) in quibus $C = 0$, $B = h$, A inter limites 0 et $2h - 1$ situs, *formas reductas* vocabimus, quae igitur a formis reductis determinantis negatiui, vel positiui non-quadrati, probe sunt distinguendae.

207. THEOREMA. *Duae formae reductae* (a, h, o), (a', h, o), *non identicae proprie aequiualentes esse non possunt.*

Dem. Si enim proprie aequiualere supponuntur, transeat prior in posteriorem per substitutionem propriam $\alpha, \mathfrak{G}, \gamma, \delta$, habebunturque quatuor aequationes: $a\alpha\alpha + 2h\alpha\gamma = a' \ldots [1]$, $a\alpha\mathfrak{G} + h(\alpha\delta + \mathfrak{G}\gamma) = h \ldots [2]$, $a\mathfrak{G}\mathfrak{G} + 2h\mathfrak{G}\delta = 0 \ldots [3]$, $\alpha\delta - \mathfrak{G}\gamma = 1 \ldots [4]$. Multiplicando aequationem secundam per $\mathfrak{G}$, tertiam per α et subtrahendo fit $-h(\alpha\delta - \mathfrak{G}\gamma)\mathfrak{G} = \mathfrak{G}h$, siue, propter [4], $-\mathfrak{G}h = \mathfrak{G}h$, vnde necessario $\mathfrak{G} = 0$. Quare ex [4], $\alpha\delta = 1$, et $\alpha = \pm 1$. Hinc ex [1], $a \pm 2\gamma h = a'$, quae aequatio consistere nequit, nisi $\gamma = 0$ (quoniam tum a tum a' per hyp. inter 0 et $2h - 1$ iacent) *i. e.* nisi $a = a'$, siue formae (a, h, o), (a', h, o) identicae, contra hyp.

Hinc sequentia problemata, quae pro determinantibus non-quadratis multo maiorem difficultatem facessebant, nullo negotio solui poterunt.

I. *Propositis duabus formis* F, F' *eiusdem determinantis quadrati, inuestigare an proprie aequiualeant.* Quaerantur duae formae reductae formis F, F' resp. proprie aequiualentes; quae si identicae sunt, propositae proprie aequiualentes erunt, sin minus, non erunt.

II. *Iisdem positis inuestigare an improprie aequiualeant.* Sit forma alterutri propositarum *e. g.* formae F opposita, G; quae si formae F' proprie aequiualet, F et F' improprie aequiualebunt, et contra.

208. Problema. *Propositis duabus formis F, F' determinantis hh proprie aequiualentibus: inuenire transformationem propriam alterius in alteram.*

Sol. Formae F proprie aequiualeat forma reducta Φ, quae itaque per hyp. etiam formae F' proprie aequiualebit. Quaeratur per art. 206 transformatio propria formae F in Φ, quae sit $\alpha, \mathfrak{c}, \gamma, \delta$; nec non transformatio propria formae F' in Φ, quae sit $\alpha', \mathfrak{c}', \gamma', \delta'$. Tunc Φ transformabitur in F' per substitutionem propriam $\delta', -\mathfrak{c}', -\gamma', \alpha'$ et hinc F in F' per substitutionem propriam $\alpha\delta' - \mathfrak{c}\gamma', \mathfrak{c}\alpha' - \alpha\mathfrak{c}', \gamma\delta' - \delta\gamma', \delta\alpha' - \gamma\mathfrak{c}'$.

Operae pretium est, aliam formulam pro hac transformatione formae F in F' euoluere, ad quam formam reductam Φ ipsam nouisse ne opus quidem sit. Ponamus formam F esse (a', b', c), $F' = (a', b', c')$, $\Phi = (A, h, o)$. Quoniam rationibus $h - b : a$ vel $c : -(h+b)$ in numeris minimis aequalis est ratio $\mathfrak{c} : \delta$, facile perspicitur $\frac{h-b}{\mathfrak{c}} = \frac{a}{\delta}$ fore *integrum*, qui sit f; nec non $\frac{c}{\mathfrak{c}} = \frac{-h-b}{\delta}$ integrum fore qui ponatur $= g$. Habebitur autem $A = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$ adeoque $\mathfrak{c}A = u\alpha\alpha\mathfrak{c} + 2b\alpha\mathfrak{c}\gamma + c\mathfrak{c}\gamma\gamma$, siue (substitutis pro $a\mathfrak{c}$, $\delta(h-b)$, pro c, $\mathfrak{c}g$,) $\mathfrak{c}A = \alpha\alpha\delta h + b(2\mathfrak{c}\gamma - \alpha\delta)\alpha + \mathfrak{c}\mathfrak{c}\gamma\gamma g$ siue (propter $b = -h - \delta g$), $\mathfrak{c}A = 2\alpha(\alpha\delta - \mathfrak{c}\gamma)h + (\alpha\delta - \mathfrak{c}\gamma)^2 g = 2\alpha h + g$. Simili modo $\delta A = a\alpha\alpha\delta + 2b\alpha\mathfrak{c}\delta + c\gamma\gamma\delta = \alpha\alpha\delta\delta f + b(2\alpha\delta - \mathfrak{c}\gamma\gamma) - \mathfrak{c}\gamma\gamma h = (\alpha\delta - \mathfrak{c}\gamma)^2 f + 2\gamma(\alpha\delta - \mathfrak{c}\gamma)h = 2\gamma h + f$. Quare $\alpha = \frac{\mathfrak{c}A - g}{2h}$, $\gamma = \frac{\delta A - f}{2h}$.

Prorsus eodem modo positis $\frac{h-b'}{c'} = \frac{a'}{\delta'} = f'$, $\frac{c'}{c'}$ $= \frac{-h-b'}{\delta'} = g'$ fit $\alpha' = \frac{c'A-g'}{2h}$, $\gamma' = \frac{\delta'A-f'}{2h}$. Quibus valoribus ipsorum $\alpha, \gamma, \alpha' \gamma'$ in formula modo tradita pro transformatione formae F in F' substitutis, transit in hanc:

$\frac{cf'-\delta'g}{2h}$, $\frac{c'g-cg'}{2h}$, $\frac{\delta f'-\delta' f}{2h}$, $\frac{c'f-\delta g'}{2h}$, ex qua A omnino abiit.

Si duae formae F, F' improprie aequiualentes proponuntur, et transformatio impropria alterius in alteram quaeritur, sit forma G opposita forma F, et transformatio propria formae G in F' haec $\alpha, c, \gamma, \delta$. Tunc manifestum est $\alpha, c, -\gamma, -\delta$ fore transformationem impropriam formae F in F'.

Denique patet, si formae propositae et proprie et improprie aequiualentes sint, hoc modo inuenire posse transformationes duas alteram propriam alteram impropriam.

209. Nihil itaque iam superest quam vt ex vna transformatione omnes reliquas similes deducere doceamus. Hoc vero pendet a solutione aequationis indeterminatae $tt - hhuu = mm$, designante m diuisorem communem maximum numerorum $a, 2b, c$, si (a, b, c) est alterutra formarum aequiualentium. Sed haec aequatio semper duobus tantum modis solui potest, nempe ponendo aut $t = m$, $u = 0$, aut $t = -m$, $u = 0$. Ponamus

enim dari adhuc aliam solutionem $t = T$, $u = U$, ita vt U non $= 0$. Quia mm ipsum $4hh$ certo metitur, erit $\frac{4TT}{mm} = \frac{4hhUU}{mm} = 4$, atque tum $\frac{4TT}{mm}$ tum $\frac{4hhUU}{mm}$ quadrata integra. Sed nullo negotio perspicitur, numerum 4 duorum quadratorum integrorum differentiam esse non posse, nisi quadratum minus sit 0 i. e. $U = 0$, contra hyp. — Si itaque forma F in formam F' per substitutionem $\alpha, \mathfrak{b}, \gamma, \delta$ transit, alia transformatio huic similis non dabitur praeter transformationem $-\alpha, -\mathfrak{b}, -\gamma, -\delta$. Quare si duae formae aut proprie tantum, aut improprie tantum aequiualent, *duae* tantum transformationes dabuntur; si vero tum proprie tum improprie, *quatuor*, nempe duae propriae duaeque impropriae.

210. Theorema. *Si duae formae reductae* (a, h, o), $(a', h. o)$ *improprie sunt aequiualentes, erit* $aa' \equiv mm \pmod{2mh}$, *designante m diuisorem communem maximum numerorum* a, $2h$, *vel* a', $2h$; *et vice versa, si* a, $2h$; a', $2h$ *eundem diuisorem communem maximum m habent, atque est* $aa' \equiv mm \pmod{2mh}$, *formae* (a, h, o), (a', h, o) *improprie aequiualentes erunt.*

Dem. I. Transeat forma (a, h, o) in formam (a', h, o) per substitutionem impropriam $\alpha, \mathfrak{b}, \gamma, \delta$ ita vt habeantur quatuor aequationes $a\alpha\alpha + 2h\alpha\gamma = a' \ldots [1]$; $a\alpha\mathfrak{b} + h(\alpha\delta + \mathfrak{b}\gamma) = h \ldots [2]$; $a\mathfrak{b}\mathfrak{b} + 2h\mathfrak{b}\delta = 0 \ldots [3]$; $a\delta - \mathfrak{b}\gamma = -1 \ldots [4]$. Hinc sequitur, multiplicando [4] per h et subtrahendo a [2], quod ita exprimimus [2] $- h$ [4], ... $(a\alpha + 2h\gamma)\mathfrak{b} = 2h \ldots [5]$; similiter ex $\gamma\delta$ [2] —

$\gamma\gamma$ [3] — $(a + a\alpha\gamma + h\gamma\delta)$ [4] deletis quae sese destruunt ... — $a\alpha\delta = a + 2h\gamma\delta$, siue — $(a\alpha + 2h\gamma)\delta = a$ ... [6]; denique ex a [1] ... $a\alpha(a\alpha + 2h\gamma) = aa'$, siue $(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$ siue $(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)}$ ... [7]. Iam ex [5] et [6] sequitur $a\alpha + 2h\gamma$ metiri ipsos $2h$ et a, adeoque etiam ipsum m, qui est diuisor communis maximus ipsorum a, $2h$; manifesto autem m metietur etiam ipsum $a\alpha + 2h\gamma$; quare necessario $a\alpha + 2h\gamma$ erit aut $= +m$ aut $= -m$. Hinc statim sequitur ex [7], $mm \equiv aa' \pmod{2mh}$. *Q. E. P.*

II. Si a, $2h$; a', $2h$ eundem diuisorem communem maximum m habent, insuperque est $aa' \equiv mm \pmod{2mh}$, $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa' - mm}{2mh}$ erunt integri. Facile vero confirmatur, formam (a, h, o) transire in (a', h, o) per substitutionem $-\frac{a'}{m}$, $-\frac{2h}{m}$, $\frac{aa' - mm}{2mh}$, $\frac{a}{m}$; nec non hanc transformationem esse impropriam. Quare formae illae erunt improprie aequiualentes. *Q. E. S.*

Hinc etiam statim diiudicari potest, an forma aliqua reducta data (a, h, o) sibi ipsi improprie aequiualens sit. Scilicet designato diuisore communi maximo numerorum a, $2h$ per m, esse debebit $aa \equiv mm \pmod{2mh}$.

211. Omnes formae reductae determinantis dati hh obtinentur, si in forma indefinita (A, h, a) pro A omnes numeri a o vsque ad $2h - 1$ incl. substituuntur, quarum itaque multitudo erit $2h$. Perspicuum est omnes formas determinantis hh

in totidem *classes* distribui posse, hasque iisdem proprietatibus praeditas fore quas supra (artt. 175, 195) pro classibus formarum determinantis negatiui, et positiui non quadrati attigimus. Ita omnes formae determinantis 25 in decem classes distribuentur, quae per formas reductas in singulis contentas distingui poterunt. Hae formae reductae sunt: (0, 5, 0), (1, 5, 0), (2, 5, 0), (5, 5, 0), (8, 5, 0), (9, 5, 0), quae sibi ipsae simul improprie aequiualent; (3, 5, 0) cui improprie aequiualet (7, 5, 0); (4, 5, 0) cui improprie aequiualet (6, 5, 0).

212. Problema. *Inuenire omnes repraesentationes numeri dati M per formam datam axx + 2bxy + cyy determinantis hh.*

Solutio huius problematis ex principiis art. 165 prorsus eodem modo peti potest, vt supra (artt. 180, 181, 205) pro formis determinantis negatiui et positiui non quadrati ostendimus; quod, quum nulli difficultati sit obnoxium, hic repetere superfluum esset. Contra haud abs re erit, solutionem ex alio principio quod casui praesenti proprium est deducere.

Positis vt artt. 206, 208, $h-b : a = c : -(h+b) = \mathfrak{e} : \mathfrak{d}$; $\frac{h-b}{\mathfrak{e}} = \frac{a}{\mathfrak{d}} = f$; $\frac{c}{\mathfrak{e}} = \frac{-h-b}{\mathfrak{d}} = g$, nullo negotio probatur, formam propositam esse productum ex factoribus $\mathfrak{d}x - \mathfrak{e}y$ et $fx - gy$. Vnde manifestum est, quamuis repraesentationem numeri M per formam propositam praebere resolutionem numeri M in binos fa-

ctores. Si itaque omnes diuisores numeri M sunt d, d', d'' etc. (inclusis etiam 1, et M, et singulis *bis* sumtis puta tum positiue tum negatiue), patet omnes repraesentationes numeri M obtineri, si successiue ponatur $\delta x - \mathfrak{G}y = d$, $fx - gy = \frac{M}{d}$; $\delta x - \mathfrak{G}y = d'$, $fx - gy = \frac{M}{d'}$ etc., valores ipsorum x, y hinc euoluantur, eaeque repraesentationes eiiciantur vbi x aut y valores fractos obtinent. Manifesto vero ex duabus primis aequationibus sequitur $x = \frac{\mathfrak{G}M - \delta dd}{(\mathfrak{G}f - \delta g)d}$, et $y = \frac{\delta M - \mathfrak{G}dd}{(\mathfrak{G}f - \delta g)d}$, quos valores semper *determinatos* fore inde manifestum quod $\mathfrak{G}f - \delta g = 2h$, adeoque numerator certo non $= 0$. — Ceterum ex eodem principio, puta resolubilitate cuiusuis formae determinantis quadrati in binos factores, etiam reliqua problemata solui potuissent: sed methodo ei quam supra pro formis determinantis non quadrati tradidimus analoga etiam hic vti maluimus.

Ex. Quaeruntur omnes repraesentationes numeri 12 per formam $3xx + 4xy - 7yy$. Haec resoluitur in factores $x - y$ et $3x + 7y$. Omnes diuisores numeri 12 sunt $\pm$ 1, 2, 3, 4, 6, 12. Positis $x - y = 1$, $3x + 7y = 12$ fit $x = \frac{19}{10}$, $y = \frac{9}{10}$, qui valores tamquam fracti sunt reiiciendi. Eodem modo ex diuisoribus -1, ± 3, ± 4, ± 6, ± 12 valores inutiles obtinentur; ex diuisore $+2$ vero obtinentur valores $x = 2$, $y = 0$, et ex diuisore -2 hi $x = -2$, $y = 0$; praeter has duas repraesentationes igitur aliae non dantur.

Methodus haec adhiberi nequit, si $M = 0$. In hoc casu manifestum est omnes valores ipsorum x, y aut aequationi $\delta x - \gamma y = 0$, aut huic $fx - gy = 0$ satisfacere debere. Omnes autem solutiones aequationis prioris continentur in formula $x = \gamma z$, $y = \delta z$, designante z indefinite numerum integrum quemcunque (siquidem vti supponitur γ, δ inter se primi sunt); similiterque ponendo diuisorem communem maximum numerorum f, g, $= m$, omnes solutiones aequationis posterioris exhibebuntur per formulam $x = \frac{gz}{m}$, $y = \frac{hz}{m}$. Quare hae duae formulae generales omnes repraesentationes numeri M in hoc casu complectentur.

* * *

In praecedentibus omnia quae ad cognoscendam aequiualentiam et ad inueniendas omnes transformationes formarum nec non ad repraesentationes omnes numerorum datorum per formas datas indagandas pertinent, ita sunt explicata, vt nihil amplius desiderari posse videatur. Superest itaque tantummodo, vt propositis duabus formis quae propter *determinantium inaequalitatem* aequiualentes esse nequeunt, diiudicare doceamus, annon altera sub altera contenta sit, et in hoc casu omnes transformationes illius in hanc inuenire.

213. Supra artt. 157, 158 ostendimus, si forma f determinantis D formam F determinantis E implicet atque in ipsam transeat per substitutionem α, γ, γ, δ, fore $E = (\alpha\delta - \gamma\gamma)^2 D$; si fue-

$\alpha\delta - \beta\gamma = \pm 1$, formam f non modo implicare formam F sed ipsi aequiualentem esse et proin si f ipsam F implicet neque vero eidem aequiualeat, quotientem $\frac{E}{D}$ esse integrum maiorem quam 1. Problema itaque hic soluendum erit, *diiudicare an forma data f determinantis D formam datam F determinantis Dee implicet*, vbi e supponitur esse numerus positiuus maior quam 1. Hoc negotium ita absoluemus, vt multitudinem finitam formarum sub f contentarum assignare doceamus quae ita sint comparatae, vt F si sub f contenta est necessario alicui ex illis aequiualere debeat.

I. Ponamus omnes diuisores (positiuos) numeri e (inclusis etiam 1 et e) esse m, m', m'' etc., atque $e = mn = m'n' = m''n''$ etc. Designemus breuitatis gratia formam in quam f transit per substitutionem propriam m, 0, 0, n ita $(m; 0)$, formam in quam f transit per substitutionem propriam m, 1, 0, n per $(m; 1)$ etc. generaliterque formam in quam f per subst. propriam, m k, 0, n transmutatur per $(m; k)$. Simili modo transeat f per subst. propriam m', 0, 0, n' in $(m'; 0)$; per hanc m', 1, 0, n' in $(m'; 1)$; etc., per m'', 0, 0, n'' in $(m''; 0)$ etc. etc. Omnes hae formae sub f proprie contentae erunt, et cuiusuis determinans $= Dee$. Complexum omnium formarum $(m; 0), (m; 1), (m; 2) \ldots (m; m - 1)$ $(m'; 0), (m'; 1) \ldots (m'; m' - 1); (m''; 0)$ etc. quarum multitudo erit $m + m' + m''$ + etc. et quas omnes inter se diuersas fore facile perspicitur, designemus per Ω.

Si *e. g.* forma f est haec $(2, 5, 7)$ atque $e = 5$, Ω comprehendet sequentes sex formas $(1; 0)$; $(5; 0)$, $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$ quae si euoluuntur sunt $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$

II. Iam dico, si forma F determinantis Dee sub f proprie contenta sit, necessario eandem alicui formarum Ω proprie aequiualentem fore. Ponamus formam f transformari in F per substitutionem propriam $\alpha, \mathfrak{C}, \gamma, \mathfrak{d}$, eritque $\alpha\mathfrak{d} - \mathfrak{C}\gamma = e$. Sit numerorum $\gamma, \mathfrak{d}$ (qui ambo simul 0 esse nequeunt) diuisor communis maximus positiue acceptus $= n$, atque $\frac{e}{n} = m$, qui manifesto erit integer. Accipiantur g, h ita vt sit $\gamma g + \mathfrak{d}h = n$, denique sit k residuum minimum positiuum numeri $\alpha g + \mathfrak{C}h$ secundum modulum m. Tum forma $(m; k)$ quae manifesto erit inter formas Ω, formae F proprie aequiualebit, et quidem in ipsam transformabitur per substitutionem propriam $\frac{\gamma}{n} \cdot \frac{\alpha g + \mathfrak{C}h - k}{m} + h, \frac{\mathfrak{d}}{n} \cdot \frac{\alpha g + \mathfrak{C}h - k}{m} - g$, $\frac{\gamma}{n}, \frac{\mathfrak{d}}{n}$. Nam *primo* perspicuum est hos quatuor numeros esse integros; *secundo* facile confirmatur substitutionem esse propriam; *tertio* patet, formam in quam $(m; k)$ per substitutionem illam transeat eandem esse in quam f *) transeat per substitutionem $m\left(\frac{\gamma}{n} \cdot \frac{\alpha g + \mathfrak{C}h - k}{m} + h\right) +$

*) Quippe quae per substitutionem m, k, o, n, in $(m; k)$ transit V, art. 159.

$\frac{k\gamma}{n}$, $m\left(\frac{\delta}{n}\cdot\frac{\alpha g+\mathfrak{C}h-k}{m}-g\right)+\frac{k\delta}{n}$, γ, δ siue quoniam $mn = e = \alpha\delta-\mathfrak{C}\gamma$ adeoque $\mathfrak{C}\gamma + mn = \alpha\delta$, $\alpha\delta - mn = \mathfrak{C}\gamma$, per hanc $\frac{1}{n}(\alpha\gamma g + \alpha\delta h)$, $\frac{1}{n}(\mathfrak{C}\gamma g + \mathfrak{C}\delta h)$, γ, δ, siue denique quoniam $\gamma g+\delta h = n$, per hanc α, $\mathfrak{C}$, γ, δ i. e. per hyp., in F. Quare $(m; k)$ et F proprie aequiualentes erunt. *Q. E. D.*

Ex his igitur semper diiudicari potest, an forma aliqua data f determinantis D formam F determinantis *Dee* proprie implicet. Si vero quaeritur an f ipsam F improprie implicet, inuestigari tantummodo debet an forma ipsi F opposita sub f proprie contenta sit, art. 159.

214. Problema. *Propositis duabus formis, f, determinantis D, et F determinantis Dee, quarum prior posteriorem proprie implicat: exhibere omnes transformationes proprias formae f in F.*

Sol. Designante Ω eundem formarum complexum vt in art. praec., excerpantur ex hoc complexu omnes formae quibus F proprie aequiualet, quae sint Φ, Φ', Φ'' etc. Quaeuis harum formarum sequenti modo suppeditabit transformationes proprias formae f in F, et quidem aliae alias (i. e. singulae diuersas), cunctae vero cunctas (i. e. nulla transformatio propria formae f in F erit quam non vna ex formis Φ, Φ' etc. praebeat). Quoniam methodus pro omnibus formis Φ, Φ' etc. eadem est, de vna tantum loquemur.

Ponamus Φ esse $(M; K)$, atque $e = MN$ ita vt f in Φ per substitutionem propriam M, K, o, N transeat. Porro designentur omnes transformationes propriae formae Φ in F indefinite per $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$. Tum manifesto f transibit in Φ per substitutionem propriam $M\mathfrak{a} + K\mathfrak{c}$, $M\mathfrak{b} + K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$, et hoc modo ex quauis transformatione propria formae Φ in F sequetur transformatio propria formae f in F. — Eodem modo tractandae sunt formae reliquae Φ', Φ'' etc., quarum singulae transformationes propriae in F transformationem propriam formae f in F praebebunt.

Vt appareat hanc solutionem ex omni parte completam esse, ostendendum erit

I. *Hoc modo omnes transformationes proprias possibiles formae f in F obtineri.* Sit transformatio quaecunque propria formae f in F haec α, $\mathfrak{C}$, γ, δ atque vt in art. praec. II, n diuisor communis maximus numerorum γ, δ; numeri m, g, h, k autem eodem modo vt illic determinati. Tunc forma $(m; k)$ erit inter formas Φ, Φ' etc., et $\frac{\gamma}{n} \cdot \frac{\alpha\gamma + \mathfrak{C}h - k}{m} + h$, $\frac{\delta}{n} \cdot \frac{\alpha\gamma + \mathfrak{C}h - k}{m} - g$, $\frac{\gamma}{n}$, $\frac{\delta}{n}$ aliqua ex transformationibus propriis huius formae in F; ex hac vero per regulam modo traditam obtinetur transformatio α, $\mathfrak{C}$, γ, δ; haec omnia in art. praec. sunt demonstrata.

II. *Omnes transformationes hoc modo prodeuntes inter se diuersas esse, seu nullam bis obtineri.* Nullo quidem negotio perspicitur, plures transformationes diuersas eiusdem formae Φ,

vel Φ' etc. in F eandem transformationem formae f in F producere non posse; quod vero etiam formae diuersae e. g. Φ et Φ' eandem transformationem suppeditare nequeant, ita demonstratur. Supponamus, transformationem propriam $\alpha, \mathfrak{C}, \gamma, \delta$ formae f in F obtineri *tum* ex transformatione propria $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ formae Φ in F, *tum* ex transformatione propria $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \mathfrak{d}'$ formae Φ' in F. Sit $\Phi = (M; K)$, $\Phi' = (M'; K')$, $e = MN = M'N'$. Habebuntur itaque aequationes $\alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' \ldots [1]$, $\mathfrak{C} = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}' \ldots [2]$, $\gamma = N\mathfrak{c} = N'\mathfrak{c}' \ldots [3]$, $\delta = N\mathfrak{d} = N'\mathfrak{d}' \ldots [4]$, $\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1 \ldots [5]$. Ex $\mathfrak{a}[4] - \mathfrak{b}[3]$ sequitur adiumento aequ. [5], $N = N'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}')$, quare N' metietur ipsum N; similiter ex $\mathfrak{a}'[4] - \mathfrak{b}'[3]$ fit $N(\mathfrak{a}'\mathfrak{d} - \mathfrak{b}'\mathfrak{c}) = N'$, quare N metietur ipsum N', vnde, quia tum N tum N' supponuntur esse positiui, erit necessario $N = N'$, et $M = M'$, et hine ex 3 et 4, $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{d} = \mathfrak{d}'$. Porro fit ex $\mathfrak{a}[2] - \mathfrak{b}[1]$, $K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$, hinc $K \equiv K' \pmod{M}$ quod fieri nequit nisi $K = K'$, quia tum K tum K' iacent inter limites 0 et $M - 1$. Quamobrem formae Φ, Φ' non sunt diuersae, contra hyp.

Ceterum patet, si D fuerit negatiuus vel positiuus quadratus, per methodum hanc omnes transformationes proprias formae f in F reuera inueniri posse; si vero D positiuus non-quadratus, formulae certae generales assignari poterunt in quibus omnes transformationes propriae (quarum multitudo infinita) contentae erunt.

Denique, si forma F improprie sub forma f contenta est, omnes transformationes impropriae illius in hanc per methodum traditam facile exhiberi poterunt. Scilicet si $\alpha, \mathfrak{G}, \gamma, \delta$ indefinite omnes transformationes proprias formae f in formam quae formae F opposita est, designare supponitur: omnes transf. impropriae formae f in F exhibebuntur per $\alpha, -\mathfrak{G}, \gamma, -\delta$.

Ex. Desiderantur omnes transformationes formae $(2, 5, 7)$ in $(275, 0 - 1)$, quae sub illa tum proprie tum improprie contenta est. Complexum formarum Ω pro hoc casu iam in art. praec. tradidimus; examine instituto inuenitur, tum $(5; 1)$ tum $(5; 4)$ formae $(275, 0, -1)$ proprie aequiualere. Omnes transformationes propriae formae $(5; 1)$ *i. e.* $(50, 35, 19)$ in $(275, 0, -1)$ per theoriam nostram supra explicatam inueniuntur contineri sub formula generali $16t - 275u, -t + 16u, -15t + 275u, t - 15u$, vbi t, u designant indefinite omnes numeros integros aequationi $tt - 275uu = 1$ satisfacientes; quare omnes transformationes propriae formae $(2, 5, 7)$ in $(275, 0, -1)$ hinc oriundae contentae erunt sub formula generali $65t - 1100u, -4t + 65u, -15t + 275u, t - 15u$. Simili modo omnes transformationes propriae formae $(5; 4)$ *i. e.* $(50, 65, 79)$ in $(275, 0, -1)$ continentur sub formula generali $14t + 275u, t + 14u, -15t - 275u, -t - 15u$, adeoque omnes transformationes propriae formae $(2, 5, 7)$ in $(275, 0, -1)$ hinc oriundae sub hac $10t + 275u, t + 10u, -15t - 275u, -t - 15u$. Hae duae formulae igitur omnes

transformationes proprias quaesitas amplectuntur. — Eodem vero modo inuenitur omnes transformationes improprias formae $(2, 5, 7)$ in $(275, 0, -1)$ sub sequentibus duabus formulis contentas esse: (I) ... $65t - 1100n$, $4t - 65u$, $-15t + 275u$, $-t + 15u$; et (II) ... $10t + 275u$, $-t - 10u$, $-15t - 275u$, $t + 15u$.

215. Hucusque formas determinantis 0 ab omnibus disquisitionibus exclusimus; de his itaque, vt theoria nostra ab omni parte completa euadat, quaedam adhuc sunt adiicienda. Quoniam generaliter demonstratum est, si forma aliqua determinantis D formam determinantis D' implicet, D' esse multiplum ipsius D, statim patet formam cuius determinans $= 0$ aliam formam quam cuius determinans etiam sit $= 0$ implicare non posse. Quare duo tantummodo problemata soluenda restant, scilicet 1° *propositis duabus formis f, F, quarum posterior habet determinantem* 0, *diiudicare vtrum prior posteriorem implicet necne, et in illo casu omnes transformationes illius in hanc exhibere.* 2° *Inuenire omnes repraesentationes numeri dati per formam datam determinantis* 0. Problema primum aliam methodum requirit, quando determinans prioris formae f etiam est 0, aliam quando non est 0. Haec omnia iam exponemus.

I. Ante omnia obseruamus, quamuis formam $axx + 2bxy + cyy$, cuius determinans $bb - ac = 0$, ita exhiberi posse $m(gx + hy)^2$, denotantibus g, h numeros inter se primos, m integrum. Sit enim m diuisor communis maxi-

mus ipsorum a, c eodem signo acceptus quo hi numeri ipsi sunt affecti (hos signa opposita habere non posse facile perspicitur), eruntque $\frac{a}{m}$, $\frac{c}{m}$ integri inter se primi non negatiui, productum ex ipsis $= \frac{bb}{mm}$ i. e. quadratum, adeoque illi ipsi quadrata (art. 21). Sit $\frac{a}{m} = gg$, $\frac{b}{m} = hh$, eruntque etiam g, h inter se primi, $gghh = \frac{bb}{mm}$, et $gh = \pm \frac{b}{m}$. Hinc patet $m(gx \pm hy)^2$ fore $= axx + 2bxy + cyy$.

Iam propositae sint duae formae f, F, vtraque determinantis o, et quidem sit $f = m(gx + hy)^2$, $F = M(GX + HY)^2$, ita vt g ad h, G ad H sint primi. Tum dico si forma f implicet formam F, m aut ipsi M aequalem esse aut saltem ipsum M metiri et quotientem esse quadratum; et vice versa si $\frac{M}{m}$ sit quadratum integrum, F contentam esse sub f. Si enim f per substitutionem $x = \alpha X + \mathfrak{G} Y$, $y = \gamma X + \delta Y$ in F transire supponitur, erit $\frac{M}{m}(GX+HY)^2 = ((\alpha g + \gamma h) X + (\mathfrak{G} g + \delta h) Y)^2$, vnde facile sequitur $\frac{M}{m}$ esse quadratum. Ponatur $= ee$, eritque $e(GX+HY) = \pm ((\alpha g + \gamma h) X + (\mathfrak{G} g + \delta h) Y)$, i. e. $\pm eG = \alpha g + \gamma h$, $\pm eH = \mathfrak{G} g + \delta h$; si itaque $\mathfrak{G}$, $\mathfrak{H}$ ita determinantur vt sit $\mathfrak{G} G + \mathfrak{H} H = 1$, erit $\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\mathfrak{G} g + \delta h)$, adeoque *integer*. *Q. E. P.* — Si

vero, vice versa, supponitur, $\frac{M}{m}$ esse quadratum integrum $= ee$, forma f implicabit formam F. Scilicet integri $\alpha, \mathfrak{C}, \gamma, \delta$ ita poterunt determinari vt fiat $\alpha g + \gamma h = \pm eG$, $\mathfrak{C}g + \delta h = \pm eH$. Accipiantur enim integri $\mathfrak{g}$, $\mathfrak{h}$ ita vt fiat $\mathfrak{g}g + \mathfrak{h}h = 1$, satisfietque aequationibus illis ponendo $\alpha = \pm eG\mathfrak{g} + hz$, $\mathfrak{h} = \pm eG\mathfrak{h} - gz$, $\mathfrak{C} = \pm eH\mathfrak{g} + hz'$, $\delta = \pm eH\mathfrak{h} - gz'$, quicunque valores integri ipsis z, z' tribuantur; quare F contenta erit sub f, *Q. E. S.* Simul haud difficulter intelligitur, has formulas omnes valores quas $\alpha, \mathfrak{C}, \gamma, \delta$ nancisci possunt, i. e. omnes transformationes formae f in F exhibere, si modo z, z' indefinite omnes numeros integros exhibere supponantur.

II. Propositis duabus formis $f = axx + 2bxy + cyy$ cuius determinans non $= 0$, et $F = M(GX + HY)^2$ cuius determinans $= 0$ (designantibus vt ante G, H numeros inter se primos), dico *primo*, si f implicet ipsam F, numerum M per formam f repraesentari posse; *secundo*, si M per f repraesentari possit, F sub f contentam esse; *tertio*, si in hoc casu omnes repraesentationes numeri M per formam f indefinite exhibeantur ita $x = \xi$, $y = \upsilon$, omnes transformationes formae f in F exhiberi ita $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$. Quae omnia sequenti modo demonstramus.

1° Ponamus f transire in F per substitutionem $\alpha, \mathfrak{C}, \gamma, \delta$, accipianturque numeri $\mathfrak{G}$, $\mathfrak{H}$ ita vt sit $\mathfrak{G}G + \mathfrak{H}H = 1$. Tunc manifestum est,

si ponatur $x = \alpha\mathfrak{G} + \mathfrak{C}\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, valorem formae f fieri M, adeoque M repraesentabilem esse per formam f.

2° Si supponitur esse $a\xi\xi + 2b\xi\upsilon + c\upsilon\upsilon = M$, manifestum est per substitutionem $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$, formam f transire in F. Quod vero

3° in hoc casu substitutio $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$ *omnes* transformationes formae f in F exhibeat, si ξ, υ supponantur exhibere omnes valores ipsorum x, y, qui faciunt $f = M$, ita perspicitur. Sit α, $\mathfrak{C}$, γ, δ transformatio quaecunque formae f in F, et vt ante $\mathfrak{G}G + \mathfrak{H}H = 1$. Tum inter valores ipsorum x, y erunt etiam hi, $x = \alpha\mathfrak{G} + \mathfrak{C}\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, ex quibus obtinetur substitutio $G(\alpha\mathfrak{G} + \mathfrak{C}\mathfrak{H})$, $H(\alpha\mathfrak{G} + \mathfrak{C}\mathfrak{H})$, $G(\gamma\mathfrak{G} + \delta\mathfrak{H})$, $H(\gamma\mathfrak{G} + \delta\mathfrak{H})$, siue $\alpha + \mathfrak{H}(\mathfrak{C}G - \alpha H)$, $\mathfrak{C} + \mathfrak{G}(\alpha H - \mathfrak{C}G)$, $\gamma + \mathfrak{H}(\delta G - \gamma H)$, $\delta + \mathfrak{G}(\gamma H - \delta G)$. Sed quoniam $a(\alpha X + \mathfrak{C}Y)^2 + 2b(\alpha X + \mathfrak{C}Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 = M(GX + HY)^2$ erit $a(\alpha\delta - \mathfrak{C}\gamma)^2 = M(\delta G - \gamma H)^2$, $c(\mathfrak{C}\gamma - \alpha\delta)^2 = M(\mathfrak{C}G - \alpha H)^2$, adeoque (quum determinans formae f per $(\alpha\delta - \mathfrak{C}\gamma)^2$ multiplicatus aequalis sit determinanti formae F i. e. $= 0$, adeoque etiam $\alpha\delta - \mathfrak{C}\gamma = 0$), $\delta G - \gamma H = 0$, $\mathfrak{C}G - \alpha H = 0$. Hinc substitutio illa transit in hanc α, $\mathfrak{C}$, γ, δ, vnde patet, formulam traditam *omnes* transformationes formae f in F suppeditare.

III. Superest vt omnes repraesentationes numeri dati per formam datam determinantis 0 exhibere doceamus. Sit forma haec $m(gx +$

$hy)^2$, patetque statim, numerum illum per m diuisibilem, et quotientem quadratum esse debere. Si itaque numerus propositus statuitur $= mee$, perspicuum est, pro quibus valoribus ipsorum x, y fiat $m(gx + hy)^2 = mee$, pro iisdem fieri $gx + hy$ aut $= + e$, aut $= - e$. Quare omnes repraesentationes habebuntur, si omnes solutiones aequationum linearium $gx + hy = e$, $gx + hy = - e$ in integris, sunt inuentae. Has vero solubiles esse constat (siquidem g, h sunt inter se primi vt supponitur). Scilicet si $\mathfrak{g}$, $\mathfrak{h}$ ita determinantur vt sit $\mathfrak{g}g + \mathfrak{h}h = 1$, aequationi priori satisfiet ponendo $x = \mathfrak{g}e + \mathfrak{h}z$, $y = \mathfrak{h}e - \mathfrak{g}z$; posteriori vero faciendo $x = - \mathfrak{g}e + \mathfrak{h}z$, $y = - \mathfrak{h}e - \mathfrak{g}z$, denotante z integrum quemcunque. Simul vero formulae hae *omnes* valores integros ipsorum x, y exhibent, si z indefinite numerum quemuis integrum designare supponitur.

* * *

His disquisitionibus coronidis loco apponimus

216. Problema. *Inuenire omnes solutiones aequationis generalis *) indeterminatae secundi gradus duas incognitas implicantis*

$$axx + 2bxy + cyy + 2dx + 2ey + f = 0$$

(vbi a, b, c etc. sunt integri quicunque dati) per numeros integros.

*) Si aequatio proponeretur in qua coefficiens secundus, quartus vel quintus non esset par, multiplicata per 2 eam formam reciperet quam hic supponimus.

Sol. Introducamus loco incognitarum x, y alias $p = (bb - ac)\, x + be - cd$, et $q = (bb - ac)\, y + bd - ae$, qui manifesto semper erunt integri, quando x, y sunt integri Quo facto habebitur aequatio $app + 2bpq + cqq + (bb - ac)\,(aee - 2bde + cdd) = 0$, siue posito breuitatis gratia numero $(bb - ac)\,(aee - 2bde + cdd) = -M$, haec $app + 2bpq + cqq = M$. Iam omnes solutiones huius aequationis, i. e. omnes repraesentationes numeri M per formam (a, b, c) in praecedentibus inuenire docuimus. Si vero ex singulis valoribus ipsorum p, q, valores respondentes ipsorum x, y adiumento aequationum $x = \frac{p + cd - be}{bb - ac}$, $y = \frac{q + ae - bd}{bb - ac}$ determinantur, facile perspicitur, omnes hos valores aequationi propositae satisfacere, et nullos valores integros ipsorum x, y dari qui hoc modo non obtineantur. Si itaque ex omnibus valoribus ipsorum x, y sic prodeuntibus valores fractos eiicimus, omnes solutiones quaesitae remanebunt.

Circa hanc solutionem sequentia sunt obseruanda.

1° Si aut M per formam (a, b, c) repraesentari non potest, aut ex nulla repraesentatione valores *integri* ipsorum x, y sequuntur: aequatio in integris nullo modo solui poterit.

2° Quando determinans formae (a, b, c), i. e. numerus $bb - ac$ est negatiuus, vel positiuus quadratus simulque M non $= 0$: multitudo repraesentationum numeri M per formam (a, b, c)

erit finita, et proin etiam multitudo omnium solutionum aequationis propositae (si quae omnino dantur) finita erit.

3° Quando $bb - ac$ est positiuus non-quadratus, vel quadratus et simul $M = 0$: numerus M, si vllo modo, *infinitis modis diuersis* per formam (a, b, c) repraesentari poterit; sed quoniam impossibile est, has repraesentationes omnes *ipsas* inuenire et tentare vtrum valores integros ipsorum x, y praebeant an fractos, necessarium est regulam tradere, per quam, quando forte nulla omnino repraesentatio valores integros ipsorum x, y praebere potest, de hac re *certi* fieri possimus (nam quotcunque repraesentationes in hoc casu *tentatae* fuerint, absque tali regula ad certitudinem numquam peruenieremus); quando vero aliae repraesentationes dant valores integros ipsorum x, y, aliae fractos: docendum erit quomodo hae ab illis a priori generaliter dignosci possint.

4° Quando $bb - ac = 0$: valores ipsorum x, y per formulas praecedentes omnino non possunt determinari; quare pro hoc casu *methodus peculiaris* inuestigari debebit.

217. Pro eo casu, vbi $bb - ac$ est numerus positiuus non-quadratus, supra docuimus, omnes repraesentationes numeri M per formam $app + 2bpq + cqq$ (si quae omnino dentur) exhiberi posse, per vnam vel per plures formulas tales $p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u)$, $q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$, denotantibus $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ numeros integros da-

tos, m diuisorem communem maximum numerorum a, $2b$, c; denique t, u indefinite omnes numeros integros aequationi $tt - (bb - ac)\,uu = mm$ satisfacientes. Quoniam omnes valores ipsorum t, u tum positiue tum negatiue accipi possunt: pro singulis illarum formarum *quaternas* alias substituere poterimus, $p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u)$, $q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}n)$; $p = \frac{1}{m}(\mathfrak{A}t - \mathfrak{B}u)$, $q = \frac{1}{m}(\mathfrak{C}t - \mathfrak{D}u)$; $p = \frac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u)$, $q = \frac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u)$; $p = -\frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u)$, $q = -\frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$, ita vt multitudo omnium formularum nunc quater maior sit quam antea, t et u vero non amplius omnes numeros aequationi $tt - (bb - ac)\,uu = mm$ satisfacientes exprimant, sed positiuos tantum. Quaeuis harum formarum itaque seorsim considerari, et qui valores ipsorum t, u praebeant valores integros ipsorum x, y, inuestigari debebit.

Ex formula $p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u)$, $q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$ ... [1] sequuntur valores ipsorum x, y hi: $x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(bb - ac)}$, $y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(bb - ac)}$. Supra vero ostendimus, omnes valores (positiuos) ipsorum t constituere progressionem recurrentem t, t', t'' etc., similiter valores respondentes ipsius u quoque seriem recurrentem formare u, u', u'' etc.; praeterea assignari posse numerum ϱ ta-

lem, vt secundum modulum quemcunque datum fiat $t^{\varrho} \equiv t^{0}$, $t^{\varrho+1} \equiv t'$, $t^{\varrho+2} \equiv t''$ etc., $u^{\varrho} \equiv u^{0}$, $u^{\varrho+1} \equiv u'$ etc. Pro hoc modulo accipiemus numerum $m(bb - ac)$, designabimusque breuitatis gratia valores ipsorum x, y qui prodeunt ponendo $t = t^{0}$, $u = u^{0}$, et quibus tribuemus indicem 0, per x^{0}, y^{0}; similiterque eos qui prodeunt faciendo $t = t'$, $u = u'$, per x', y' quibus tribuemus indicem 1, etc. Tunc nullo negotio perspicietur, si x^{h}, y^{h} fuerint numeri integri atque ϱ rite determinatus, etiam $x^{h+\varrho}$, $y^{h+\varrho}$; nec non $x^{h+2\varrho}$, $y^{h+2\varrho}$ et generaliter $x^{h+k\varrho}$, $y^{h+k\varrho}$, integros fore; et contra si x^{h} vel y^{h} sit fractus, etiam $x^{h+k\varrho}$, vel $y^{h+k\varrho}$ fractum fore. Hinc facile concluditur, si valores ipsorum x, y, quibus indices $0, 1, 2 \ldots \varrho - 1$ competunt, euoluantur, et pro nullo horum indicum *tum* x, *tum* y integer sit, nullum omnino indicem dari, pro quo tum x, tum y valores integros recipiant, in quo casu ex formula [1] nulli valores integri ipsorum x, y deduci poterunt. Si vero inter illos indices aliqui sunt, puta μ, μ', μ'' etc. quibus valores integri ipsorum x, y respondent, omnes valores integri ipsorum x, y, qui quidem ex formula [1] obtineri possunt, ii erunt, quorum indices sub aliqua formularum $\mu + k\varrho$, $\mu' + k\varrho$, $\mu'' + k\varrho$ etc. sunt contenti, denotantae k indefinite omnes numeros integros positiuos, inclusa etiam cifra.

Formulae reliquae sub quibus valores ipsorum p, q contenti sunt, prorsus eodem modo sunt tractandae. Si contingeret, vt ex nulla omnium harum formularum valores integri ipsorum x, y

obtineantur, aequatio proposita in integris nullo prorsus modo solui posset; quoties vero reuera est solubilis, omnes solutiones in integris per praecepta in praecc. tradita exhiberi poterunt.

218. Quando $bb - ac$ est numerus quadratus atque $M = 0$, omnes valores ipsorum p, q comprehensi erunt sub duabus huiusmodi formulis $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, vbi z indefinite designat quemuis numerum integrum, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ vero sunt integri dati, quorum primus cum secundo, tertius cum quarto diuisorem communem non habent (art. 212). Omnes itaque valores integri ipsorum x, y ex formula prima oriundi contenti erunt sub formula [1]

$$x = \frac{\mathfrak{A}z + cd - he}{bb - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{bb - ac},$$

omnesque reliqui ex formula secunda oriundi sub hac [2]

$$x = \frac{\mathfrak{A}'z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{bb - ac}.$$

Sed quoniam vtraque formula etiam valores fractos praebere potest (nisi $bb - ac = 1$); opus est vt eos valores ipsius z, qui tum ipsum x tum ipsum y integrum reddunt, a reliquis in vtraque formula separemus; attamen sufficit primam solam considerare, quum pro altera prorsus eadem methodus adhibenda sit.

Quoniam $\mathfrak{A}$, $\mathfrak{B}$ inter se primi sunt, duos numeros a, b ita determinare licebit vt fiat $a\mathfrak{A} + b\mathfrak{B} = 1$. Quo facto habetur $(ax + by)(bb -$

$ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$, vnde statim patet, omnes valores ipsius z qui valores integros ipsorum x, y producere possint, necessario numero $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ sec. mod. $bb - ac$ congruos, siue sub formula $(bb - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ contentos esse debere, designante z' indefinite numerum integrum. Hinc facile loco formulae [1] obtinemus sequentem

$$x = \mathfrak{A}z' + \mathfrak{b} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$

$$y = \mathfrak{B}z' - \mathfrak{a} \times \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{bb - ac}$$

quam aut pro omnibus valoribus ipsius z' aut pro nullo valores integros ipsorum x, y praebere manifestum est, et quidem casus prior semper locum habebit quando $\mathfrak{A}(bd - ae)$ et $\mathfrak{B}(be - cd)$ sec. mod. $bb - ac$ sunt congrui, posterior quando sunt incongrui. — Prorsus eodem modo tractanda erit formula [2], solutionesque in integris (si quas praebere potest) a reliquis separandae.

219. Quando $bb - ac = 0$, forma $axx + 2bxy + cyy$ exhiberi poterit ita: $m(\alpha x + \mathfrak{c}y)^2$, vbi m, α, $\mathfrak{c}$ sunt integri (art. 215.). Ponatur $\alpha x + \mathfrak{c}y = z$, transitque aequatio proposita in hanc: $mzz + 2dx + 2ey + f = 0$, vnde et ex $z = \alpha x + \mathfrak{c}y$, deducitur

$$x = \frac{\mathfrak{c}mzz + 2ez + \mathfrak{c}f}{2\alpha e - 2\mathfrak{c}d}, \quad y = \frac{\alpha mzz + 2dz + \alpha f}{2\mathfrak{c}d - 2\alpha e}$$

Iam patet, nisi fuerit $\alpha e = \mathfrak{c}d$ (quem casum

statim seorsim considerabimus), valores ipsorum x, y, ex his formulis deductos tribuendo ipsi z valorem quemcunque, aequationi propositae satisfacere; quare nihil superest, nisi vt eos valores ipsius z determinare doceamus ex quibus valores integri ipsorum x, y sequantur.

Quoniam $\alpha x + \mathfrak{C} y = z$, necessario pro z numeri *integri* tantum accipi possunt; praeterea vero manifestum est, si aliquis valor ipsius z tum ipsum x tum ipsum y integrum reddat, omnes valores ipsius z illi secundum modulum $2\alpha e - 2\mathfrak{C}d$ congruos itidem valores integros producere. Quodsi itaque pro z omnes numeri integri a o vsque ad $2\alpha e - 2\mathfrak{C}a - 1$ (quando $\alpha e - \mathfrak{C}d$ est positiuus) aut ad $2\mathfrak{C}d - 2\alpha e - 1$ (quando $\alpha e - \mathfrak{C}d$ est negatiuus) incl. substituuntur, et pro nullo horum valorum tum x tum y integri fiunt, nullus omnino valor ipsius z valores integros ipsorum x, y producet, aequatioque proposita in integris nullo modo poterit resolui; si vero quidam ex illis valoribus ipsius z ipsis x, y valores integros conciliant, puta hi ζ, ζ', ζ'' etc. (quos etiam per solutionem congruentiarum secundi gradus ex principiis sect. IV. inuenire licet); *omnes* solutiones prodibunt ponendo $z = (2\alpha e - 2\mathfrak{C}d)\nu + \zeta$, $z = (2\alpha e - 2\mathfrak{C}d)\nu + \zeta'$ etc., designante ν indefinite omnes numeros integros.

220. Pro eo quem exclusimus casu, vbi $\alpha e = \mathfrak{C}d$, methodum peculiarem indagare oportet. Supponamus, α, $\mathfrak{C}$ inter se primos esse, quod licere ex art. 215. I constat, eritque $\frac{d}{\alpha} =$

$\frac{\varepsilon}{\zeta}$ numerus integer (art. 19), quem statuemus $= h$. Tunc aequatio proposita hanc induit formam: $(m\alpha x + m\zeta y + h)^2 - hh + f = 0$, manifestoque adeo rationaliter solui nequit, nisi $hh - f$ fuerit numerus quadratus. Sit $hh - f = kk$, patetque aequationi propositae sequentes duas aequiualere: $m\alpha x + m\zeta y + h + k = 0$, et $m\alpha x + m\zeta y + h - k = 0$, *i. e.* quamlibet solutionem aequationis propositae etiam alterutri harum aequationum satisfacere, et vice versa. Aequatio prior manifesto in integris solui nequit, nisi $h + k$ per m fuerit diuisibilis, similiterque posterior solutionem in integris non admittet, nisi $h - k$ per m fuerit diuisibilis. Hae vero conditiones ad resolubilitatem vtriusque aequationis sufficiunt (quia α, ζ inter se primi esse supponuntur), omnesque solutiones secundum regulas notas exhiberi poterunt.

221. Casum in art. 217 consideratum (quia omnium difficillimus est) exemplo illustramus. Proposita sit aequatio $xx + 8xy + yy + 2x - 4y + 1 = 0$. Ex hac primo per introductionem aliarum incognitarum $p = 15x - 9$, $q = 15y + 6$ deriuatur aequatio $pp + 8pq + qq = -540$. Huius autem solutiones omnes in integris, contineri inueniuntur sub quatuor formulis sequentibus:

$$p = 6t,\ q = -24t - 90u$$
$$p = 6t,\ q = -24t + 90u$$
$$p = -6t,\ q = 24t - 90u$$
$$p = -6t,\ q = 24t + 90u$$

denotantibus t, u indefinite omnes numeros integros positiuos aequationi $tt - 15uu = 1$ satis-

facientes, quos complectitur formula $t = \frac{1}{2}((4 + \sqrt{15})^n + (4 - \sqrt{15})^n)$, $u = \frac{1}{2\sqrt{15}}((4 + \sqrt{15})^n - (4 - \sqrt{15})^n)$, si n indefinite omnes numeros integros positiuos (inclusa etiam cifra) designat. Quamobrem omnes valores ipsorum x, y contenti erunt sub formulis his:

$x = \frac{1}{5}(2t + 3)$, $y = -\frac{1}{5}(8t + 30u + 2)$
$x = \frac{1}{5}(2t + 3)$, $y = -\frac{1}{5}(8t - 30u + 2)$
$x = \frac{1}{5}(-2t + 3)$, $y = \frac{1}{5}(8t - 30u - 2)$
$x = \frac{1}{5}(-2t + 3)$, $y = \frac{1}{5}(8t + 30u - 2)$.

Praeceptis autem nostris rite applicatis, reperietur, vt valores *integri* prodeant, in formula prima et secunda eos valores ipsorum t, u accipi debere, qui proueniant ex indice *n pari;* in tertia quartaque vero eos, qui ex *impari n* obtineantur. — Solutiones simplicissimae habentur hae: $x = 1, -1, -1$; $y = -2, 0, 12$ resp.

Ceterum obseruare conuenit, solutionem problematis in artt. praecc. explicati plerumque per multifaria artificia abbreuiari posse, praesertim quantum ad exclusionem solutionum inutilium i. e. fractiones implicantium pertinet; sed haec ne nimis longi fiamus hoc loco praeterire coacti sumus.

222. Quoniam complura ex iis quae hucusque pertractauimus etiam ab aliis geometris considerata sunt, horum merita silentio praeterire non possumus. De *formarum aequiualentia* disquisitiones generales instituit ill. La Grange, *Nouv. Mem. de l'Ac. de Berlin*, 1773 *p.* 263 *et* 1775 *p.* 323. *sqq.*, vbi imprimis docuit, pro quo-

uis determinante dato multitudinem finitam formarum dari ita comparatarum, vt quaeuis forma illius determinantis alicui ex ipsis aequiualens sit, adeoque omnes formas determinantis dati in classes distribui posse. Postea clar. Le Gendre plures proprietates elegantes huius classificationis, ad maximam partem per inductionem detexit, quas infra trademus demonstrationibusque muniemus. Ceterum distinctionem aequiualentiae propriae et impropriae, cuius vsus maxime in disquisitionibus subtilioribus conspicuus est, nemo hucusque attigerat.

Problema famosum in art. 216 sqq. explicatum ill. La Grange primus complete resoluit, *Hist. de l'Ac. de Berlin* 1767, *p.* 165, *et* 1768 *p.* 181 *sqq.* Exstat solutio (sed minus completa) etiam in *Suppl. ad Euleri Algebram* iam saepius laudatis. Iam antea ill. Euler idem argumentum aggressus fuerat, *Comm. Petr. T. VI p.* 175; *Comm. Nou. T. IX p.* 3; *Ibid. T. XVIII p.* 185 *sqq.*, sed inuestigationem suam eo semper restrinxit, vt ex aliqua solutione, quam iam cognitam esse supponit, aliae deriuentur; praetereaque ipsius methodi in paucis tantummodo casibus *omnes* solutiones suppeditare valent (vid. La Grange *Hist. de l'Ac. de Berlin* 1767, *p.* 237). Quum vltima harum trium commentt. recentioris dati sit quam solutio La Grangiana, quae problema omni generalitate amplectitur nihilque hoc respectu desiderandum relinquit: Euler tunc temporis (Tomus XVIII Commentariorum pertinet ad annum 1773, et a. 1774 est publicatus) illam solutionem nondum nouisse videtur. Ceterum solutio nostra (perinde vt omnia reliqua

quae in hac sectione hactenus tradidimus), principiis omnino diuersis est superstructa.

Quae ab aliis, Diophanto, Fermatio etc. huc pertinentia sunt tradita, casus maxime speciales spectant; quare quum eorum quae praesertim memoratu digna visa sunt iam supra mentio facta sit, sigillatim omnia enarrare supersedemus.

* * *

Quae hactenus de formis secundi gradus exposuimus, pro primis tantum elementis huius doctrinae sunt habenda: innixius hanc disquisitionem persequentibus campus se aperuit nobis vastissimus, ex quo ea quae attentione imprimis digna videntur in sequentibus excerpemus. Namque argumentum hoc tam fertile est, vt permulta alia, quae iam nunc inuenire nobis contigit, breuitatis gratia silentio praeterire oporteat: multo vero plura sine dubio adhuc latent nouosque conatus expectant. Ceterum in limine harum inuestigationum statim adnotare conuenit, formas determinantis o inde exclusas esse, nisi contrarium moneatur.

223. Iam supra (artt. 175, 195, 211) ostendimus, proposito numero quocunque integro D (siue positiuo siue negatiuo) assignari posse multitudinem finitam formarum F, F', F'' etc. determinantis D, ita comparatarum, vt quaeuis forma determinantis D proprie aequiualens sit alicui ex illis et quidem vnicae tantum. Omnes

igitur formae determinantis D (quarum multitudo est infinita) secundum illas formas *classificari* poterunt, formando scilicet e complexu omnium formarum formae F proprie aequiualentium classem primam; e formis quae formae F' proprie aequiualent, secundam etc.

Ex singulis classibus formarum determinantis dati D, forma aliqua eligi, et tamquam *forma repraesentans* totius classis considerari poterit. Per se quidem prorsus arbitrarium est, quaenam forma ex quaque classe accipiatur, attamen ea semper praeferenda erit, quae reliquas *simplicitate* superare videtur. Simplicitas formae alicuius (a, b, c) manifesto ex magnitudine numerorum a, b, c aestimanda est, meritoque forma (a', b', c') minus simplex dicetur quam (a, b, c), si $a' > a$, $b' > b$, $c' > c$. Sed hinc res nondum determinatur penitus, arbitrioque nostro relinquitur *e. g.*, vtram ex formis $(17, 0, -45)$, $(5, 0, -153)$ pro simpliciori habere malimus. Plerumque tamen e re erit, sequentem normam obseruare:

I. Quando determinans D est negatiuus, adoptentur formae reductae in singulis classibus contentae tamquam formae repraesentantes; vbi vero in eadem classe duae formae reductae reperiuntur (quae erunt oppositae, art. 172), recipiatur ea cuius terminus medius positiuus.

II. Quando determinans D est positiuus non-quadratus, euoluatur periodus formae alicuius reductae in classe proposita contentae, in qua

aut duae formae ancipites inuenientur aut nulla (art. 187).

1) In casu priori sint formae ancipites hae: (A, B, C), (A', B', C'); residua minima numerorum B, B' secundum modulos A, A' resp. M, M' (quae positiue accipi poterunt nisi sunt $= 0$); denique $\frac{D - MM}{A} = N$, $\frac{D - M'M'}{A'} = N'$. His ita factis, ex formis $(A, M, -N)$, $(A', M', -N')$ ea quae simplicissima videtur pro forma repraesentante accipiatur. In hoc iudicio forma cuius terminus medius $= 0$ praeferatur; quando vero terminus medius aut in vtraque aut in neutra est 0, ea quae terminum primum minorem habet alteri praehabenda, et quando termini primi magnitudine sunt aequales signis diuersi, signum negatiuum positiuo postponendum.

2) Quando vero nulla forma anceps in tota periodo habetur, eligatur ex omnibus periodi formis ea quae terminum primum sine respectu signi minimum habet, ita quidem, vt si duae formae in eadem periodo occurrant, in quarum altera idem terminus primus signo positiuo affectus sit in altero negatiuo, posterior priori postponatur. Sit haec forma (A, B, C), deducaturque ex ipsa eodem modo vt in casu praec. forma alia $(A, M, -N)$ (puta, accipiendo pro M residuum absolute minimum ipsius B secundum mod. A, et faciendo $N = \frac{D - MM}{A}$): haec demum pro repraesentante adoptetur.

Quodsi vero eueniret, vt idem terminus primus minimus A pluribus periodi formis commu-

nis sit, omnes hae formae eo quo praescripsimus modo tractandae et ex formis prodeuntibus ea cuius terminus medius quam minimus euadit tamquam forma repraesentans assumenda erit.

Ita e. g. pro $D = 305$ habetur periodus inter alias haec: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, ex qua primo eligitur forma $(7, 16, -7)$, hinc que secundo deducitur forma repraesentans $(7, 2, -43)$.

III. Quando determinans est positiuus quadratus $= kk$, eruatur forma reducta $(A, k, 0)$ in classe proposita contenta et, si $A < k$ aut $= k$, pro forma repraesentante ipsa recipiatur; si vero $A > k$, assumatur illius loco forma $(A - 2k, k, 0)$, cuius terminus primus erit negatiuus, sed minor quam k.

Ex. Hoc modo omnes formae determinantis -235) distribuuntur in classes sedecim, quarum repraesentantes erunt: $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$, octoque aliae a praecedentibus in solis signis terminorum externorum diuersae, $(-1, 0, -235)$, $(-2, 1, -118)$ etc.

Omnes formae determinantis 79 in sex classes discedunt, quarum repraesentantes $(1, 0, -79)$, $(3, 1, -26)$, $(3, -1, -26)$, $(-1, 0, 79)$, $(-3, 1, 26)$, $(-3, -1, 26)$.

224. Per hanc itaque classificationem formae quae proprie aequiualentes sunt a reliquis omnino segregabuntur. Duae formae eiusdem determinantis D, si ex eadem classe sunt, proprie aequiualentes erunt; quiuis numerus per vnam repraesentabilis etiam per alteram repraesentari poterit; et si numerus quicunque M per formam priorem ita repraesentari potest, vt indeterminatae valores inter se primos habeant, idem numerus per alteram formam eodem modo repraesentari poterit, et quidem ita, vt vtraque repraesentatio ad eundem valorem expressionis $\sqrt{D}$ (mod. M) pertineat. Si vero duae formae ad classes diuersas pertinent, proprie aequiualentes non erunt; a repraesentabilitate numeri alicuius dati per vnam ad repraesentabilitatem eiusdem numeri per alteram concludi nequit; contra, si numerus M per alteram repraesentari potest ita vt valores indeterminatarum inter se primi sint, statim certi sumus, nullam similem repraesentationem eiusdem numeri per formam alteram dari, quae ad eundem valorem expr. $\sqrt{D}$ (mod. M) pertineat. (V. artt. 167, 168).

Contra vtique fieri potest, vt formae duae F, F', e classibus diuersis K, K' improprie aequiualentes sint, in quo casu *quaeuis* forma ex altera classe *cuiuis* formae ex altera improprie aequiualebit; quaeuis forma ex K formam sibi oppositam habebit in K', classesque ipsae K, K' *oppositae* dicentur. Ita in exemplo primo art. praec. classis tertia formarum det. — 235 quartae, septima octauae opposita est; in ex. secundo classis secunda tertiae, quinta sextae. Propositis

itaque duabus formis quibuscunque e classibus oppositis, quiuis numerus M qui per alteram repraesentari potest etiam per alteram poterit; quod, si in altera fit per valores indeterminatarum inter se primos, in altera perinde fieri poterit, ita tamen, vt hae duae repraesentationes ad valores oppositos expr. $\sqrt{D}$ (mod. M) pertineant. — Ceterum regulae supra traditae pro electione formarum repraesentantium ita sunt constitutae, vt classes oppositae formas repraesentantes oppositas semper nanciscantur.

Denique dantur etiam classes *sibi ipsis oppositae*. Scilicet si forma aliqua simul cum forma opposita in eadem classe continetur, facile perspicitur, omnes formas huius classis tum proprie tum improprie inter se aequiualentes esse, oppositasque suas secum habere. Hanc indolem quaeuis classis habebit, in qua forma anceps continetur, et vice versa in quauis classe sibi ipsi opposita necessario forma anceps reperietur (art. 163, 165), quamobrem *classis anceps* nuncupabitur. Ita inter classes formarum determinantis — 235 octo ancipites habentur, quarum repraesentantes sunt (1, 0, 235), (2, 1, 118), (5, 0, 47), (10, 5, 26), (— 1, 0, — 235), (— 2, 1, — 118), (— 5, 0, — 47), (— 10, 5, — 26); inter classes formarum determinantis 79 duae, quarum repraesentantes (1, 0, — 79), (— 1, 0, 79). — Ceterum si formae repraesentantes secundum regulas nostras determinatae sunt, classes ancipites nullo negotio inde cognosci poterunt. Scilicet pro determinante positiuo non quadrato classis anceps certo formam repraesentantem an-

cipitem nanciscitur, (art. 194); pro determinante negatiuo forma repraesentans classis ancipitis aut ipsa anceps erit, aut talis cuius termini externi sunt aequales (art. 172); denique pro determinante positiuo quadrato per art. 210 facile diiudicatur, an forma repraesentans sibi ipsi improprie aequiualens sit adeoque classis quam repraesentat, anceps.

225. Iam supra (art. 175.) ostendimus, in forma (a, b, c) determinantis negatiui terminos externos eadem signa habere tum inter se tum cum terminis externis cuiusuis aliae formae illi aequiualentis. Si a, c sunt positiui, formam (a, b, c) *positiuam* vocabimus, nec non totam classem in qua (a, b, c) continetur et quae e solis formis positiuis constabit, *classem positiuam* dicemus. Contra (a, b, c) erit *forma negatiua*, et in *classe negatiua* contenta, si a, c sunt negatiui. Per formam positiuam numeri negatiui, per negatiuam positiui repraesentari nequeunt. Si forma (a, b, c) est repraesentans alicuius classis positiuae, forma $(-a, b, -c)$ repraesentans classis negatiuae erit, vnde sequitur, multitudinem classium positiuarum multitudini negatiuarum aequalem esse, et, simul ac illae fuerint assignatae, etiam has haberi. Quocirca in disquisitionibus super formis determinantis negatiui plerumque sufficit, classes positiuas considerare, quippe quarum proprietates ad classes negatiuas facile transferuntur.

Ceterum distinctio haec vnice in formis determinantis negatiui locum habet; per formas

determinantis positiui sine discrimine numeri positiui et negatiui repraesentari possunt, quin adeo haud raro duae formae tales (a, b, c), $(-a, b, -c)$ in hoc casu ad eandem classem sunt referendae.

226. Formam quamcunque (a, b, c) *primitiuam* vocamus, si numeri a, b, c diuisorem communem non habent; alioquin dicetur *deriuata*, et quidem, posito numerorum a, b, c diuisore communi maximo $= m$, forma (a, b, c) erit *deriuata e forma primitiua* $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$. Ex hac definitione statim liquet, omnes formas, quarum determinans per nullum quadratum (praeter 1) diuisibilis sit, necessario primitiuas esse. Porro ex art. 161 patet, si in aliqua classe data formarum determinantis D forma primitiua inueniatur, omnes formas huius classis primitiuas fore, in quo casu classis ipsa *primitiua* dicetur. Porro manifestum est, si forma aliqua F determinantis D deriuata sit ex forma primitiua f determinantis $\frac{D}{mm}$, classesque in quibus formae F, f resp. contineantur sint K, k, omnes formas e classe K deriuatas fore e classe primitiua k; quocirca classem K ipsam *ex classe primitiua k deriuatam* in hoc casu vocabimus.

Si (a, b, c) est forma primitiua, neque vero a, c simul pares (i. e. si aut vterque impar aut saltem alteruter), facile intelligitur, non modo a, b, c, sed etiam $a, 2b, c$ diuisorem communem habere non posse, in quo casu forma

(a, b, c) dicetur *proprie primitiua* siue simpliciter *forma propria.* Si vero (a, b, c) est forma primitiua, numeri a, c autem ambo pares, patet, numeros a, $2b$, c diuisorem communem 2 habere (qui simul erit maximus), vocaturque (a, b, c) *forma improprie primitiua*, siue simpliciter *forma impropria* *). In hoc casu b necessario erit impar (alioquin enim (a, b, c) non esset forma primitiua); quare erit $bb \equiv 1 \pmod 4$ adeoque quoniam ac per 4 diuisibilis, determinans $bb - ac \equiv 1 \pmod 4$. Formae impropriae itaque tantummodo pro determinante formae $4n + 1$, si est positiuus, vel formae, $-(4n + 3)$, si est negatiuus, locum habent. — Ex art. 161 autem perspicuum est, si in classe aliqua data forma proprie primitiua inueniatur, omnes formas huius classis proprie primitiuas esse; contra classem quae formam improprie primitiuam implicet ex solis formis improprie primitiuis constare. Quamobrem classis ipsa in casu priori *proprie primitiua* seu simpliciter *propria*; in posteriori, *improprie primitiua* seu *impropria* appellabitur. Ita e. g. inter classes positiuas formarum determinantis — 235 sex sunt propriae, puta quarum repraesentantes $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$, totidemque inter negatiuas; binae vero inter vtrasque impropriae.

*) Hos terminos *proprie* et *improprie* ideo hic elegimus quia alii magis idonei non occurrebant, quod admonemus, ne quis inter hanc significationem eamque qua inde ab art. 157 vsi sumus, nexum occultum quaerat, qui nullus adest. Ceterum ambiguitas certe hinc non est metuenda.

— Classes formarum determinantis 79 (vtpote numeri formae $4n + 3$) omnes sunt propriae.

Si forma (a, b, c) est deriuata, et quidem e primitiua $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, haec aut proprie primitiua aut improprie esse poterit. In casu priori m erit diuisor communis maximus etiam numerorum a, $2b$, c; in posteriori horum numerorum diu. comm. max. erit $2m$. Hinc intelligitur distinctio inter *formam e forma proprie primitiua deriuatam*, et *formam ex improprie primitiua deriuatam*; nec non (quoniam propter art. 161 omnes formae eiusdem classis hoc respectu perinde se habent) inter *classem deriuatam e classe proprie primitiua* et *classem ex improprie primitiua deriuatam*.

Per has distinctiones fundamentum primum nacti sumus, cui distributionem omnium classium formarum determinantes dati in varios *ordines* superstruere possumus. Classes duas, quarum repraesentantes sunt formae (a, b, c), (a', b', c') in *eundem ordinem* coniiciemus, *tum* si numeri a, b, c eundem diuisorem communem maximum habent vt a', b', c', *tum* a, $2b$, c eundem vt a', b', c'; si vero aut alterutra aut vtraque harum conditionum locum non habet, classes ad *ordines diuersos* referentur. Hinc statim patet, omnes classes proprie primitiuas vnum ordinem constituere; omnes classes improprie primitiuas, alium; si mm est quadratum determinantem D metiens classes deriuatae e classibus proprie primitiuis determinantis $\frac{D}{mm}$ for-

mabunt ordinem peculiarem, aliumque classes deriuatae e classibus improprie primitiuis determinantis $\frac{D}{mm}$ etc. Si forte D per nullum quadratum (praeter 1) diuisibilis est, ordines classium deriuatarum non aderunt adeoque aut vnus tantum ordo dabitur (quando $D \equiv 2$ vel 3 secundum mod. 4) puta ordo classium proprie primitiuarum, aut duo quando $D \equiv 1 \pmod 4$) scilicet O. classium proprie primitiuarum et O. cl. impr. primitiuarum. Per principia calculi combinationum haud difficile conditur regula sequens generalis: Si supponitur $D = D' \cdot 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \ldots$ ita vt D' nullum factorem quadraticum implicet, et a, b, c etc. sint numeri primi impares diuersi (ad quam formam quiuis numerus redigi potest faciendo $\mu = 0$ quando D per 4 non est diuisibilis; et α, β, γ etc. omnes $= 0$ siue quod eodem redit omittendo factores $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$ etc. quando D per nullum quadratum impar diuidi potest): habebuntur aut ordines $(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$ nempe quando $D' \equiv 2$ vel $3 \pmod 4$; aut ordines $(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$, quando $D' \equiv 1 \pmod 4$. Sed demonstrationem huius regulae supprimimus, quoniam neque difficilis neque hic adeo necessaria est.

Ex. 1. Pro $D = 45 = 5 \cdot 3^2$ habentur sex classes, quarum repraesentantes $(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $6, 3, -6)$. Hae distribuuntur in quatuor ordines, scilicet O. I com-

prehendet duas classes proprias quarum repr. (1, 0, — 45), (— 1, 0, 45); O. II continebit duas classes improprias, quarum repr. (2, 1, — 22), (— 2, 1, 22); O. III continebit vnam classem deriuatam e propria determinantis 9, puta cuius repr. (3, 0, — 15); O. IV constabit ex vna classe deriuata ex impropria det. 9, puta cuius repr. (6, 3, — 6).

Ex. 2. Classes positiuae determinantis — 99 = — 11. 3^2 inter quatuor ordines distribuentur: O. I complectetur classes proprie primitiuas sequentes *): (1, 0, 99), (4, 1, 25), (4, — 1, 25), (5, 1, 20), (5, — 1, 20), (9, 0, 11); O. II continebit classes improprias (2, 1, 50), (10, 1, 10); O. III classes deriuatas e propriis determinantis — 11, (3, 0, 33), (9, 3, 12), (9, — 3, 12); O. IV classem vnicam deriuatam ex impropria det. — 11, (6, 3, 18). — Classes negatiuae huius determinantis prorsus eodem modo in ordines distribui poterunt.

Obseruamus, *classes oppositas semper ad eundem ordinem referri*, cuius theorematis ratio nullo negotio perspicitur.

227. Ex his diuersis ordinibus imprimis ordo classium proprie primitiuarum maximam attentionem meretur. Nam singulae classes deriuatae a certis classibus primitiuis (determinantis minoris) originem trahunt, ex quarum conside-

*) Adhibendo breuitatis caussa formas repraesentantes pro classibus ipsis quarum vice funguntur.

ratione ea quae ad illas spectant plerumque sponte sequuntur. Infra autem docebimus, quamlibet classem improprie primitiuam simili modo quasi associatam esse aut vnicae classi proprie primitiuae aut tribus (eiusdem determinantis). Porro pro determinantibus negatiuis classes negatiuas praeterire licebit, quippe quibus singulis certae classes positiuae semper respondent. Vt itaque naturam classium proprie primitiuarum profundius penetremus, ante omnia differentiam certam essentialem explicabimus, secundum quam totus ordo classium propriarum in plura *genera* subdiuidi potest. Quoniam hoc argumentum grauissimum hactenus nondum attigimus, res ab integro nobis erit repetenda.

228. THEOREMA. *Per formam quamcunque proprie primitiuam F repraesentari possunt infinite multi numeri per numerum primum quemcunque datum p non diuisibiles.*

Dem. Si forma $F = axx + 2bxy + cyy$, manifestum est, p omnes tres numeros a, $2b$, c simul metiri non posse. Iam quando a per p non est diuisibilis, patet, si pro x assumatur numerus quicunque per p non diuisibilis, pro y vero numerus per p diuisibilis, valorem formae F fieri non diuisibilem per p; quando c per p non est diuisibilis, idem obtinetur tribuendo ipsi x valorem diuisibilem ipsique y valorem non diuisibilem; denique quando tum a tum c per p sunt diuisibiles, adeoque $2b$ non diuisibilis, forma F valorem per p non diuisibilem induet tribuendo tum ipsi x tum ipsi y valores quoscunque per p non diuisibiles. *Q. E. D.*

Manifestum est, theorema etiam pro formis *improprie primitiuis* locum habere, si modo non fuerit $p = 2$.

Quoniam plures huiusmodi conditiones simul consistere possunt, vt idem numerus per quosdam numeros primos datos diuisibilis sit, per alios non diuisibilis (v. art. 32.): facile perspicitur, numeros x, y infinite multis modis ita determinari posse, vt forma primitiua $axx + 2bxy + cyy$ valorem per quotcunque numeros primos datos non diuisibilem adipiscatur, a quibus vnice excludendus est 2 quoties forma est improprie primitiua. Hinc patet, theorema generalius ita proponi posse: *Per formam quamcunque primitiuam repraesentari possunt infinite multi numeri, qui ad numerum quemcunque datum (imparem, quando forma est improprie primitiua) sint primi.*

229. Theorema. *Sit F forma primitiua determinantis D, p numerus primus ipsum D metiens: tum numeri per p non diuisibiles qui per formam F repraesentari possunt in eo conuenient, vt vel omnes sint residua quadratica ipsius p, vel omnes non residua.*

Dem. Sit $F = (a, b, c)$; m, m' duo numeri quicunque per p non diuisibiles qui per formam F repraesentari possunt, scilicet $m = agg + 2bgh + chh$, $m' = ag'g' + 2bg'h' + ch'h'$. Tum erit $mm' = (agg' + b(gh' + hg') + chh')^2 - D(gh' - hg')^2$; quare mm' quadrato congruus erit secundum modulum D, adeoque etiam secundum p, i. e. mm' erit residuum quadraticum ipsius p. Hinc sequitur, aut vtrumque

m, m' esse residuum quadraticum ipsius p, aut vtrumque non-residuum. *Q. E. D.*

Simili modo probatur, quando determinans D per 4 sit diuisibilis, omnes numeros impares per F repraesentabiles vel esse $\equiv 1$, vel omnes $\equiv 3 \pmod 4$. Scilicet productum e duobus numeris talibus in hoc casu semper erit residuum quadr. ipsius 4, adeoque $\equiv 1 \pmod 4$; quare vel vterque erit $\equiv 1$, vel vterque $\equiv 3$.

Denique quando D per 8 est diuisibilis, productum e duobus numeris quibuscunque imparibus, qui per F repraesentari possunt, erit R. Q. ipsius 8 et proin $\equiv 1 \pmod 8$. Quare in hoc casu omnes numeri impares per F repraesentabiles vel erunt $\equiv 1$, vel omnes $\equiv 3$, vel omnes $\equiv 5$, vel omnes $\equiv 7 \pmod 8$.

Ita e. g. quum per formam $(10, 3, 17)$ repraesentari possit numerus 10 qui est N. R. ipsius 7: omnes numeri per 7 non diuisibiles, qui per formam illam repraesentari possunt, non-residua ipsius 7 erunt. — Quum -3 per formam $(-5, 1, 49)$ repraesentabilis et sec. mod. 4 sit $\equiv 1$, omnes numeri impares per formam hanc repraesentabiles perinde se habebunt.

Ceterum, si ad proprositum praesens necessarium esset, facile demonstrare possemus, numeros per formam F repraesentabiles ad nullum numerum primum qui ipsum D non metiatur, talem relationem fixam habere, sed promiscue tum residua tum non-residua numeri cuiusuis primi ipsum D non metientis per formam F re-

praesentari posse. Contra respectu numerorum 4 et 8 analogon quoddam etiam in aliis casibus locum habet, quos praeterire non possumus.

I. *Quando determinans D formae primitiuae F est* $\equiv 3 \pmod 4$: *omnes numeri impares, per formam F repraesentabiles, erunt vel* $\equiv 1$, *vel omnes* $\equiv 3 \pmod 4$. Si enim m, m' sunt duo numeri per F repraesentabiles, productum mm' eodem modo vt supra sub formam $pp - Dqq$ redigi poterit. Quando itaque vterque m, m' est impar, necessario alter numerorum p, q par erit, alter impar, adeoque alterum quadratorum pp, $qq \equiv 0$, alterum $\equiv 1 \pmod 4$. Vnde facile deducitur, $pp - Dqq$ certo esse $\equiv 1 \pmod 4$, adeoque aut vtrumque m, $m' \equiv 1$, aut vtrumque $\equiv 3 \pmod 4$. Ita *e. g.* per formam $(10, 3, 17)$ alii numeri impares quam qui sunt formae $4n + 1$ repraesentari nequeunt.

II. *Quando determinans D formae primitiuae F est* $\equiv 2 \pmod 8$: *omnes numeri impares, per F repraesentabiles, erunt vel partim* $\equiv 1$ *partim* $\equiv 7$, *vel partim* $\equiv 3$ *partim* $\equiv 5 \pmod 8$. Ponamus enim m, m' esse duos numeros impares per F repraesentabiles, quorum igitur productum mm' sub formam $pp - Dqq$ redigi poterit. Quando ergo vterque m, m' est impar, necessario p impar esse debebit (quia D par), adeoque $pp \equiv 1 \pmod 8$; qq vero erit vel $\equiv 0$, vel $\equiv 1$, vel $\equiv 4$, et proin Dqq vel $\equiv 0$ vel $\equiv 2$. Hinc $mm' = pp - Dqq$ fit vel $\equiv 1$ vel $\equiv 7 \pmod 8$; si itaque m est vel $\equiv 1$ vel $\equiv 7$, etiam m' erit vel 1 vel $\equiv 7$; si vero m est vel

$\equiv 3$, vel $\equiv 5$, etiam m' erit vel $\equiv 3$ vel $\equiv 5$. *E. g.* omnes numeri impares per formam $(3, 1, 5)$ repraesentabiles sunt aut $\equiv 3$, aut $\equiv 5 \pmod 8$, nullique numeri formae $8n + 1$ aut $8n + 7$ per formam illam repraesentari possunt.

III. *Quando determinans D formae primitiuae F est* $\equiv 6 \pmod 8$: *per formam hanc repraesentari possunt numeri impares vel tales tantum qui sunt* $\equiv 1$ *et* $\equiv 3 \pmod 8$, *vel tales tantum qui sunt* $\equiv 5$ *et* $\equiv 7 \pmod 8$. Demonstrationem praecedenti (in II) omnino similem quisque nullo negotio euoluere poterit. — Ita *e. g.* per formam $(5, 1, 7)$ vnice tales numeri impares possunt repraesentari qui sunt aut $\equiv 5$ aut $\equiv 7 \pmod 8$.

230. Omnes igitur numeri qui per formam primitiuam datam F determinantis D repraesentari possunt, relationem fixam habebunt ad singulos diuisores primos ipsius D (per quos quidem ipsi non sunt diuisibiles), numeri impares vero qui per F possunt repraesentari, in quibusdam casibus etiam ad numeros 4 et 8 relationem fixam habebunt, scilicet ad 4, quoties D aut $\equiv 0$ aut $\equiv 3 \pmod 4$, et ad 8 quoties D aut $\equiv 0$, aut $\equiv 2$ aut $\equiv 6 \pmod 8$*). Talem relationem ad singulos hos numeros, *characterem* seu *characterem particularem* formae F vocabimus sequentique modo exprimemus:

*) Pro determinantibus per 8 diuisibilibus relatio ad numerum 4 negligi potest, quoniam in hoc casu sub relatione ad 8 iam est contenta.

Quando sola residua quadratica numeri primi p per formam F repraesentari possunt, tribuemus ipsi characterem $R\ p$, in casu opposito characterem $N\ p$; similiter scribemus 1, 4, quando alii numeri impares per formam F repraesentari nequeunt nisi qui sunt $\equiv 1 \pmod 4$, vnde statim liquet quales characteres exprimantur per signa 3, 4; 1, 8; 3, 8; 5, 8; 7, 8. Denique formis per quas numeri impares tales soli repraesentari possunt qui sec. mod. 8 sunt vel $\equiv 1$ vel $\equiv 7$, tribuemus characterem 1 *et* 7, 8; ex quo significatio characterum 3 *et* 5, 8; 1 *et* 3, 8; 5 *et* 7, 8 sponte sequitur.

Characteres singuli formae primitiuae datae (a, b, c) determinantis D semper ex vno saltem numerorum a, c (qui manifesto per formam illam ambo sunt repraesentabiles) cognosci possunt. Nam quoties p est diuisor primus ipsius D, certe vnus numerorum a, c per p non erit diuisibilis; si enim vterque per p diuisibilis esset, p etiam ipsum bb $(= D + ac)$ metiretur, et proin etiam ipsum b, *i. e.* forma (a, b, c) non esset primitiua. Simili modo in iis casibus vbi forma (a, b, c) ad numerum 4 vel 8 relationem fixam habet, certo ad minimum vnus numerorum a, c impar erit, ex quo igitur relatio illa deprehendi poterit. Ita e. g. character formae (7, 0, 23) respectu numeri 23 e numero 7 concluditur N 23, eiusdem formae character respectu numeri 7 habetur ex numero 23 puta $R\ 7$; denique character huius formae respectu numeri 4, puta 3, 4, vel e numero 7 vel e numero 23 colligi potest.

Quoniam omnes numeri qui per formam aliquam F in classe K contentam repraesentari possunt, etiam per quamlibet aliam formam huius classis sunt repraesentabiles: manifesto singuli characteres formae F omnibus reliquis formis huius classis quoque competent, quapropter illos tamquam characteres totius classis considerare licebit. Singuli itaque characteres formae cuiuslibet primitiuae datae ex ipsius forma repraesentante cognoscuntur. Classes oppositae semper characteres omnes eosdem habebunt.

231. Complexus *omnium* characterum particularium formae vel classis datae constituet characterem integrum huius formae vel classis. Ita e. g. character integer formae $(10, 3, 17)$, vel totius classis quam repraesentat erit $1, 4; N\,7; N\,27$. Simili modo character integer formae $(7, 1, -17)$ erit $7, 8; R\,3; N\,5$, nam character particularis $3, 4$ in hoc casu omittitur quia in charactere $7, 8$ iam est contentus. — Ex hoc fonte petimus subdiuisionem totius ordinis classium proprie primitiuarum (positiuarum quando det. est negatiuus) determinantis dati in plura *genera* diuersa, referendo omnes classes quae eundem characterem integrum habent ad genus idem; quarumque characteres integri diuersi sunt, ad genera diuersa. Singulis vero generibus eos characteres integros tribuemus quos classes sub ipsis contentae habent. Ita e. g. pro determinante -161 habentur sedecim classes positiuae proprie primitiuae, quae sequenti modo in quatuor genera distribuuntur:

Character	Classium formae repraesentantes
1, 4; R 7; R 23	(1, 0, 161), (2, 1, 81), (9, 1, 18) (9, — 1, 18)
1, 4; N 7; N 23	(5, 2, 33), (5, — 2, 33), (10, 3, 17) (10, — 3, 17)
3, 4; R 7; N 23	(7, 0, 23), (11, 2, 15), (11, — 2, 15) (14, 7, 15)
3, 4; N 7; R 23	(3, 1, 54), (3, — 1, 54), (6, 1, 27) (6, — 1, 27).

De multitudine characterum integrorum diuersorum, qui quidem a priori sunt possibiles, teneantur sequentia.

I. Quando determinans D per 8 est diuisibilis, respectu numeri 8 quatuor characteres particulares diuersi sunt possibiles; numerus 4 nullum characterem peculiarem suppeditat (annot. ad art. praec.). Praeterea respectu singulorum diuisorum primorum imparium ipsius D bini characteres dantur; quare si illorum multitudo est m, dabuntur omnino 2^{m+2} characteres integri diuersi (statuendo $m = 0$, quoties D est potestas binaria).

II. Quando det. D per 8 non est diuisibilis, sed tamen per 4, insuperque per m numeros primos impares: omnino habebuntur 2^{m+1} characteres integri diuersi.

III. Quando det. D est par neque vero per 4 diuisibilis, erit vel $\equiv 2 \pmod 8$ vel $\equiv 6$. In casu priori dabuntur duo characteres particulares respectu numeri 8 puta 1 *et* 7, 8, atque

5 *et* 5, 8; in casu posteriori totidem. Posita igitur multitudine diuisorum primorum imparium ipsius D, $= m$: habebuntur omnino 2^{m+-1} characteres integri diuersi.

IV. Quando D est impar, erit vel $\equiv 1$, vel $\equiv 3 \pmod 4$. In casu posteriori respectu numeri 4 duo characteres diuersi dantur, qualis relatio in casu priori in characterem integrum non ingreditur. Quare designante m idem vt ante, in casu priori dabuntur 2^m, in posteriori 2^{m+-1} characteres integri diuersi.

Probe vero notandum est, hinc neutiquam sequi, totidem genera reuera dari quot characteres diuersi a priori sint possibiles. In exemplo quidem nostro horum semissi tantum reuera classes siue genera respondent, nullaeque classes positiuae dantur, quibus characteres 1, 4; R 7, N 23 vel 1, 4; N7; R 23; vel 3, 4; R7; R23 vel 3, 4; N7; N23 competant. De quo argumento grauissimo infro fusius agetur.

Formae $(1, 0, -D)$, quae haud dubie inter omnes formas determinantis D pro simplicissima habenda est, nomen *formae principalis* abhinc tribuemus; classem totam in qua illa reperitur *classem principalem* vocabimus; denique genus totum in quo classis principalis contenta est, *genus principale* dicetur. Probe itaque distinguendae sunt forma principalis, forma e classe principali et forma e genere principali; nec non classis principalis et classis e genere principali. His denominationibus semper vtemur, etiamsi

forte pro determinante aliquo aliae classes praeter principalem, vel alia genera praeter genus principale non dentur, vti e. g. euenit plerumque quando D est numerus primus positiuus formae $4n + 1$.

232. Quamquam ea quae de formarum characteribus explicata sunt proxime eum in finem sunt allata, vt subdiuisio ordinis *positiui proprie primitiui* inde petatur: tamen nihil impedit quominus eadem etiam ad formas classesque negatiuas aut ad improprie primitiuas applicentur, atque tum ordo improprie primitiuus positiuus, tum ordo proprie primitiuus negatiuus, tum ordo improprie primitiuus negatiuus ex eodem principio in genera subdiuidantur. Ita postquam e. g. ordo proprie primitiuus formarum determinantis 145 in duo genera sequentia subdiuisus est

$R5, R26$	$(1, 0, -145), (5, 0, -29)$
$N5, N26$	$(3, 1, -48), (3, -1, 48)$

etiam ordo improprie primitiuus perinde in duo genera subdiuidi potest:

$R5, R29$	$(4, 1, -36), (4, -1, -36)$
$N5, N29$	$(2, 1, -72), (10, 5, -12)$

vel, sicuti classes positiuae formarum determinantis — 129 in quatuor genera distribuuntur:

$1,4; R3; R43$	$(1, 0, 129), (10, 1, 13), (10, -1, 13)$
$1,4; N3; N43$	$(2, 1, 65), (5, 1, 26), (5, -1, 26)$
$3,4; R3; N43$	$(3, 0, 43), (7, 2, 19), (7, -2, 19)$
$3,4; N3; R43$	$(7, 3, 23), (11, 5, 14), (11, -5, 14)$

etiam classes negatiuae in quatuor ordines discedunt

$3, 4; N3; N43$	$(-1,0,-129), (-10,1,-13), (-10,-1,-13)$
$3, 4; R3; R43$	$(-2,1,-65), (-5,1,-16), (-5,-1,-26)$
$1, 4; N4; R43$	$(-3,0,-43), (-7,2,-19), (-7,-2,-19)$
$1, 4; R3; N43$	$(-6,3,-23), (-11,5,-14), (-11,-5,-14)$

Attamen quum systema classium negatiuarum systemati positiuarum semper tam simile euadat, plerumque superfluum videbitur illud seorsim construere. Ordinem improprie primitiuum autem ad proprie primitiuum reducere infra docebimus.

Tandem quod attinet ad ordines deriuatos: pro horum subdiuisione regulae nouae non sunt necessariae. Quum enim quiuis ordo deriuatus ex aliquo ordine primitiuo (determinantis minoris) originem trahat, illiusque classes singulae ad singulas huius sponte referantur: manifesto subdiuisio ordinis deriuati e subdiuisione ordinis primitiui peti poterit.

233. Si forma (primitiua) $F = (a, b, c)$ ita est comparata, vt inueniri possint duo numeri g, h tales vt fiat $gg \equiv a$, $gh \equiv b$, $hh \equiv c$ secundum modulum datum m, dicemus formam illam esse residuum quadraticum numeri m atque $gx + hy$ valorem expressionis $\sqrt{}\ (axx + 2bxy + cyy)$ (mod. m), siue breuius (g, h) valorem expr. $\sqrt{}\ (a, b, c)$ vel $\sqrt{}\ F$ (mod. m).

Generalius, si multiplicator M, ad modulum m primus, eius est indolis vt fieri possit $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ (mod. m), dicemus $M \times (a, b, c)$ siue MF esse res. quad. ipsius m, atque (g, h) valorem expressionis $\sqrt{M(a, b, c)}$ vel $\sqrt{MF}$ (mod. m). Ita e. g. forma $(3, 1, 54)$ est res. quadr. ipsius 23 atque $(7, 10)$ valor expr. $\sqrt{(3, 1, 54)}$ (mod. 23); similiter $(2, -4)$ valor expr. $\sqrt{5}$ $(10, 3, 17)$ (mod. 23). Vsus harum definitionum infra ostendetur: hic notentur propositiones sequentes:

I. Si $M(a, b, c)$ est R. Q. numeri m, hic determinantem formae (a, b, c) metietur. Si enim (g, h) est valor expressiones $\sqrt{M(a, b, c)}$ (mod. m), siue $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ (mod. m): erit $bbMM - acMM \equiv 0$, siue $(bb - ac)\,MM$ per m diuisibilis. Quoniam autem M ad m primus esse supponitur, etiam $bb - ac$ per m diuisibilis erit.

II. Si $M(a, b, c)$ est R. Q. ipsius m, atque m aut numerus primus aut potestas numeri primi, puta $= p^u$: character particularis formae (a, b, c) respectu numeri p erit vel Rp, vel Np, prout M est residuum vel non-residuum ipsius p. Hoc statim inde sequitur, quod tum aM tum cM est residuum ipsius m siue ipsius p, atque ad minimum vnus numerorum a, c per p non diuisibilis (art. 230).

Simili modo, si (manentibus reliquis) $m = 4$, erit vel 1, 4 vel 3, 4 character part. formae (a, b, c) prout $M \equiv 1$ vel $\equiv 3$; nec non si

$m = 8$ vel altior potestas numeri 2, erit 1, 8; 3; 8; 5, 8; 7, 8 char. part. formae (a, b, c) pront $M \equiv 1; 3; 5; 7 \pmod 8$ resp.

III. Vice versa si m est numerus primus aut numeri primi imparis potestas $= p^\mu$, determinantem $bb - ac$ metiens, atque M vel residuum vel non-residuum ipsius p, prout character formae (a, b, c) respectu ipsius p est Rp vel Np resp: erit M (a, b, c) resid. quadr. ipsius m. Quando enim a per p non est diuisibilis, aM erit res. ipsius p adeoque etiam ipsius m; si itaque g est valor expr. $\sqrt{\ } aM \pmod m$, h valor expr. $\frac{bg}{a} \pmod m$, erit $gg \equiv aM$; $ah \equiv bg$ adeoque $agh \equiv bgg \equiv abM$ et $gh \equiv bM$; denique $ahh \equiv bgh \equiv bbM \equiv bbM - (bb - ac) M \equiv acM$ adeoque $hh \equiv cM$, i. e. (g, h) valor expr. $\sqrt{\ } M$ (a, b, c). Quando vero a per m est diuisibilis, certo c non erit; vnde facile perspicitur, eadem resultare, si pro h assumatur valor expr. $\sqrt{\ } cM \pmod m$, pro g valor expr. $\frac{bh}{c} \pmod m$.

Simili modo demonstratur, si m fuerit $= 4$ ipsumque $bb - ac$ metiatur, numerusque M accipiatur vel $\equiv 1$ vel $\equiv 3$ prout 1, 4 vel 3, 4 fuerit char. part. formae (a, b, c): fore M (a, b, c) res. qu. ipsius m. Nec non, si m fuerit $= 8$ vel altior potestas ipsius 2 per quam $bb - ac$ diuisibilis sit, atque M accipiatur $\equiv 1; 3; 5; 7 \pmod 8$ prout character part. formae (a, b, c) respectu numeri 8 postulet: M (a, b, c) fore res. qu. ipsius m.

IV. Si determinans formae (a, b, c) est $= D$, atque M (a, b, c) res. qu. ipsius D, omnes character particulares formae (a, b, c) tum respectu singulorum diuisorum primorum imparium ipsius D, tum respectu numeri 4 vel numeri 8 (si ipsum D metiuntur) ex numero M statim cognosci possunt. Ita e. g. quum 3 (20, 10, 27) sit resid. qu. ipsius 440, scilicet (150, 9) valor expr. $\sqrt{}$ 3 (20, 10, 27) sec. mod. 440, atque $3N5$, $3R11$: characteres formae (20, 10, 27) sunt 3, 8; $N5$; $R11$. Soli characteres particulares respectu numerorum 4 et 8, quoties determinantem non metiuntur, nexum necessarium cum numero M non habent.

V. Vice versa, si numerus M ad D primus omnes characteres particulares formae (a, b, c) in se complectitur (exceptis characteribus respectu numerorum 4, 8, quando ipsum D non metiuntur): erit M (a, b, c) res. qu. ipsius D. Nam ex III patet, si D sub formam $\pm A^{\alpha} B^{\beta} C^{\gamma} \ldots$ redigatur, ita vt A, B, C etc. sint numeri primi diuersi, fore M (a, b, c) resid. qu. singulorum A^{α}, B^{β}, C^{γ} etc. Si igitur valor expr. $\sqrt{}$ M (a, b, c) secundum mod. A^{α}, est $(\mathfrak{A}, \mathfrak{A}')$; secundum mod. B^{β}, $(\mathfrak{B}, \mathfrak{B}')$; sec. mod. C^{γ}, $(\mathfrak{C}, \mathfrak{C}')$ etc. numerique g, h ita determinantur vt sit $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc.; $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ etc. secundum modulos A^{α}, B^{β}, C^{γ} etc. resp. (art. 32): facile perspicietur, fore $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ secundum omnes modulos A^{α}, B^{β}, C^{γ} etc. adeoque etiam secundum modulum D qui illorum est productum.

VI. Propter has rationes numeri tales vt M vocabuntur *numeri characteristici* formae (a, b, c), poteruntque per V. plures huiusmodi numeri nullo negotio inueniri simulac omnes characteres particulares huius formae sunt eruti; simplicissimi autem tentando plerumque euoluuntur facillime. Manifestum est, si M sit numerus characteristicus formae primitiuae datae determinantis D, omnes numeros, ipsi M secundum mod. D congruos, fore numeros characteristicos eiusdem formae; formas in eadem classe, siue etiam in classibus diuersis ex eodem genere, contentas eosdem numeros characteristicos habere, quamobrem quiuis numerus characteristicus formae datae etiam toti classi et generi tribui potest; denique 1 semper esse numerum characteristicum formae classis et generis principalis, siue quamlibet formam e genere principali esse residuum determinantis sui.

VII. Si (g, h) est valor expr. $\sqrt{M}\,(a, b, c)$ (mod. m), atque $g' \equiv g$, $h' \equiv h$ (mod. m): erit etiam (g', h') valor eiusdem expressionis. Tales valores pro *aequiualentibus* haberi possunt; contra si (g, h), (g', h') sunt valores eiusdem expr. $\sqrt{M}\,(a, b, c)$, neque tamen simul $g' \equiv g$, $h' \equiv h$ (mod. m), *diuersi* sunt censendi. Manifesto quoties (g, h) est valor talis expressionis, etiam $(-g, -h)$ erit, facileque demonstratur, hos valores semper esse diuersos nisi $m = 2$. Aeque facile demonstratur, expressionem $\sqrt{M}\,(a, b, c)$ (mod. m) plures valores diuersos quam duos tales (oppositos) habere non posse, quando m sit aut numerus primus impar aut nu-

meri primi imparis potestas aut $= 4$; quando vero m sit $= 8$ aut altior potestas numeri 2, quatuor omnino dari. Hinc facile deducitur per VI, si determinans D formae (a, b, c) sit $= \pm 2^{\mu} A^{\alpha} B^{\beta} \ldots$, designantibus A, B etc. numeros primos impares diuersos quorum multitudo $= n$, atque M numerus characteristicus illius formae: dari omnino vel 2^n vel 2^{n+1} vel 2^{n+2} valores diuersos expr. $\sqrt{M}\ (a, b, c)$ (mod. D), prout μ vel < 2 vel $= 2$ vel > 2. Ita e. g. habentur sedecim valores expr. $\sqrt{7}\ (12, 6, -17)$ (mod. 240), puta $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Demonstrationem ampliorem quum ad sequentia non sit adeo necessaria breuitatis gratia non apponimus.

VIII. Denique obseruamus, si duarum formarum aequiualentium (a, b, c), (a', b', c') determinans sit D, numerus characteristicus M, priorque transeat in posteriorem per substitutionem $\alpha, \beta, \gamma, \delta$: ex quouis valore expr. $\sqrt{M}\ (a, b, c)$ vt (g, h) sequi valorem expr. $\sqrt{M}\ (a', b', c')$, puta $(\alpha g + \gamma h, \beta g + \delta h)$. Demonstrationem quisque nullo negotio eruere poterit.

234. Postquam haec de formis in classes genera et ordines distribuendis praemisimus, proprietatesque generales quae ex his distinctionibus statim defluunt explicauimus, ad aliud argumentum grauissimum transimus a nemine hucusque attactum, de formarum *compositione*. In cuius disquisitionis limine, ne posthac demonstrationum

seriem continuam interrumpere oporteat, statim intercalamus

LEMMA. *Habentur quatuor series numerorum integrorum* $a, a', a'' \ldots a^{(n)}$; $b, b', b'' \ldots b^{(n)}$; $c, c', c'' \ldots c^{(n)}$; $d, d', d'' \ldots d^{(n)}$ *ex aeque multis (puta* $n+1$*) terminis constantes, atque ita comparatae, vt* $cd' - dc'$, $cd'' - dc''$ *etc.,* $c'd'' - d'c''$ *etc. etc. respectiue sint* $= k(ab' - ba')$, $k(ab'' - ba'')$ *etc.,* $k(a'b'' - b'a'')$ *etc. etc., siue generaliter* $c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$, *denotante k numerum integrum datum;* λ, μ *integros quoscunque inaequales inter* 0 *et n incl. quorum maior* μ **); praeterea omnes* $a^\lambda b^\mu - b^\lambda a^\mu$ *diuisorem communem non habent. Tunc inueniri possunt quatuor numeri integri* $\alpha, \mathfrak{G}, \gamma, \delta$ *tales, vt sit* $\alpha a + \mathfrak{G} b = c$, $\alpha a' + \mathfrak{G} b' = c'$, $\alpha a'' + \mathfrak{G} b'' = c''$ *etc.;* $\gamma a + \delta b = d$, $\gamma a' + \delta b' = d'$ *etc. siue generaliter* $\alpha a^\nu + \mathfrak{G} b^\nu = c^\nu$, $\gamma a^\nu + \delta b^\nu = d^\nu$; *quo facto erit* $\alpha\delta - \mathfrak{G}\gamma = k$.

Quum per hyp. numeri $ab' - ba'$, $ab'' - ba''$ etc. $a'b'' - b'a''$ etc. (quorum multitudo erit $= \frac{1}{2}(n+1)n$) diuisorem communem non habeant, inueniri poterunt totidem alii numeri integri, per quos illis resp. multiplicatis productorum summa fiat $= 1$ (art. 40). Designentur hi multiplicatores per $(0, 1)$, $(0, 2)$ etc. $(1, 2)$ etc., siue generaliter multiplicator ipsius $a^\lambda b^\mu - b^\lambda a^\mu$ per (λ, μ), ita vt sit $\Sigma(\lambda, \mu)(a^\lambda b^\mu -$

*) Considerando a tamquam a^0, b tamquam b^0 etc. — Ceterum manifesto eadem aequatio valebit quoque quando $\lambda = \mu$ aut $\lambda > \mu$.

$b^\lambda a^\mu) = 1$. (Per literam Σ denotamus aggregatum omnium valorum expressionis, cui praefixa est, qui oriuntur tribuendo ipsis λ, μ omnes valores inaequales inter 0 et n, ita vt sit $\mu > \lambda$). Quo facto si statuitur $\Sigma(\lambda, \mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha$, $\Sigma(\lambda, \mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \mathfrak{b}$, $\Sigma(\lambda, \mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma$, $\Sigma(\lambda, \mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta$: hi α, $\mathfrak{b}$, γ, δ proprietatibus praescriptis erunt praediti.

Dem. I. Denotante ν numerum quemcunque integrum inter 0 et n, erit $\alpha a^\nu + \mathfrak{b} b^\nu = \Sigma(\lambda, \mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu) = \frac{1}{k} \Sigma(\lambda, \mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu) = \frac{1}{k} c^\nu \Sigma(\lambda, \mu)(c^\lambda d^\mu - d^\lambda c^\mu) = c^\nu \Sigma(\lambda, \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu$. Et per calculum similem eruitur $\gamma a^\nu + \delta b^\nu = d^\nu$. *Q. E. P.*

II. Quoniam igitur $c^\lambda = \alpha a^\lambda + \mathfrak{b} b^\lambda$, $c^\mu = \alpha a^\mu + \mathfrak{b} b^\mu$, fit $c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$, similique modo $a^\lambda c^\mu - c^\lambda a^\mu = \mathfrak{b}(a^\lambda b^\mu - b^\lambda a^\mu)$; $d^\lambda b^\mu - b^\lambda d^\mu = \gamma(a^\lambda b^\mu - b^\lambda a^\mu)$; $a^\lambda d^\mu - d^\lambda a^\mu = \delta(a^\lambda b^\mu - b^\lambda a^\mu)$; ex quibus formulis valores ipsorum α, $\mathfrak{b}$, γ, δ multo facilius erui possunt, si modo λ, μ ita accipiuntur vt $a^\lambda b^\mu - b^\lambda a^\mu$ non sit $= 0$, quod certo fieri poterit, quia omnes $a^\lambda b^\mu - b^\lambda a^\mu$ per hyp. diuisorem communem non habent, adeoque *omnes* $= 0$ esse nequeunt. — Ex iisdem aequationibus deducitur, multiplicando primam

per quartam, secundam per tertiam et subtrahendo, $(\alpha\delta - \beta\gamma)\,(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)\,(c^\lambda d^\mu - d^\lambda c^\mu) = k\,(a^\lambda b^\mu - b^\lambda a^\mu)^2$, vnde necessario $\alpha\delta - \beta\gamma = k$. *Q. E. S.*

235. Si forma $AXX + 2BXY + CYY \ldots F$ transit in productum e duabus formis $axx + 2bxy + cyy \ldots f$, et $a'x'x' + 2b'x'y' + c'y'y' \ldots f'$ per substitutionem talem $X = pxx' + p'xy' + p''yx' + p'''yy'$, $Y = qxx' + q'xy' + q''yx' + q'''yy'$ (quod breuitatis causa in sequentibus semper ita exprimemus: Si F transit in ff' per substitutionem $p, p', p'', p'''; q, q', q'', q'''$ *)), dicemus simpliciter, formam F *transformabilem* esse in ff'; si insuper haec transformatio ita est comparata, vt sex numeri $pq' - qp'$, $pq'' - qp''$, $pq''' - qp'''$, $p'q'' - q'p''$, $p'q''' - q'p'''$, $p''q''' - q''p'''$ diuisorem communem non habeant: formam F e formis f, f' *compositam* vocabimus.

Inchoabimus hanc disquisitionem a suppositione generalissima, formam F in ff' transire per substitutionem $p, p', p'', p'''; q, q', q'', q'''$ et quae inde sequantur euoluemus. Manifesto huic suppositioni ex asse aequiualebunt sequentes nouem aequationes (i. e. simulac hae aequationes locum habent, F per substitutionem dictam transibit in ff', et vice versa):

*) In hac igitur designatione ad ordinem tum coefficientium p, p' etc. tum formarum f, f' probe respicere oportet. Facile autem perspicietur, si ordo formarum f, f' conuertatur vt prior fiat posterior, coefficientes p', q' cum his p'', q'' commutandos esse, reliquos suo quemlibet loco manere.

$$App + 2Bpq + Cqq = aa' \ldots\ldots\ldots [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac' \ldots\ldots\ldots [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca' \ldots\ldots\ldots [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc' \ldots\ldots [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \ldots\ldots [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \ldots [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb' \ldots [9]$$

Sint determinantes formarum F, f, f' resp. D, d, d'; diuisores communes maximi numerorum $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ resp. M, m, m' (quos omnes positiue acceptos supponimus). Porro determinentur sex numeri integri $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ ita vt sit $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, $\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$. Denique designentur numeri $pq' - qp'$, $pq'' - qp''$, $pq''' - qp'''$, $p'q'' - q'p''$, $p'q''' - q'p'''$, $p''q''' - q''p'''$ resp. per P, Q, R, S, T, U, sitque ipsorum diuisor communis maximus positiue acceptus $= k$. — Iam ponendo

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \quad [10]$$

fit ex aequ. 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \quad [11]$$

Ex his vndecim aequationibus 1 ... 11, sequentes nouas euoluimus *):

*) Origo harum aequationum haec est: 12 ex 5. 5 — 1. 2; 13 ex 5. 9 — 1. 7 — 2. 6; 14 ex 10. 11 — 6. 7; 15 ex 5. 8 + 5. 8 + 10. 10 + 11. 11 — 1. 4 — 2. 3 —

$$DPP = d'aa \quad [12]$$
$$DP(R - S) = 2d'ab \quad [13]$$
$$DPU = d'ac - (\Delta\Delta - dd') \quad [14]$$
$$D(R - S)^2 = 4d'bb + 2(\Delta\Delta - dd') \quad [15]$$
$$D(R - S)U = 2d'bc \quad [16]$$
$$DUU = d'cc \quad [17]$$
$$DQQ = da'a' \quad [18]$$
$$DQ(R + S) = 2da'b' \quad [19]$$
$$DQT = da'c' - (\Delta\Delta - dd') \quad [20]$$
$$D(R + S)^2 = 4db'b' + 2(\Delta\Delta - dd') \quad [21]$$
$$D(R + S)T = 2db'c' \quad [22]$$
$$DTT = dc'c' \quad [23]$$

Hinc rursus deducuntur hae duae:

$$0 = 2d'aa(\Delta\Delta - dd')$$
$$0 = (\Delta\Delta - dd')^2 - 2d'ac(\Delta\Delta - dd')$$

scilicet prior ex 12. 15 — 13. 13, posterior ex 14. 14 — 12. 17; vnde facile perspicitur, necessario esse $\Delta\Delta - dd' = 0$, siue sit $a = 0$, siue non sit $= 0$ *). Supponemus itaque, in aequatt. 14, 15, 20, 21 ad dextram deleri $\Delta\Delta - dd'$.

Iam statuendo

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n$$

6. 7 — 6. 7; 16 ex 8. 9 — 3. 7 — 4. 6; 17 ex 8. 8 — 3. 4. Deductio sex reliquarum eodem modo adornatur, si modo aequationes 2, 5, 7 cum aequationibus 3, 6, 8 resp. commutantur, et reliquae 1, 4, 9, 10, 11 eodem loco deinceps retinentur, puta 18 ex 6. 6 — 1. 3 etc.

*) Haec deriuatio aequationis $\Delta\Delta = dd'$ ad institutum praesens sufficit; alioquin analysin elegantiorem sed hic nimis prolixam tradere possemus, directe deducendo ex aequationibus 1 ... 11 hanc $0 = (\Delta\Delta - dd')^2$.

(vbi n, n' etiam fractiones euadere posse probe notandum, etsi mn', $m'n$ necessario sint integri); facile ex aequatt. 12 ... 17 deducitur

$$Dmmn'n' = d' (\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'mm$$

similiterque ex aequ. 18 ... 23

$$Dm'm'nn = d (\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'm'.$$

Erit igitur $d = Dnn$, $d' = Dn'n'$, vnde nanciscimur CONCLVSIONEM PRIMAM: *Determinantes formarum F, f, f' necessario inter se habent rationem quadratorum;* et SECVNDAM: *D semper metitur numeros $dm'm'$, $d'mm$.* Patet itaque, D, d, d' eadem signa habere, nullamque formam in productum ff' transformabilem esse posse, cuius determinans maior sit quam diuisor communis maximus numerorum $dm'm'$, $d'mm$.

Multiplicentur aequationes 12, 13, 14 resp. per $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$; similiterque per eosdem numeros aequatt. 13, 15, 16, et 14, 16, 17; addantur terna producta, diuidaturque summa per Dmn', scripto pro d', $Dn'n'$. Tunc prodit

$$P = an', R - S = 2bn', U = cn'$$

Simili modo multiplicatis aequationibus 18, 19, 20 nec non 19, 21, 22 et 20, 22, 23 resp. per $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, obtinetur

$$Q = a'n, R + S = 2b'n, T = c'n.$$

Hinc habetur CONCLVSIO TERTIA: *Numeri a, $2b$, c proportionales sunt numeris P, $R -$*

S, U, positaque illorum ratione ad hos vt 1 *ad* n', *erit* n' *radix quadrata ex* $\frac{d'}{D}$; *similiterque numeri* a', $2b'$, c' *ad* Q, $R + S$, T *eandem rationem habent, quae si ponitur esse vt* 1 *ad* n, *erit* n *radix quadrata ex* $\frac{d}{D}$.

Ceterum quantitates n, n' radices vel positiuae vel negatiuae ex $\frac{d}{D}$, $\frac{d'}{D}$ esse possunt, vnde distinctionem petimus, quae primo aspectu sterilis videbitur, sed cuius vsus in sequentibus sufficienter apparebit. Scilicet dicemus, in transformatione formae F in ff' formam f accipi *directe* quando n est positiua, inuerse quando n negatiua; similiterque f' accipi directe vel inuerse prout n' positiua vel negatiua. Accedente autem conditione vt k sit $= 1$, forma F *vel* ex vtraque forma f, f' directe composita, *vel* ex vtraque inuerse *vel* ex f directe et ex f' inuerse, *vel* ex f inuerse et ex f' directe dicetur, prout vel n, n' ambae sunt positiuae, vel ambae negatiuae, vel prior positiua posterior negatiua, vel prior negatiua posterior positiua. Ceterum quisque facile intelliget, has relationes ab ordine quo formae f, f' collocantur (vid. annot. prima ad art. praes.) non pendere.

Porro obseruamus, diuisorem maximum communem numerorum P, Q, R, S, T, U puta k metiri numeros mn', $m'n$ (vti ex valoribus supra stabilitis manifestum est) adeoque quadratum kk ipsos $mmn'n'$, $m'm'nn$, atque Dkk ipsos $d'mm$, $dm'm'$. Sed et vice versa quiuis diuisor

communis ipsorum mn', $m'n$ metietur ipsum k. Sit enim e talis diuisor qui manifesto etiam numeros an', $2bn'$, cn', $a'n$, $2b'n$, $c'n$ metietur, i. e. numeros P, $R - S$, U, Q, $R + S$, T et proin etiam ipsos $2R$ et $2S$. Iam si $\frac{2R}{e}$ esset numerus impar, etiam $\frac{2S}{e}$ impar esse deberet (quoniam summa et differentia sunt pares) adeoque etiam productum impar. Hoc autem productum fit $= \frac{4}{ee}(b'b'nn - bbn'n') = \frac{4}{ee}(d'nn + a'c'nn - dn'n' - acn'n') = \frac{4}{ee}(a'c'nn - acn'n')$ adeoque par, quia e ipsos $a'n$, $c'n$, an', cn' metitur. Quare $\frac{2R}{e}$ necessario erit par, et proin R nec non S per e diuisibilis. Quoniam igitur e omnes sex P, Q, R, S, T, U metitur, metietur etiam ipsorum diuisorem communem maximum k. *Q. E. D.* — Hinc concluditur k esse diuisorem communem maximum numerorum mn', $m'n$; vnde facile perspicietur, *Dkk fore diuisorem communem maximum numerorum* $dm'm'$, $d'mm$. Quae est CONCLVSIO QVARTA. Patet itaque, quoties F ex f et f' composita sit, D fore diuisorem communem maximum, numerorum $dm'm'$, $dm'm$, et vice versa; quae proprietas etiam tamquam definitio formae compositae adoptari potuisset. Forma igitur composita e formis f, f' determinantem maximum possibilem inter omnes formas in productum ff' transformabiles habet.

Antequam vlterius progredi possimus, ante omnia valorem ipsius Δ accuratius definire oportet,

quem quidem ostendimus esse $= \sqrt{dd'} = \sqrt{DDnnn'n'}$, sed cuius *signum* hinc nondum determinatur. Ad hunc finem ex aequ. fundamentalibus 1 — 11 eruimus $DPQ = \Delta aa'$ (quae aequ. obtinetur ex 5. 6 — 1. 11), adeoque $Daa'nn' = \Delta aa'$, vnde, nisi aliquis numerorum a, a' est $= 0$, fit $\Delta = Dnn'$. Sed prorsus simili modo ex aequatt. fundd. octo aliae deduci possunt in quibus ad laeuam Dnn' ad dextram Δ multiplicati habeantur per $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc' *), vnde facile concluditur propterea quod neque omnes a, $2b$, c, neque omnes a', $2b'$, c' possunt esse $= 0$, in omnibus casibus fieri $\Delta = Dnn'$, adeoque Δ idem signum habere vt D, d, d' vel oppositum, prout n, n' eadem signa habeant vel diuersa.

Porro obseruamus, numeros aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb' + 2\Delta$, $2bb' - 2\Delta$ omnes per mm' diuisibiles esse. De nouem prioribus hoc per se manifestum est, de duobus reliquis autem simili modo demonstrari potest vt antea ostendimus R et S per e diuisibiles esse. Scilicet patet, $4bb + 4\Delta$ et $4bb' - 4\Delta$ per mm' diuisibiles esse (quoniam $4\Delta = \sqrt{16dd'}$ atque $4d$ per mm, $4d'$ per $m'm'$ diuisibilis, adeoque $16dd'$ per $mmm'm'$ et 4Δ per mm') et differentiam quotientium parem; productum ex quotientibus facile demonstratur esse par, vnde vterque quotiens par, et $2bb' + 2\Delta$, $2bb' - 2\Delta$ per mm' diuisibiles.

*) Analysin quam lectores facile detegere poterunt breuitatis caussa supprimere oportet.

Iam ex vndecim aequationibus fundamentalibus facile deducuntur sex sequentes:

$$APP = aa'q'q' - 2ab'qq' + ac'qq$$
$$AQQ = aa'q''q'' - 2ba'qq'' + ca'qq$$
$$ARR = aa'q'''q''' - 2(bb' + \Delta)qq'' + cc'qq$$
$$ASS = ac'q''q'' - 2(bb' - \Delta)q'q'' + ca'q'q'$$
$$ATT = ac'q'''q''' - 2bc'q'q''' + cc'q'q'$$
$$AUU = ca'q'''q''' - 2cb'q''q''' + cc'q''q''$$

Hinc sequitur, omnes APP, AQQ etc. diuisibiles esse per mm', vnde facile deriuatur, quoniam kk diuisor communis maximus numerorum PP, QQ, RR etc., etiam Akk per mm' diuisibilem esse. Substitutis autem pro a, $2b$, c, a', $2b'$, c' valoribus suis $\frac{P}{n'}$ etc. siue $\frac{1}{n'}(pq' - qp')$ etc., transibunt in sex alias aequationes, in quibus ad dextram habebuntur producta ex quantitate $\frac{1}{nn'}(q'q'' - qq''')$ in PP, QQ, RR etc. Calculum facillimum lectoribus relinquimus. Hinc sequitur (quoniam omnes PP, QQ etc. esse $= 0$ nequeunt) $Ann' = q'q'' - qq'''$.

Simili modo ex aequationibus fundamentalibus deriuantur sex aliae aequationes, a praecedentibus in eo tantummodo discrepantes, quod pro A vbique habetur C et pro q, q', q'', q''' resp. p, p', p'', p''', quas ipsas breuitatis caussa non adscribimus. Hinc eodem modo sequitur, Ckk per mm' diuisibilem esse atque $Cnn' = p'p'' - pp'''$.

Denique ex eodem fonte petuntur sex aequationes hae:

$$BPP = -aa'p'q' + ab'(pq' + qp') - ac'pq$$
$$BQQ = -aa'p''q'' + ba'(pq'' + qp'') - ca'pq$$
$$BRR = -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq$$
$$BSS = -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q'$$
$$BTT = -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'q'q'$$
$$BUU = -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'q''q''$$

vnde perinde vt ante concluditur, $2Bkk$ diuisibilem esse per mm' atque $2Bnn' = pq''' + qp''' - p'q'' - q'p''$.

Quoniam itaque Akk, $2Bkk$, Ckk per mm' sunt diuisibiles, facile perspicietur, etiam Mkk per mm' diuisibilem esse debere. Ex aequationibus fundamentalibus autem colligitur, M metiri ipsos aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', adeoque etiam ipsos am', $2bm'$, cm' (qui sunt diuisores comm. max. trium primorum mediorum et vltimorum resp.); denique etiam ipsum mm' qui est horum diu. comm. max. Hinc patet, in eo casu vbi forma F ex formis f, f' composita est siue $k = 0$, necessario esse $M = mm'$. Quae est CONCLVSIO QVINTA.

Si diu. comm. max. numerorum A, B, C est $\mathfrak{M}$, hic erit vel $= M$ (quando forma F est proprie primitiua vel ex proprie primitiua deriuata) vel $= \frac{1}{2} M$ (quando F est forma improprie primitiua vel ex improprie prim. deriuata); similiter designando diuisores comm. max. numerorum a, b, c; a', b', c' resp. per $\mathfrak{m}$, $\mathfrak{m}'$ erit $\mathfrak{m}$ vel $= m$ vel $\frac{1}{2} m$, et $\mathfrak{m}'$ vel $= m'$ vel $= \frac{1}{2} m'$. Iam patet, $\mathfrak{m}\mathfrak{m}$ metiri ipsum d, $\mathfrak{m}'\mathfrak{m}'$ ipsum d', adeoque $\mathfrak{m}\mathfrak{m}\mathfrak{m}'\mathfrak{m}'$

ipsum dd' siue $\Delta\Delta$, et $\mathfrak{mm}'$ ipsum Δ. Hinc ex sex vltimis aequationibus pro BPP etc. sequitur, $\mathfrak{mm}'$ metiri ipsum Bkk, adeoque (quum etiam ipsos Akk, Ckk metiatur) etiam ipsum $\mathfrak{M}kk$. Quoties igitur F ex f, f' composita est, metietur $\mathfrak{mm}'$ ipsum $\mathfrak{M}$. Quando itaque in hoc casu vtraque f, f' est proprie primitiua vel ex proprie primitiua deriuata siue $\mathfrak{mm}' = mm' = M$, erit $\mathfrak{M} = M$, siue F similis forma. Quando vero, in eadem suppositione, aut vtraque f, f' aut alterutra saltem est improprie primitiua vel ex improprie primitiua deriuata, *e. g.* forma f; ex aequationibus fundamentalibus sequitur, aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc' per $\mathfrak{M}$ diuisibiles esse adeoque etiam am', bm', cm' et hinc quoque $\mathfrak{m}m' = \frac{1}{2} mm' = \frac{1}{2} M$; vnde necessario in hoc casu erit $\mathfrak{M} = \frac{1}{2} M$, siue etiam forma F vel impr. prim. vel ex impr. prim. deriuata. Quae efficiunt CONCLVSIONEM SEXTAM.

Tandem obseruamus, si nouem aequationes $an' = P$, $2bn' = R - S$, $cn' = U$, $a'n = Q$, $2b'n = R + S$, $c'n = T$, $Ann' = q'q'' - qq'''$, $2Bnn' = pq''' + qp''' - p'q'' - q'p''$, $Cnn' = p'p'' - pp'''$ (quas, quoniam in sequentibus saepius ad ipsas reuenire oportebit, per Ω designabimus) locum habere *supponantur*, spectatis adeo ipsis n, n' tamquam incognitis, quarum tamen neutra $= 0$: per substitutionem facile confirmari, etiam aequationes fundamentales 1 — 9 necessario veras esse siue formam (A, B, C) per substitutionem p, p', p'', p'''; q, q', q'', q''' in productum e formis (a, b, c) (a', b', c') transire; praetereaque esse $bb - ac = nn\,(BB - AC)$,

$b'b' - a'c' = n'n' (BB - AC)$. Calculum quem hic apponere nimis prolixum foret lectorum industriae committimus.

236. Problema. *Propositis duabus formis quarum determinantes aut aequales sunt aut saltem rationem quadratorum inter se habent: inuenire formam ex illis compositam.*

Sol. Sint formae componendae $(a, b, c) \ldots f$, $(a', b', c') \ldots f'$; harum determinantes d, d'; diuisores communes maximi numerorum a, $2b$, c; a', $2b'$, c' resp. m, m'; diuisor comm. maximus numerorum $dm'm'$, $d'mm$ eodem signo vt d, d' affectus D. Tunc $\frac{dm'm'}{D}$, $\frac{d'mm}{D}$ erunt numeri positiui inter se primi ipsorumque productum, quadratum; quare ipsi erunt quadrata (art. 21). Hinc $\sqrt{\frac{d}{D}}$, $\sqrt{\frac{d'}{D}}$ erunt quantitates rationales quas ponemus $= n$, n', et quidem accipiemus pro n valorem positiuum vel negatiuum, prout forma f in compositionem vel directe vel inuerse ingredi debet, similiterque signum ipsius n ex ratione qua f' in compositionem ingredi debet determinabimus. Erunt itaque mn', $m'n$ numeri integri inter se primi; n et n' autem etiam fractiones esse possunt. His ita factis, obseruamus, an', cn', $a'n$, $c'n$, $bn' + b'n$, $bn' - b'n$ esse integros, quod de quatuor prioribus per se manifestum est (quum $an' = \frac{a}{m} mn'$ etc.); de duobus reliquis eodem modo probatur vt in art. praec. demonstratum fuit R et S per e diuisibiles esse.

Iam accipiantur quatuor numeri integri $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$ ad libitum, ea sola conditione vt quatuor quantitates in aequatione sequente (I) ad laeuam positae non omnes simul = o fiant, ponaturque ... (I)

$$\begin{aligned}
&\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}''' (bn' + b'n) = \mu q \\
&- \mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}'' (bn' - b'n) = \mu q' \\
&\mathfrak{Q}''' cn' - \mathfrak{Q}a'n + \mathfrak{Q}' (bn' - b'n) = \mu q'' \\
&-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q} (bn' + b'n) = \mu q'''
\end{aligned}$$

ita vt q, q', q'', q''' fiant integri diuisorem communem non habentes, quod obtinetur accipiendo pro μ diuisorem communem maximum quatuor numerorum qui in his aequationibus sunt ad laeuam. Tunc igitur per art. 40 inueniri poterunt quatuor numeri integri $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ tales vt fiat $\mathfrak{P}q + \mathfrak{P}'p' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$. Quo facto determinentur numeri p, p', p'', p''' per aequationes sequentes ... (II):

$$\begin{aligned}
&\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}''' (bn' + b'n) = p \\
&- \mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}'' (bn' - b'n) = p' \\
&\mathfrak{P}''' cn' - \mathfrak{P}a'n + \mathfrak{P}' (bn' - b'n) = p'' \\
&- \mathfrak{P}''cn' - \mathfrak{P}'c'n - \mathfrak{P} (bn' + b'n = p'''
\end{aligned}$$

Tandem ponatur $q'q'' - qq''' = Ann'$, $pq''' + qp''' - p'q'' - q'p'' = 2Bnn'$, $p'p'' - pp''' = Cnn'$. Tunc A, B, C erunt numeri integri formaque (A, B, C) ... F ex formis f, f' composita.

Dem. I. Ex aequatt. I et II nullo negotio confirmantur sequentes quatuor aequationes ... (III):

$$\begin{aligned}
&o = q'cn' - q''c'n - q''' (bn' - b'n) \\
&o = qcn' + q'''a'n - q'' (bn' + b'n)
\end{aligned}$$

$$0 = q'''an' + qc'n - q'(bn' + b'n)$$
$$0 = q''an' - q'a'n - q(bn' - b'n)$$

II. Iam ponamus, numeros integros $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \mathfrak{N}, \mathfrak{N}'$ ita determinatos esse vt fiat $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, $\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$, $\mathfrak{N}m'n + \mathfrak{N}'mn' = 1$. Tunc erit $\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1$. Hinc atque ex aequatt. (III) facile confirmatur, si statuatur.

$$-q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) = q$$
$$q'\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) = q'$$
$$-q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) = q''$$
$$q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) = q'''$$

fore ... (IV)

$$q'an' + q''a'n + q'''(bn' + b'n) = q$$
$$-qan' + q'''c'n - q''(bn' - b'n = q'$$
$$q'''cn' - qa'n + q'(bn' - b'n) = q''$$
$$-q''cn' - q'c'n - q(bn' + b'n) = q'''$$

Quoties $\mu = 1$, hae aequationes non sunt necessariae, sed ipsarum loco aequationes (I), quibus omnino analogae sunt, retineri possunt. Quodsi nunc ex aequatt. II, IV valores ipsorum Ann', $2Bnn'$, Cnn' (i. e. numerorum $q'q'' - qq'''$ etc.) euoluuntur, et quae mutuo se destruunt delentur: inuenietur, singulorum partes esse vel producta ex integris in nn', vel ex integris in $dn'n'$ vel ex integris in $d'nn$, insuperque omnes partes constituentes ipsius $2Bnn'$ implicare factorem 2. Hinc concluditur (quoniam

$dn'n' = d'nn$, et proin $\frac{dn'n'}{nn'} = \frac{d'nn}{nn'} = \sqrt{dd'}$ sunt integri), A, B, C esse numeros integros. *Q. E. P.*

III. Substituendo ex aequatt. (II) valores ipsorum p, p', p'', p''', facile comprobatur adiumento aequatt. (III) et huius $\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$, esse $pq' - qp' = an'$, $pq''' - qp''' - p'q'' + q'p'' = 2bn'$, $p''q''' - q''p''' = cn'$, $pq'' - qp'' = a'n$, $pq''' - qp''' + p'q'' - q'p'' = 2b'n$, $p'q''' - q'p''' = c'n$, quae aequationes identicae sunt cum sex prioribus (Ω) art. praec.; tres reliquae autem iam per hyp. locum habent. Quare (*ibid. sub fin.*) forma F transibit in ff' per substitutionem p, p', p'', p'''; q, q', q'', q'''; ipsiusque determinans erit $= D$, siue aequalis diuis. comm. max. numerorum $dm'm'$, $d'mm$, quamobrem per concl. quartam art. praec. F ex f, f' composita erit. *Q. E. S.* Denique facile perspicietur, F ex f, f' *ita* compositam esse vt praescriptum sit, quum signa quantitatum n, n' iam ab initio rite sint determinata.

237. Theorema. *Si forma F in productum e duabus formis f, f' est transformabilis, atque forma f' formam f'' implicat: F etiam in productum e formis f, f'' transformabilis erit.*

Dem. Retineantur pro formis F, f, f' omnia signa art. 235; forma f'' sit $= (a'', b'', c'')$, transeatque f' in f'' per substitutionem α, β, γ, δ. Tunc nullo negotio perspicietur, F transire in ff'' per substitutionem $\alpha p + \gamma p'$, $\beta p + \delta p'$, $\alpha p'' +$

$\gamma p'''$, $\epsilon p'' + \delta p'''$; $\alpha q + \gamma q'$, $\epsilon q + \delta q'$; $\alpha q'' + \gamma q'''$, $\epsilon q'' + \delta q'''$. *Q. E. D.*

Positis breuitatis caussa coefficientibus $\alpha p + \gamma p'$, $\epsilon p + \delta p'$ etc., $= \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$; $\mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$; numeroque $\alpha\delta - \epsilon\gamma = e$: ex aequatt. Ω art. 235 facile confirmatur, esse $\mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' = an'e$, $\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' = 2bn'e$, $\mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' = cn'e$; $\mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' = \alpha\alpha a'n + 2\alpha\gamma b'n + \gamma\gamma c'n = a''n$, $\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' = 2b''n$, $\mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' = c''n$; $\mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' = Ann'e$, $\mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' = 2Bnn'e$, $\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' = Cnn'e$. Iam designato determinante formae f'' per d'', erit e radix quadrata ex $\frac{d''}{d'}$, et quidem positiua vel negatiua, prout forma f' formam f'' vel proprie vel improprie implicat. Quare $n'e$ erit radix quadrata ex $\frac{d''}{D}$; vnde patet, nouem aequationes praecedentes aequationibus Ω art. 235 prorsus analogas esse, formamque f in transformatione formae F in ff'' eodem modo accipi, vt in transformatione formae F in ff'; formam f'' vero in illa vel eodem modo vt f' in hac, vel opposito, prout f' ipsam f'' proprie implicet vel improprie.

238. Theorema. *Si forma F sub forma F' est contenta atque in productum e formis f, f' transformabilis: etiam forma F' in idem productum transformabilis erit.*

Dem. Retentis pro formis F, f, f' iisdem signis vt supra et supponendo formam F' trans-

ire in F per substitutionem α, β, γ, δ, facile perspicietur, F' per substitutionem $\alpha p + \beta q$, $\alpha p' + \beta q'$, $\alpha p'' + \beta q''$, $\alpha p''' + \beta q'''$; $\gamma p + \delta q$, $\gamma p' + \delta q'$, $\gamma p'' + \delta q''$, $\gamma p''' + \delta q'''$, idem fieri quod F per substitutionem p, p', p'', p'''; q, q', q'', q''', adeoque F' per substitutionem illam transire in ff'. *Q. E. D.*

Praeterea per similem calculum vt in art. praec. facile confirmatur, F' eodem modo in ff' transformabilem fore vt F, quando F' ipsam F proprie implicet; quando vero F improprie sub F' contenta sit, transformationes formae F in ff' et formae F' in ff' oppositas fore respectu vtriusque formae f, f', scilicet quae ex his formis in alteram transformationem directe ingrediatur, in altera accipi inuerse.

Ex combinatione theorematis praesentis cum theor. art. praec. obtinemus sequens generalius: *Si forma F in productum ff' est transformabilis, atque formae f, f' resp. implicant formas g, g', forma F vero sub forma F' contenta est: G in productum gg' transformabilis erit.* Nam per theor. art. praes. G, transformabilis erit in ff', hinc per theor. art. praec. in fg' et per idem theor. etiam in gg'. Porro patet, si omnes tres formae f, f', G formas g, g', F proprie implicent, G eodem modo in gg' transformabilem fore respectu formarum g, g' vt F in ff' respectu formarum f, f'; idem euenire, si illae tres implicationes omnes sint impropriae; denique aeque facile determinari poterit, *quomodo* G in gg' transformabilis sit,

si ex illis implicationibus aliqua duabus reliquis sit dissimilis.

Si formae F, f, f' formis G, g, g' resp. sunt aequiualentes, hae eosdem determinantes habebunt vt illae, et quod pro formis f, f' sunt numeri m, m', idem erunt pro formis g, g' (art. 161). Hinc nullo negotio per conclus. quartam art. 235 deducitur, in hocce casu G ex g, g' *compositam* fore, si F ex f, f' composita sit, et quidem formam g in compositionem illam eodem modo ingredi vt f in hanc, quando F ipsi G eodem modo aequiualeat vt f ipsi g, et contra; similiterque g' in compositione priori vel eodem modo vel opposito accipiendam vt f' in posteriori, prout aequiualentia formarum f', g' aequiualentiae formarum F, G similis sit vel dissimilis.

239. Theorema. *Si forma F ex formis f, f' composita est: quaeuis alia forma in productum ff' eodem modo transformabilis vt F, ipsam F proprie implicabit.*

Dem. Retentis pro F, f, f' omnibus signis art. 235, aequationes Ω etiam hic locum habebunt. Ponamus formam $F' = (A', B', C')$, cuius determinans $= D'$, transire in productum ff' per substitutionem $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''; \mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \mathfrak{q}'''$ designemusque numeros $\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}'$, $\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}''$, $\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}'''$, $\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}''$, $\mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}'''$, $\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$ resp. per P', Q', R', S', T', U'. Tunc habebuntur nouem aequationes ipsis Ω omnino similes puta $P' = an'$, $R' - S' = 2bn'$, $U' =$

$c\mathfrak{n}'$, $Q' = a'\mathfrak{n}$, $R' + S' = 2b'\mathfrak{n}$, $T' = c'\mathfrak{n}$, $\mathfrak{q}'\mathfrak{q}''$ $- \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}'$, $\mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}'$, $\mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}'$, quas per Ω' designabimus. Quantitates $\mathfrak{n}$, $\mathfrak{n}'$ hic erunt radices quadratae ex $\frac{d}{D'}$, $\frac{d'}{D'}$ et quidem iisdem signis resp. affectae vt n, n'; si igitur radix quadrata ex $\frac{D}{D'}$ positiue accepta (quae erit numerus integer) statuitur $= k$, erit $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. Hinc et ex aequatt. senis prioribus in Ω et Ω' manifestum est, fore $P' = kP$, $Q' = kQ$, $R' = kR$, $S' = kS$, $T' = kT$, $U' = kU$. Quare per lemma art. 234 determinari poterunt quatuor numeri integri α, β, γ, δ tales vt fiat $\alpha\mathfrak{p} + \beta\mathfrak{q} = \mathfrak{p}$, $\gamma\mathfrak{p}$ $+ \delta\mathfrak{q} = \mathfrak{q}$; $\alpha\mathfrak{p}' + \beta\mathfrak{q}' = \mathfrak{p}'$, $\gamma\mathfrak{p}' + \delta\mathfrak{q}' = \mathfrak{q}'$ etc., atque $\alpha\delta - \beta\gamma = k$. Substitutis his valoribus ipsorum $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{q}'$ etc. in aequatt. tribus vltimis Ω', facile confirmatur adiumento aequationum $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ triumque vltimarum Ω, fore $A'\alpha\alpha$ $+ 2B'\alpha\gamma + C'\gamma\gamma = A$, $A'\alpha\beta + B'(\alpha\delta + \beta\gamma) +$ $C'\gamma\delta = B$, $A'\beta\beta + 2B'\beta\delta + C'\delta\delta = C$, quapropter forma F' per substitutionem α, β, γ, δ (quae propria erit, quoniam $\alpha\delta - \beta\delta = k$ est positiuus) transibit in F, i. e. formam F proprie implicabit. *Q. E. D.*

Si itaque F' e formis f, f' etiam composita est (eodem modo vt F ex iisdem), formae F, F' eundem determinantem habebunt, eruntque adeo proprie aequiualentes. Generalius, si forma G e formis g, g' eodem modo composita est vt F ex f, f' resp., formaeque g, g' ipsis f, f' proprie aequiualent: formae F, G proprie aequiualebunt.

Quum is casus vbi ambae formae componendae compositionem directe ingrediuntur simplicissimus sit, ad ipsumque reliqui facile reducantur, illum solum in sequentibus contemplabimur, ita vt si forma aliqua simpliciter dicatur e duabus aliis composita, semper subintelligere oporteat, ex vtraque illam proprie esse compositam *). Eadem restrictio valebit, quoties forma in productum e duabus aliis transformabilis dicetur.

240. Theorema. *Si e formis f, f' composita est forma F; ex F et f'' forma $\mathfrak{F}$; ex f, f'' forma F'; ex F' et f' forma $\mathfrak{F}'$: formae $\mathfrak{F}$, $\mathfrak{F}'$ proprie aequiualentes erunt.*

Dem. I. Sit $f = axx + 2bxy + cyy$, $f' = a'x'x' + 2b'x'y' + c'y'y'$, $f'' = a''x''x'' + 2b''x''y'' + c''y''y''$, $F = AXX + 2BXY + CYY$, $F' = A'X'X' + 2B'X'Y' + C'Y'Y'$, $\mathfrak{F} = \mathfrak{A}\mathfrak{X}\mathfrak{X} + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}\mathfrak{Y}$, $\mathfrak{F}' = \mathfrak{A}'\mathfrak{X}'\mathfrak{X}' + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'\mathfrak{Y}'$; determinantes harum septem formarum resp. d, d', d'', D, D', $\mathfrak{D}$, $\mathfrak{D}'$, qui omnes eadem signa et rationem quadratorum inter se habebunt. Porro sit m diuisor communis maximus numerorum a, $2b$, c, similemque significationem habeant m', m'', M relatiue ad formas f', f'', F. Tum ex concl. 4 art. 235, D erit diu. comm. max. numerorum $dm'm'$, $d'mm$, adeoque $Dm''m''$ diu. comm. max. numerorum $dm'm'm''m''$,

*) Similiter vt in compositione rationum (quae cum compositione formarum magnam analogiam habet) subintelligi solet, rationes componendas directe accipiendas esse nisi vbi contrarium monetur.

$d'mmm''m''$; $M = mm'$; $\mathfrak{D}$ diu. comm. max. num. $Dm''m''$, $d''MM$, siue numerorum $Dm''m''$, $d''mmm'm'$. Hinc concluditur, $\mathfrak{D}$ esse diu. comm. max. trium numerorum $dm'm'm''m''$, $d'mmm''m''$, $d''mmm'm'$; ex simili autem ratione $\mathfrak{D}'$ eorundem trium numerorum diuisor communis maximus erit; quare quum $\mathfrak{D}$, $\mathfrak{D}'$ eadem signa habeant, erit $\mathfrak{D} = \mathfrak{D}'$, siue formae $\mathfrak{F}$, $\mathfrak{F}'$ eundem determinantem habebunt.

II. Iam transeat F in ff' per substitutionem $X = pxx' + p'xy' + p''yx' + p'''yy'$, $Y = qxx' + q'xy' + q''yx' + q'''yy'$, atque $\mathfrak{F}$ in Ff'' per substitutionem $\mathfrak{X} = \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy''$, $\mathfrak{Y} = \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy''$, designenturque radices quadratae positiuae ex $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\mathfrak{D}}$, $\frac{d''}{\mathfrak{D}}$ per n, n', $\mathfrak{N}$, $\mathfrak{n}''$. Tunc per art. 253 habebuntur decem et octo aequationes, quarum semissis altera ad transformationem formae F in ff' pertinebit, altera ad transformationem formae $\mathfrak{F}$ in Ff''. Prima erit $pq' - qp' = an'$, ad cuius instar facile formari poterunt reliquae breuitatis gratia hic omittendae. Ceterum quantitates n, n', $\mathfrak{N}$, $\mathfrak{n}''$ rationales quidem erunt, sed non necessario numeri integri.

III. Si valores ipsorum X, Y in valoribus ipsorum $\mathfrak{X}$, $\mathfrak{Y}$ substituuntur, prodit substitutio talis: $\mathfrak{X} = (1)\ xx'x'' + (2)\ xx'y'' + (3)\ xy'x'' + (4)\ xy'y'' + (5)\ yx'x'' + (6)\ yx'y'' + (7)\ yy'x'' + (8)\ yy'y''$; $\mathfrak{Y} = (9)\ xx'x'' + (10)\ xx'y'' + (11)\ xy'x'' + (12)\ xy'y'' + (13)\ yx'x'' + (14)\ yx'y'' + (15)\ yy'x'' + (16)\ yy'y''$, per quam manifesto

$\mathfrak{F}$ transibit in productum $ff'f''$. Coefficiens (1) erit $= pp + qp''$; valores quindecim reliquorum non apponimus, quippe quos quisque nullo negotio euoluet. Designemus numerum (1) (10) — (2) (9) per (1, 2), numerum (1) (11) — (3) (9) per (1, 3), et generaliter $(g)\ (8+h) - (h)\ (8+g)$ per (g, h), supponendo g, h esse integros inaequales inter 1 et 16 quorum maior h*); hoc modo omnino viginti et octo signa habebuntur. Iam denotatis radicibus quadratis positiuis ex $\frac{d}{\mathfrak{D}}$, $\frac{d'}{\mathfrak{D}}$ per $\mathfrak{n}, \mathfrak{n}'$ (quae erunt $= \mathfrak{n}\mathfrak{M}$, $\mathfrak{n}'\mathfrak{M}$), eruentur sequentes 28 aequationes: $(1, 2) = aa'\mathfrak{n}''$, $(1, 3) = aa''\mathfrak{n}'$, $(1, 4) = ab'\mathfrak{n}'' + ab''\mathfrak{n}'$, $(1, 5) = a'a''\mathfrak{n}$, $(1, 6) = a'b\mathfrak{n}'' + a'b''\mathfrak{n}$, $(1, 7) = a''b\mathfrak{n}' + a''b'\mathfrak{n}$, $(1, 8) = bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}nn'\mathfrak{n}''$, $(2, 3) = ab''\mathfrak{n}' - ab'\mathfrak{n}''$, $(2, 4) = ac''\mathfrak{n}'$, $(2, 5) = a'b''\mathfrak{n} - a'b\mathfrak{n}''$, $(2, 6) = a'c''\mathfrak{n}$, $(2, 7) = bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}nn'\mathfrak{n}''$, $(2, 8) = bc''\mathfrak{n}' + b'c''\mathfrak{n}$, $(3, 4) = ac'\mathfrak{n}''$, $(3, 5) = a''b'\mathfrak{n} - a''b\mathfrak{n}'$, $(3, 6) = bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}nn'\mathfrak{n}''$, $(3, 7) = a''c'\mathfrak{n}$, $(3, 8) = bc'\mathfrak{n}'' + b''c'\mathfrak{n}$, $(4, 5) = b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}nn'\mathfrak{n}''$, $(4, 6) = b'c''\mathfrak{n} - bc''\mathfrak{n}'$, $(4, 7) = b''c'\mathfrak{n} - bc'\mathfrak{n}''$, $(4, 8) = c'c''\mathfrak{n}$, $(5, 6) = ca'\mathfrak{n}''$, $(5, 7) = ca''\mathfrak{n}'$, $(5, 8) = b'c\mathfrak{n}'' - b''c\mathfrak{n}'$, $(6, 7) = b''c\mathfrak{n}' - b'c\mathfrak{n}''$, $(6, 8) = cc''\mathfrak{n}'$, $(7, 8) = cc'\mathfrak{n}''$, quas per Φ designabimus, nouemque aliae: $(10)\ (11) - (9)\ (12) = an'\mathfrak{n}''\mathfrak{A}$, $(1)\ (12) -$

*) Horum signorum significatio praesens non est confundenda cum ea in qua in art. 234 accepta erant; nam numeri per haec signa *hic* expressi apprime respondent iis, qui in art. 234 per numeros similibus signis *illic* denotatos multiplicabantur.

$(2)(11) - (3)(10) + (4)(9) = 2an'n''\mathfrak{B}$, $(2)(3) - (1)(4) = an'n''\mathfrak{C}$, $-(9)(16) + (10)(15) + (11)(14) - (12)(13) = 2bn'n''\mathfrak{A}$, $(1)(16) - (2)(15) - (3)(14) + (4)(13) + (5)(12) - (6)(11) + (7)(10) + (8)(9) = 4bn'n''\mathfrak{B}$, $-(1)(8) + (2)(7) + (3)(6) - (4)(5) = 2bn'n''\mathfrak{C}$, $(14)(15) - (13)(16) = cn'n''\mathfrak{A}$, $(5)(16) - (6)(15) - (7)(14) + (8)(13) = 2cn'n''\mathfrak{B}$, $(6)(7) - (5)(8) = cn'n''\mathfrak{C}$, quas designabimus per Ψ *).

IV. Originem omnium harum 37 aequationum deducere nimis prolixum foret: sufficiet quasdam confirmauisse, ad quarum instar reliquae haud difficulter demonstrari poterunt.

1) Habetur $(1,2) = (1)(10) - (2)(9) = (pq' - qp')\,pp + (pq''' - qp''' - p'q'' + q'p'')\,pq + (p''q''' - q''p''')\,qq = n''(App + 2Bpq + Cqq) = n''aa'$, quae est aequ. prima.

2) Fit $(1,3) = (1)(11) - (3)(9) = (pq'' - qp'')(pq' - qp') = a''\mathfrak{N}an' = aa''\mathfrak{n}'$, aequ. secunda.

3) Erit $(1,8) = (1)(16) - (8)(9) = (pq' - qp')\,pp''' + (pq''' - qp''')\,pq''' - (p'q'' - q'p'')\,qp''' + (p''q''' - q''p''')\,qq''' = n''(App''' + B(pq''' + qp''') + Cqq''') + b''\mathfrak{N}(pq''' - qp''') = n''(bb' + \sqrt{dd'}) + b''\mathfrak{N}(bn + b'n')$ **)

*) Obseruare conuenit, 18 alias aequationes his Ψ similes erui posse, in quibus ad dextram loco factorum a, $2b$, c habeantur a', $2b'$, c'; a'', $2b''$, c'': sed has quum ad institutum nostrum non sint necessariae omittimus.

**) Hoc sequitur ex aequ. 10 art. 235 et sqq. Quantitas radicalis $\sqrt{dd'}$ fit $= Dnn' = \mathfrak{D}nn'\mathfrak{N}\mathfrak{N} = \mathfrak{D}nn'$.

$= n''bb' + n'bb'' + nb'b'' + \mathfrak{D}nn'n''$, aequatio octaua in Φ. Aequationes reliquas lectoribus confirmandas linquimus.

V. Ex aequatt. Φ sequitur, viginti octo numeros (1, 2), (1, 3) etc. nullum diuisorem communem habere, sequenti modo. Primo obseruamus, viginti septem producta e ternis factoribus, quorum primus vel n, secundus aliquis numerorum a', $2b'$, c', tertiusque aliquis numerorum a'', $2b''$, c''; vel primus n', secundus aliquis e numeris a, $2b$, c, tertius aliquis numerorum a'', $2b''$, c''; vel denique primus n'', secundus aliquis numerorum a, $2b$, c tertiusque aliquis e numeris a', $2b'$, c' — singula haec viginti septem producta propter aequatt. Φ aequalia esse vel alicui ex viginti octo numeris (1, 2), (1, 3) etc. vel plurium summae aut differentiae, (e. g. $na'a'' = (1, 5)$, $2na'b'' = (1, 6) + (2, 5)$, $4nb'b'' = (1, 8) + (2, 7) + (3, 6) + (4, 5)$, et sic de reliquis); quamobrem si hi numeri diuisorem communem haberent, hic necessario etiam omnia illa producta metiri deberet. Hinc vero facile deducitur adiumento art. 40 et per methodum saepius in praecedentibus adhibitam, eundem diuisorem etiam numeros $nm'm''$, $n'mm''$, $n''mm'$ metiri debere, adeoque horum quadrata quae sunt $\frac{dm'm'm''m''^2}{\mathfrak{D}}$, $\frac{d'mmm''m''}{\mathfrak{D}}$, $\frac{d''mmm'm'}{\mathfrak{D}}$ per illius quadratum diuisibilia esse, *Q. E. A.*, quoniam per I trium numeratorum diuisor communis maximus est $\mathfrak{D}$, adeoque quadrata ipsa diuisorem communem habere nequeunt.

VI. Haec omnia pertinent ad transformationem formae f in fff''; et ex transformationibus

formae F in ff' formaeque $\mathfrak{F}$ in Ff'' deducta sunt. Sed prorsus simili modo e transformationibus formae F' in ff'' formaeque $\mathfrak{F}$ in $F'f'$ deriuabitur transformatio formae $\mathfrak{F}'$ in $ff'f''$ talis: $\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' +$ etc., $\mathfrak{Y}' = (9)'xx'x'' + (10)'xx'y'' +$ etc. (designando omnes coefficientes similiter vt in transformatione formae $\mathfrak{F}$ in $ff'f''$, singulisque distinctionis caussa lineolam affigendo), ex qua perinde vt ante 28 aequationes ipsis Φ analogae deducentur, quas per Φ' designabimus, nouemque aliae ipsis Ψ analogae, quas exprimemus per Ψ'. Scilicet denotando $(1)'(10)' - (2)'(9)'$ per $(1, 2)'$, $(1)'(11)' - (3)'(9)'$ per $(1, 3)'$ etc., aequationes Φ' erunt $(1, 2)' = aa'\mathfrak{n}''$, $(1, 3)' = ab'\mathfrak{n}'' + ab''\mathfrak{n}'$ etc.; aequationes Ψ' autem $(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}'$ etc. (Euolutionem vberiorem breuitatis gratia lectoribus relinquimus; ceterum periti nouum calculum ne necessarium quidem esse, sed analysin primam per analogiam facile huc transferri posse inuenient). Quibus ita factis, ex Φ et Φ' statim sequitur $(1, 2) = (1, 2)'$, $(1, 3) = (1, 3)'$, $(1, 4) = (1, 4)'$, $(2, 3) = (2, 3)'$ etc.; hinc vero et inde quod omnes $(1, 2)$, $(1, 3)$, $(2, 3)$ etc. diuisorem communem (per V) non habent, adiumento lemmatis art. 234 concluditur, quatuor numeros integros α, $\mathfrak{C}$, γ, δ ita determinari posse, vt fiat $\alpha(1)' + \mathfrak{C}(9)' = (1)$, $\alpha(2)' + \mathfrak{C}(10)' = (2)$, $\alpha(3)' + \mathfrak{C}(11)' = (3)$ etc.; $\gamma(1)' + \delta(9)' = (9)$, $\gamma(2)' + \delta(10)' = (10)$ etc., atque $\alpha\delta - \mathfrak{C}\gamma = 1$.

VII. Hinc atque substituendo ex tribus aequatt. primis Ψ valores ipsorum $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$,

et ex tribus aequ. primis Ψ' valores ipsorum $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$ facile confirmatur fore $a(\mathfrak{A}_{\alpha\alpha} + 2\mathfrak{B}_{\alpha\gamma} + \mathfrak{C}_{\gamma\gamma}) = a\mathfrak{A}'$, $a(\mathfrak{A}_{\alpha\mathfrak{c}} + \mathfrak{B}(\alpha\delta + \mathfrak{c}\gamma) + \mathfrak{C}_{\gamma\delta}) = n\mathfrak{B}'$, $a(\mathfrak{A}_{\mathfrak{c}\mathfrak{c}} + 2\mathfrak{B}_{\mathfrak{c}\delta} + \mathfrak{C}\delta\delta) = a\mathfrak{C}'$, vnde, nisi $a = 0$, manifesto sequitur, formam $\mathfrak{F}$ transire in $\mathfrak{F}'$ per substitutionem propriam α, $\mathfrak{c}$, γ, δ. — Adhibendo autem loco trium aequationum primarum in Ψ et Ψ' tres sequentes, facile confirmabuntur tres aequationes modo traditis omnino similes, in quibus loco factoris a vbique inuenitur b; vnde patet, eandem conclusionem etiamnum valere si modo non sit $b = 0$. Denique adhibendo tres vltimas aequationes Ψ, Ψ' inuenietur eodem modo, conclusionem veram esse nisi $c = 0$. Quocirca, quum certo omnes a, b, c simul $= 0$ esse nequeant, necessario forma $\mathfrak{F}$ per subst. α, $\mathfrak{c}$, γ, δ transibit in $\mathfrak{F}'$, adeoque huic formae proprie aequiualebit. *Q. E. D.*

241. Talem formam vt $\mathfrak{F}$ vel $\mathfrak{F}'$, quae oritur, si vna trium formarum datarum componitur cum ea quae ex compositione duarum reliquarum resultat, *ex his tribus formas compositam* vocabimus, patetque ex art. praec., nihil hic interesse quonam ordine tres formae componantur. Simili modo propositis quotcunque formis f, f', f'', f''' etc. (quarum determinantes rationem quadratorum inter se habere debent), si forma f componitur cum f', resultans cum f'', quae hinc oritur cum f''' etc.: forma quae ad finem huius operationis prodit *ex omnibus formis* f, f', f'', f''' etc. composita dicetur. Facile vero demonstratur, etiam hic arbitrarium esse quonam ordine formae componantur; *i. e.* quocun-

que ordine hae formae componantur, formas ex compositione oriundas semper proprie aequiualentes esse. — Porro manifestum est, si formis f, f', f'' etc. proprie aequiualeant formae g, g', g'' etc. resp., formam compositam ex his proprie aequiualentem fore formae ex illis compositae.

242. Propositiones praecedentes formarum compositionem maxima vniuersalitate complectuntur; progredimur iam ad applicationes magis particulares, per quas illarum ordinem interrumpere noluimus. Ac primo quidem resumemus problema art. 236, quod per conditiones sequentes limitabimus: *primo* vt formae componendae eundem determinantem habeant, siue sit $d = d'$; *secundo* vt m, m' sint inter se primi; *tertio* vt forma quaesita directe ex vtraque f, f' composita sit. Hinc etiam mm, $m'm'$ inter se primi erunt; quare diuisor communis maximus numerorum $dm'm'$, $d'mm$ i. e. D fiet $= d = d'$, atque $n = n' = 1$. Quatuor quantitates $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, quae ad libitum assumi possunt, statuemus $= -1, 0, 0, 0$ resp., quod semper licebit vnico casu excepto vbi a, a', $b + b'$ simul sunt $= 0$, ad quem igitur hic non respiciemus; manifesto autem hic casus occurrere nequit nisi in formis determinantis positiui quadrati. Tunc patet, μ fieri diuisorem communem maximum numerorum a, a', $b + b'$; numeros $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ ita accipi debere vt fiat $\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$; ipsum $\mathfrak{P}$ vero omnino arbitrarium esse. Hinc prouenit, substituendo l. c. pro p, q, p', q' etc. valores suos: $A = \frac{aa'}{\mu\mu}$, $B =$

$\frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + p'''(bb' + D))$; C autem per aequationem $AC = BB - D$ poterit determinari, si modo non simul a et $a' = 0$.

In hac igitur solutione valor ipsius A non pendet a valoribus ipsorum $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (qui infinitis modis diuersis determinari possunt); B autem alios valores obtinebit tribuendo his numeris alios valores, operaeque pretium est inuestigare, quomodo omnes valores ipsius B inter se connexi sint. Ad hunc finem obseruamus

I. Quomodocunque determinentur $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, valores ipsius B inde prodeuntes omnes congruos esse secundum modulum A. Ponamus, si statuatur $\mathfrak{P} = \mathfrak{p}$, $\mathfrak{P}' = \mathfrak{p}'$, $\mathfrak{P}'' = \mathfrak{p}''$, $\mathfrak{P}''' = \mathfrak{p}'''$, fieri $B = \mathfrak{B}$; faciendo autem $\mathfrak{P} = \mathfrak{p} + \mathfrak{d}$, $\mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}'''$, prodire $B = \mathfrak{B} + \mathfrak{D}$. Tunc igitur erit $a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''' = 0$, $aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \mu\mathfrak{D}$. Multiplicando aequationis posterioris partem primam per $a\mathfrak{p}' + a'\mathfrak{p}'' + (b + b')\mathfrak{p}'''$ secundam per μ, et subtrahendo a producto primo quantitatem $(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (bb' + D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b)\mathfrak{d}''')$, quae propter aequationem priorem manifesto erit $= 0$, habebitur euolutione facta et sublatis quae se destruunt $aa'(\mu\mathfrak{d} + ((b' - b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' + ((b - b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' - (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}''') = \mu\mu\mathfrak{D}$, vnde manifesto $\mu\mu\mathfrak{D}$ per aa', siue $\mathfrak{D}$ per $\frac{aa'}{\mu\mu}$ i. e. per A diuisibilis erit, atque $\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D}$ (mod. A).

II. Si valores $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$ ipsorum $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ reddant $B = \mathfrak{B}$, inueniri posse alios valores horum numerorum ex quibus B nanciscatur valorem quemcunque datum ipsi $\mathfrak{B}$ secundum mod. A congruum, puta $\mathfrak{B} + kA$. Primo obseruamus, quatuor numeros μ, c, c', $b - b'$ diuisorem communem habere non posse; nam si quem haberent, hic metiretur sex numeros a, a', $b + b'$, c, c', $b - b'$ adeoque tum ipsos a, $2b$, c, tum ipsos a', $2b'$, c' et proin etiam ipsos m, m', qui per hyp. inter se sunt primi. Quamobrem quatuor numeri integri h, h', h'', h''' poterunt assignari tales vt fiat $h\mu + h'c + h''c' + h'''(b - b') = 1$. Quo facto si statuitur $kh = \mathfrak{d}$, $k(h''(b + b') - h'''a') = \mu\mathfrak{d}'$, $k(h'(b + b') + h'''a) = \mu\mathfrak{d}''$, $-k(h'a' + h''a) = \mu\mathfrak{d}'''$, patet, ipsos $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$, $\mathfrak{d}'''$ esse integros; porro facile confirmatur, fieri $a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''' = 0$, $aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \frac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b - b')h''') = \mu kA$. Ex aequatione priori patet, etiam $\mathfrak{p} + \mathfrak{d}$, $\mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{p}''' + \mathfrak{d}'''$ esse valores ipsorum $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$; ex posteriori, hos valores producere $B = \mathfrak{B} + kA$. *Q. E. D.* — Hinc perspicuum est, B semper ita determinari posse vt iaceat inter 0 et $A - 1$ incl., siquidem A est positiuus; vel inter 0 et $-A - 1$ si A negatiuus.

243. Ex aequationibus $\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$, $B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$ deducitur $B = b + \frac{a}{\mu}(\mathfrak{P}a' +$

$\mathfrak{P}'(b'-b) - \mathfrak{P}'''c) = b' + \frac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b - b') - \mathfrak{P}'''c')$; quare $B \equiv b \pmod{\frac{a}{\mu}}$ et $B \equiv b' \pmod{\frac{a'}{\mu}}$. Quoties $\frac{a}{\mu}$, $\frac{a'}{\mu}$ inter se primi sunt, inter 0 et $A - 1$ (siue inter 0 et $-A - 1$ quando A est negatiuus) vnicus tantum numerus iacebit qui secundum mod. $\frac{a}{\mu}$ sit $\equiv b$, et $\equiv b'$ sec. mod. $\frac{a'}{\mu}$; qui si statuitur $= \gamma$ atque $\frac{BB-D}{A} = C$, palam est, (A, B, C) e formis (a, b, c), (a', b', c') compositam fore. In hoc itaque casu ad inuentionem formae compositae ad numeros $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ non amplius oportet respicere. Ita e. g. si quaeritur forma e formis $(10, 3, 11)$, $(15, 2, 7)$ composita, erunt a, a', $b' + b'$ resp. $= 10, 15, 5$; $\mu = 5$; hinc $A = 6$; $B \equiv 3 \pmod{2.}$ et $\equiv 2 \pmod{3}$, vnde $B = 5$ atque $(6, 5, 21)$ forma quaesita. — Ceterum conditio vt $\frac{a}{\mu}$, $\frac{a'}{\mu}$ inter se primi sint omnino aequiualet huic vt numeri duo a, a' diuisorem communem maiorem non habeant quam tres a, a', $b + b'$, siue, quod eodem redit, vt diuisor communis maximus numerorum a, a' etiam numerum $b + b'$ metiatur. Notentur imprimis sequentes casus particulares:

1) Propositis duabus formis (a, b, c), (a', b', c') eiusdem determinantis D ita comparatis vt diuisor comm. max. numerorum a, $2b$, c primus sit ad diu. comm. max. num. a', $2b'$, c', atque a

primus ad a': forma ex his composita (A, B, C) inuenitur faciendo $A = aa'$, $B \equiv b \pmod{a}$ et $\equiv b' \pmod{a'}$, $C = \frac{BB - D}{A}$. Hic casus semper locum habet, quando altera formarum componendarum est forma principalis, puta $a = 1$, $b = 0$, $c = -D$. Tunc erit $A = a'$, B statui poterit $= b'$, vnde fiet $C = c'$; quare *ex forma principali et quacunque alia forma eiusdem determinantis composita est haec forma ipsa.*

2) Si duae formae *oppositae* proprie primitiuae sunt componendae, puta (a, b, c) et $(a, -b, c)$, erit $\mu = a$. Hinc facile perspicitur, formam principalem $(1, 0, -D)$ ex illis esse compositam.

3) Propositis quotcunque formis proprie primitiuis, (a, b, c), (a', b', c'), (a'', b'', c'') etc. eiusdem determinantis D, quarum termini antecedentes a, a', a'' etc. sunt numeri inter se primi, forma (A, B, C) ex illis omnibus composita inuenitur, statuendo A aequalem producto ex omnibus a, a', a'' etc.; B congruum ipsis b, b', b'' etc. secundum modulos a, a', a'' etc. resp.; $C = \frac{BB - D}{A}$. Facile enim perspicietur, ex duabus formis (a, b, c), (a', b', c') compositam fore formam $(aa', B, \frac{BB - D}{aa'})$; ex hac atque (a'', b'', c'') formam $(aa'a'', B, \frac{BB - D}{aa'a''})$ etc. — Vice versa

4) Proposita forma proprie primitiua (A, B, C) determinantis D, si terminus A in factores

quotcunque inter se primos a, a', a'' etc. resoluitur; numeri b, b', b'' etc. ipsi B vel aequales vel saltem sec. mod. a, a', a'' etc. resp. congrui accipiuntur, atque fit $ac = bb - D$, $a'c' = b'b' - D$, $a''c'' = b''b'' - D$ etc.: forma (A, B, C) composita erit e formis (a, b, c), (a', b', c'), (a'', b'', c''), siue *in has formas resolubilis*. Nullo negotio probatur, eandem propositionem adhucdum valere, etiamsi forma (A, B, C) sit improprie primitiua vel deriuata. Hoc itaque modo quaelibet forma in alias eiusdem determinantis resolui potest, quarum termini antecedentes omnes sint vel numeri primi vel numerorum primorum potestates. Talis resolutio saepenumero commode applicari potest, si ex pluribus formis datis componenda est vna. Ita e. g. si quaeritur forma composita e formis (3, 1, 234), (10, 3, 41), (15, 2, 27), resoluatur secunda in has (2, 1, 201), (5, — 2, 81), tertia in has (3, — 1, 134), (5, 2, 81), patetque, formam ex quinque formis (3, 1, 134), (2, 1, 201), (5, — 2, 81), (3, — 1, 134), (5, 2, 81) compositam, quocunque ordine accipiantur, etiam ex tribus datis compositam fore. At ex compositione primae cum quarta oritur forma principalis (1, 0, 401); eadem prouenit ex compositione tertiae cum quinta; quare ex compositione cunctarum conflatur forma (2, 1, 201).

5) Propter rei vtilitatem operae pretium est, hanc methodum adhuc amplius explicare. Ex obseruatione praecedente manifestum est, problema, quotcunque formas datas proprie primitiuas eiusdem determinantis componere, reduci posse ad compositionem formarum, quarum ter-

mini initiales sint potestates numerorum primorum (nam numerus primus tamquam sui ipsius potestas prima considerari potest). Quamobrem eum imprimis casum contemplari conuenit, vbi duae formae proprie primitiuae (a, b, c), (a', b', c') sunt componendae, in quibus a et a' sunt potestates *eiusdem* numeri primi. Sit itaque $a = h^\varkappa$, $a' = h^\lambda$ designante h numerum primum, supponamusque (quod licet), $\varkappa$ non esse minorem quam λ. Erit itaque h^λ diu. comm. max. numerorum a, a', qui si insuper ipsum $b + b'$ metitur, habebitur casus initio huius art. consideratus, eritque (A, B, C) ex propositis composita si statuitur $A = h^{\varkappa - \lambda}$, $B \equiv b \pmod{h^{\varkappa-\lambda}}$ et $\equiv b' \pmod 1$, quae conditio posterior manifesto omitti potest; $C = \frac{BB - D}{A}$. — Si vero h^λ ipsum $b + b'$ non metitur, necessario diu. comm. max. horum numerorum et ipse erit potestas ipsius h; sit igitur $= h^\nu$, eritque $\nu < \lambda$ (statui debet $\nu = 0$, si forte h et $b + b'$ inter se primi sunt). Si itaque $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ ita determinantur, vt fiat $\mathfrak{P}'h^\varkappa + \mathfrak{P}''h^\lambda + \mathfrak{P}'''(b + b') = h^\nu$, $\mathfrak{P}$ vero ad lubitum assumitur, forma (A, B, C) ex datis erit composita, si statuitur $A = h^{\varkappa + \lambda - 2\nu}$, $B = b + h^{\varkappa - \nu}(\mathfrak{P}h^\lambda + \mathfrak{P}'(b - b') - \mathfrak{P}'''c)$, $C = \frac{BB - D}{A}$. Sed facile perspicitur, in hoc casu etiam $\mathfrak{P}'$ ad libitum assumi posse, quare statuendo $\mathfrak{P} = \mathfrak{P}' = 0$, fit $B = b - \mathfrak{P}'''ch^{\varkappa-\nu}$ siue generaliter $B = kA + b - \mathfrak{P}'''ch^{\varkappa-\nu}$, designante k numerum arbitrarium (art. praec.). In hanc formulam simplicissimam

solus $\mathfrak{P}'''$ ingreditur, qui est valor expr. $\frac{h^\nu}{b+b'}$ (mod. h^λ). Si *e. g.* quaeritur forma composita ex (16, 3, 19) et (8, 1, 37), est $h = 2$, $\varkappa = 4$, $\lambda = 3$, $\nu = 2$. Hinc $A = 8$, $\mathfrak{P}'''$ valor expr. $\frac{4}{4}$ (mod. 8), qualis est 1, vnde $B = 8k - 73$, adeoque faciendo $k = 9$, $B = -1$ atque $C = 37$, siue (8, — 1, 37) forma quaesita.

Propositis itaque formis quotcunque, quarum termini initiales omnes sunt potestates numerorum primorum, circumspiciendum erit, num aliquarum termini antecedentes sint potestates *eiusdem* numeri primi, atque hae inter se respectiue per regulam modo traditam componendae. Hac ratione prodibunt formae, quarum termini primi etiamnum erunt potestates numerorum primorum, sed omnino diuersorum; forma itaque ex his composita per obseru. tertiam definiri poterit. *E. g.* propositis formis (3, 1, 47), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11), ex prima et quinta conflatur forma (27, 7, 7); ex secunda et quarta confit (16, — 6, 11), ex hac et sexta (1, 0, 140), quae negligi potest. Supersunt itaque (5, 0, 28), (27, 7, 7), ex quibus producitur (135, — 20, 4), cuius loco assumi potest proprie aequiualens (4, 0, 35). Haec itaque est resultans ex compositione sex propositarum.

Ceterum ex hoc fonte plura alia artificia in applicatione vtilia hauriri possunt; sed ne nimis

longi fiamus, vberiorem huius rei tractationem supprimimus, ad alia difficiliora properantes.

244. Si per formam aliquam f repraesentari potest numerus a, per formam f' numerus a', atque forma F in ff' est transformabilis: nullo negotio perspicitur, productum aa' per formam F repraesentabile fore. Hinc statim sequitur, quando determinantes harum formarum sint negatiui, formam F positiuam fore si vel vtraque f, f' sit positiua vel vtraque negatiua; contra F fieri negatiuam si altera formarum f, f' sit positiua altera negatiua. Subsistamus in eo imprimis casu, quem in art. praect. consideraüimus, vbi F ex f, f' composita est, atque f, f' et F eundem determinantem D habent. Supponamus insuper, repraesentationes numerorum a, a' per formas f, f' fieri per valores indeterminatarum inter se primos, atque priorem pertinere ad valorem b expressionis $\sqrt{D}$ (mod. a), posteriorem ad valorem b' expr. $\sqrt{D}$ (mod. a'), ponaturque $bb - D = ac$, $b'b' - D = a'c'$. Tunc per art. 168 formae (a, b, c), (a', b', c') proprie aequiualebunt formis f, f'; quare F etiam ex illis duabus formis composita erit. Sed ex iisdem formis composita erit forma (A, B, C), si, posito numerorum a, a', $b + b'$ diuisore communi maximo $= \mu$, statuitur $A = \frac{aa'}{\mu\mu}$, $B \equiv b$ et b' sec. modulos $\frac{a}{\mu}$, $\frac{a'}{\mu}$ resp., $AC = BB - D$; quare haec forma proprie aequiualebit formae F. Iam per formam $Axx + 2Bxy + Cyy$ repraesentatur numerus aa', faciendo $x = \mu$, $y = 0$, quorum valorum diuisor comm. max. est μ; quare aa'

etiam per formam F repraesentari poterit ita vt valores indeterminatarum habeant diuisorem communem maximum μ (art. 166). Quoties igitur euadit $\mu = 1$, aa' per formam F repraesentari poterit tribuendo indeterminatis valores inter se primos, repraesentatioque haec pertinebit ad valorem B expr. $\sqrt{D}$ (mod. aa'), ipsis b, b' secundum modulos a, a' resp. congruum. Conditio $\mu = 1$ semper locum habet, quando a, a' inter se primi sunt; generaliter autem, quando diu. comm. max. ipsorum a, a' ad $b + b'$ est primus.

245. Theorema. *Si forma f ad eundem ordinem referenda est vt g, similiterque f' est ex eodem ordine vt g': forma F ex f, f' composita eundem determinantem habebit ex eodemque ordine erit vt forma G ex g, g' composita.*

Dem. Sint formae $f, f', F = (a, b, c), (a', b', c'), (A, B, C)$ resp., ipsarumque determinantes $= d, d', D$. Porro sit numerorum $a, 2b, c$ diu. comm. max. $= m$; numerorum a, b, c diu. comm. max. $= \mathfrak{m}$; similesque significationes habeant m', $\mathfrak{m}'$ respectu formae f', et M, $\mathfrak{M}$ respectu formae F. Tunc ordo formae f determinabitur per numeros d, m, $\mathfrak{m}$, vnde iidem numeri etiam pro forma g valebunt; eadem ratione numeri d', m', $\mathfrak{m}'$ idem erunt pro forma g' quod sunt pro forma f'. Iam per art. 235, numeri D, M, $\mathfrak{M}$ determinati sunt per d, d', m, m', $\mathfrak{m}$, $\mathfrak{m}'$; scilicet erit D diuisor communis maximus ipsorum $dm'm'$, $d'mm$; $M = mm'$; atque $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (si simul $m = \mathfrak{m}$, $m' = \mathfrak{m}'$), vel $= 2\,\mathfrak{m}\mathfrak{m}'$ (si $m = 2\mathfrak{m}$, aut $m' = 2\mathfrak{m}'$). Quae

proprietates ipsorum D, M, $\mathfrak{M}$, quum inde sequantur, quod F ex f, f' composita est: facile perspicitur, D, M et $\mathfrak{M}$ etiam pro forma G valere, adeoque G esse ex eodem ordine vt F. *Q. E. D.*

Ex hac ratione ordinem in quo est forma F compositum dicemus ex ordinibus in quibus sunt formae f, f'. Ita e. g. ex duobus ordinibus proprie primitiuis semper compositus est similis ordo; ex proprie primitiuo et improprie primitiuo, improprie primitiuus. — Simili modo intelligendum est, si ordo aliquis ex pluribus aliis ordinibus compositus vocabitur.

246. Problema. *Propositis duabus formis primitiuis quibuscunque f, f', ex quarum compositione oritur F: ex generibus ad quae pertinent f, f' definire genus ad quod referenda erit F.*

Sol. I. Consideremus primo eum casum vbi ad minimum vna formarum f, f' *e. g.* prior est proprie primitiua, designemusque determinantes formarum f, f', F per d, d', D. Tunc D erit diuisor communis maximus numerorum $dm'm'$, d', vbi m' est aut 1 aut 2, prout forma f' est proprie aut improprie primitiua; F autem in casu illo pertinebit ad ordinem proprie primitiuum, in hoc ad improprie primitiuum. Iam genus formae F definietur per ipsius characteres particulares, nempe tum respectu singulorum diuisorum primorum imparium ipsius D, tum, pro quibusdam casibus, respectu numerorum 4 aut 8. Hos igitur singulos determinare oportebit.

1°. Si p est diuisor quicunque primus impar ipsius D, necessario etiam ipsos d, d' metietur, adeoque etiam inter characteres formarum f, f' occurrent ipsarum relationes ad p. Iam si per f repraesentari potest numerus a, per f' numerus a': productum aa' repraesentari poterit per F. Si itaque tum per f, tum per f' repraesentari possunt residua quadratica ipsius p (per p non diuisibilia), etiam per F residua quadratica ipsius p repraesentari poterunt, i. e. si vtraque f, f' habet characterem Rp, forma F eundem characterem habebit. Simili ratione F habebit characterem Rp, si vtraque f, f' habet characterem Np; contra F habebit char. Np, si altera formarum f, f' habet Rp, altera Np.

2°. Si in characterem integrum formae F ingreditur relatio ad numerum 4, talis relatio etiam in characteres formarum f, f' ingredi debet. Nam illud tunc tantummodo euenit, quando D est $\equiv 0$ aut $\equiv 3 \pmod 4$. Quando D per 4 est diuisibilis, etiam $dm'm'$ et d' per 4 diuisibiles erunt, vnde statim patet, f' non posse esse improprie primitiuam, adeoque esse $m' = 1$; hinc tum d tum d' per 4 diuisibiles erunt, et in vtriusque characterem ingredietur relatio ad 4. Quando $D \equiv 3 \pmod 4$, metietur D ipsos d, d'; quotientes erunt quadrata, adeoque etiam d, d' necessario vel $\equiv 0$ vel $\equiv 3 \pmod 4$, et inter characteres ipsarum f, f' relatio ad 4. Hinc eodem modo vt in (1°) sequitur, characterem formae F fore 1, 4, si vel vtraque f, f' habeat 1, 4 vel vtraque 3, 4; contra characterem formae F fore 3, 4, si altera formarum f, f' habeat 1, 4, altera 3, 4.

3°. Quando D per 8 est diuisibilis, etiam d' erit; hinc f' certo proprie primitiua, $m' = 1$ atque etiam d per 8 diuisibilis; quare inter characteres formae F aliquis e characteribus 1, 8; 3, 8; 5, 8; 7, 8 tunc tantum locum habere potest, si etiam in charactere tum formae f, tum formae f' talis relatio ad 8 adest. Facile autem confirmatur eodem modo vt ante, characterem formae F fore 1, 8, si f et f' respectu ipsius 8 eundem habeant; characterem formae F fore 3, 8, si altera formorum f, f' habeat 1, 8 altera 3, 8, vel altera 5, 8 altera 7, 8; F habere 5, 8, si f, f' habeant 1, 8 et 5, 8 vel 3, 8 et 7, 8; F habere 7, 8, si f et f' habeant vel 1, 8 et 7, 8, vel 3, 8 et 5, 8.

4°. Quando est $D \equiv 2 \pmod 8$, erit d' vel $\equiv 0$ vel $\equiv 2 \pmod 8$; hinc $m = 1$, adeoque etiam d vel $\equiv 0$ vel $\equiv 2 \pmod 8$; attamen vterque d, d' per 8 diuisibilis esse nequit, quoniam D est diuisor communis *maximus* ipsorum. Quare in eo tantum casu alteruter characterum 1 *et* 7, 8; 3 *et* 5, 8, formae D tribui debebit, vbi vel vtraque forma f, f' aliquem ex illis habet, vel altera aliquem ex illis, altera aliquem horum 1, 8; 3, 8; 5, 8; 7, 8. Hinc facile deducitur, characterem formae F determinari per tabulam sequentem, si character in margine positus pertineat ad alteram formarum f, f', ad alteram vero character in facie:

	1 *et* 7, 8 vel 1, 8 vel 7, 8	3 *et* 5, 8 vel 3, 8 vel 5, 8
1 *et* 7, 8	1 *et* 7, 8	3 *et* 5, 8
3 *et* 5, 8	3 *et* 5, 8	1 *et* 7, 8

5°. Eodem modo probatur, ipsi F tribui non posse alterutrum characterum 1 *et* 3, 8; 5 *et* 7, 8, nisi etiam aliquis ex iisdem saltem vni formarum f, f' competat, alterique vel aliquis ex iisdem, vel aliquis ex his 1, 8; 3, 8; 5, 8; 7, 8. Et quidem character formae F determinabitur per hanc tabulam, in cuius margine et facie sunt characteres formarum f, f'

	1 *et* 3, 8 vel 1, 8 vel 3, 8	5 *et* 7, 8 vel 5, 8 vel 7, 8
1 *et* 3, 8	1 *et* 3, 8	5 *et* 7, 8
5 *et* 7, 8	5 *et* 7, 8	1 *et* 3, 8

II. Si vtraque forma f, f' est improprie primitiua, erit D diuisor communis maximus numerorum $4d$, $4d$, siue $\frac{1}{4}D$ diu. comm. maximus numerorum d, d'. Hinc facile sequitur, tum d, tum d', tum $\frac{1}{4}D$ fore $\equiv 1 \pmod 4$. Ponendo autem $F = (A, B, C)$, diu. comm. max. numerorum A, B, C erit $= 2$, et diu. comm. max. numerorum $A, 2B, C$ erit 4. Quare F erit forma deriuata ex improprie primitiua $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, cuius determinans erit $\frac{1}{4}D$, et cuius genus determinabit genus formae F. Character autem illius formae, tamquam improprie primitiuae, relationes ad 4 vel 8 non implicabit, sed tantummodo relationes ad singulos diuisores primos impares ipsius $\frac{1}{4}D$. Iam quum omnes hi diuisores manifesto etiam ipsos d, d' metiantur, atque semissis cuiusuis producti duorum factorum, quorum alter per f alter per f' est repraesentabilis, per formam $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$ repraе-

sentari possit: facile perspicietur, characterem huius formae respectu cuiusuis numeri primi imparis p ipsum $\frac{1}{4}D$ metientis fore Rp, *tum* si fuerit $2Rp$ atque formae f, f' respectu ipsius p eundem characterem habeant, *tum* si fuerit $2Np$ atque characteres formarum f, f' respectu ipsius p oppositi; contra characterem illius formae fore Np, *tum* si f, f' habeant characteres aequales respectu ipsius p atque sit $2Np$, *tum* si f, f' habeant oppositos atque sit $2Rp$.

247. Ex solutione problematis praec. manifestum est, si g sit forma primitiua ex eodem ordine et genere vt f, nec non g' forma primitiua ex eodem ordine et genere vt f': formam ex g et g' compositam ad idem genus pertinere ad quod pertineat forma ex f et f' composita. Hinc sponte sequitur significatio *generis* ex duobus aliis generibus (siue etiam pluribus) *compositi*. Porro ibinde patet, si f, f' eundem determinantem habeant atque f sit forma e genere principali, F vero ex f et f' composita: F fore ex eodem genere vt f'; quocirca genus principale in compositione cum aliis generibus eiusdem determinantis semper omitti poterit. Si vero reliquis manentibus f non est e genere principali, f' autem forma primitiua: F certo erit ex alio genere quam f'. Denique si f, f' sunt formae proprie primitiuae eiusdem generis, F erit e genere principali; si vero f, f' sunt ambae proprie primitiuae eiusdem determinantis, sed e diuersis generibus, F ad genus principale pertinere non poterit. Quodsi itaque forma quaecunque proprie primitiua *cum se ipsa* componitur, forma

inde resultans, quae etiam proprie primitiua eiusdemque determinantis erit, necessario ad genus principale pertinebit.

248. Problema. *Propositis duabus formis quibuscunque f, f', e quibus composita est F: e generibus formarum f, f' definire genus formae F.*

Sol. Sit $f = (a, b, c)$, $f' = (a', b', c')$, $F = (A, B, C)$, porro $\mathfrak{m}$ diu. comm. max. numerorum a, b, c, atque $\mathfrak{m}'$ diu. comm. max. numerorum a', b', c', ita vt f, f' sint deriuatae e primitiuis $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$, $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$, quas denotabimus per $\mathfrak{f}$, $\mathfrak{f}'$ resp. Iam si saltem vna formarum $\mathfrak{f}$, $\mathfrak{f}'$ est proprie primitiua, diuisor comm. max numerorum A, B, C erit $\mathfrak{m}\mathfrak{m}'$, adeoque F deriuata e forma primitiua $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'})$ ... $\mathfrak{F}$, vnde patet, genus formae F pendere a genere formae $\mathfrak{F}$. Sed facile perspicietur, $\mathfrak{F}$ per eandem substitutionem transire in $\mathfrak{f}\mathfrak{f}'$, per quam F transeat in ff' adeoque $\mathfrak{F}$ ex $\mathfrak{f}$, $\mathfrak{f}'$ esse compositam, ipsiusque genus per problema art. 246 determinari posse. — Si vero vtraque $\mathfrak{f}$, $\mathfrak{f}'$ est improprie primitiua, diuisor c. m. numerorum A, B, C erit $2\mathfrak{m}\mathfrak{m}'$, formaque $\mathfrak{F}$ etiamnum ex $\mathfrak{f}$, $\mathfrak{f}'$ composita et manifesto e proprie primitiua $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$ deriuata. Huius itaque formae genus determinari poterit per art. 246; et quum F ex eadem forma deriuata sit, ipsius genus hinc sponte innotescit.

Ex hac solutione manifestum est, theorema in art. praec. pro formis primitiuis explicatum, scilicet *si f', g' sint ex iisdem generibus resp.*

vt f, g, formam ex eodem genere fore ex quo sit forma ex f, g composita, generaliter pro formis quibuscunque valere.

249. THEOREMA. *Si formae f, f' sunt ex iisdem ordinibus generibus et classibus vt g, g' resp.: forma ex f et f' composita ex eadem classe erit vt forma ex g et g' composita.*

Ex hoc theoremate (cuius veritas ex art. 239 protinus sequitur) sponte patebit significatio *classis e duabus classibus datis* siue etiam *e pluribus compositae.*

Si classis quaecunque K cum classe principali componitur, classis K ipsa prodibit, siue classis principalis in compositione cum aliis classibus eiusdem determinantis negligi potest. Ex compositione duarum classium oppositarum proprie primitiuarum semper oritur classis principalis eiusdem determinantis (v. art. 243). Quum itaque quaeuis classis anceps sibi ipsa opposita sit: ex compositione cuiusuis classis ancipitis proprie primitiuae cum se ipsa classis principalis eiusdem determinantis prouenit.

Propositio vltima etiam conuersa valet: scilicet *si ex compositione classis proprie primitiuae K cum se ipsa prouenit classis principalis H eiusdem determinantis, K necessario erit classis anceps.* Si enim K' est classis opposita ipsi K, e tribus classibus K, K, K' composita erit eadem classis quae oritur ex H et K'; ex illis prouenit K (quoniam K et K' producunt H, haec cum K ipsam K), ex his K'; quare K cum K' coincidet eritque adeo classis anceps.

Porro notetur propositio haec: *Si classes K, L oppositae sunt classibus K', et L' resp.: classis ex K, et L composita classi ex K' et L' compositae erit opposita.* Sint formae f, g, f', g' resp. e classibus K, L, K', L'; forma F composita ex f, g, atque F' composita ex f', g'. Quum f' ipsi f, atque g' ipsi g improprie aequiualeant, F autem composita sit ex vtraque f, g directe: F etiam ex f', g' composita erit, sed ex vtraque inuerse. Quare forma quaecunque, quae ipsi F improprie aequiualet, composita erit ex f', g' directe, adeoque ipsi F' proprie aequiualebit (artt. 238, 239), vnde F, G improprie aequiualebunt, classesque ad quas pertinent oppositae erunt.

Hinc sequitur, si classis anceps K cum classe ancipite L componatur, semper prodire classem ancipitem. Nam opposita erit classi, quae composita est e classibus ipsis K, L oppositis, adeoque sibi ipsi, quoniam hae classes sibi ipsae sunt oppositae.

Denique obseruamus, si propositae sint classes duae quaecunque K, L eiusdem determinantis, quarum prior sit proprie primitiua, semper inueniri posse classem M eiusdem determinantis, ex qua atque K composita sit L. Manifesto hoc obtinetur, accipiendo pro M classem quae composita est ex L atque classe ipsi K opposita; simul perspicietur facillime, hanc classem esse vnicam quae hac proprietate sit praedita, siue classes diuersas eiusdem det. cum eadem classe pr. prim. compositas producere classes diuersas.

Classium compositio commode per signum additionis, $+$, denotari potest, sicuti classium

identitas per signum aequalitatis. In his signis propositio modo tradita exhiberi potest ita: Si K' est classis opposita ipsi K, erit $K + K'$ classis principalis eiusdem determinantis, vndo $K + K' + L = L$; posita itaque $K' + L = M$, erit $K + M = L$, vti desiderabatur; si vero praeter M alia M' daretur, eadem proprietate praedita, siue $K + M' = L$, foret $K + K' + M' = L + K' = M$, vnde $M' = M$. — Si plures classes identicae componuntur, hoc (ad instar multiplicationis) denotari potest praefigendo ipsarum numerum, ita vt $2K$ idem designet vt $K + K$, $3K$ idem vt $K + K + K$ etc. Eadem signa etiam ad formas transferri possent, ita vt $(a + b + c) + (a' + b' + c')$ designaret formam ex $(a + b + c)$, $(a' + b' + c')$ compositam: sed ne vel species ambiguitatis oriri possit, hac abbreuiatione abstinere malumus, praesertim quod tali signo $\sqrt{M}(a, b, c)$ significationem peculiarem iam tribuimus. — Classem $2K$ ex *duplicatione* classis K oriri dicemus, classem $3K$ ex *triplicatione* etc.

250. Si D est numerus per mm diuisibilis (vbi ipsum m positiuum supponimus): dabitur ordo formarum determinantis D ex ordine proprie primitiuo determinantis $\frac{D}{mm}$ deriuatus (siue *duo*, quando D est negatiuus, nempe positiuus et negatiuus); manifesto forma $(m, o, -\frac{D}{m})$ ad illum ordinem pertinebit (scilicet ad positiuum) meritoque tamquam *forma simplicissima* in eo considerari potest (sicuti $(-m, o, \frac{D}{m})$ erit simplicissima in ordine negatiuo quando D neg.).

Si insuper est $\frac{D}{mm} \equiv 1 \pmod 4$, dabitur etiam ordo formarum det. D ex improprie primitiuo det. $\frac{D}{mm}$ deriuatus, ad quem manifesto forma $(2m, m, \frac{mm - D}{2m})$ pertinebit et pro simplicissima in eodem habebitur. (Quando D est neg., rursus duo ordines dabuntur et in negatiuo forma $(-2m, -m, \frac{D - mm}{2m})$ pro simplicissima habebitur). Ita e. g., si etiam eum casum vbi $m = 1$ huc referre lubet, in quatuor ordinibus formarum det. 45 sequentes erunt simplicissimae $(1, 0, -45)$, $(2, 1, -22)$, $(3, 0, -15)$, $(6, 3, -6)$. Quibus ita intellectis, offert se

Problema. *Proposita forma quacunque F ex ordine O, inuenire formam proprie primitiuam (positiuam) eiusdem determinantis, ex cuius compositione cum forma in O simplicissima oriatur F.*

Sol. Sit forma $F = (ma, mb, mc)$ deriuata e primitiua $f = (a, b, c)$ cuius determinans $= d$, supponamusque *primo*, f esse proprie primitiuam. Primo obseruamus, si forte a ad $2dm$ non sit primus, certo dari alias formas ipsi (a, b, c) proprie aequiualentes, quarum termini primi hac proprietate sint praediti. Nam per art. 228 dantur numeri ad $2dm$ primi per formam illam repraesentabiles; sit talis numerus $a' = \alpha\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$, supponamusque, (quod licet), α, γ esse inter se primos; tum, acceptis $\mathfrak{G}, \delta$ ita vt fiat $\alpha\delta - \mathfrak{G}\gamma = 1$, transeat f per substitutionem $\alpha, \mathfrak{G}, \gamma, \delta$ in formam (a', b', c'), quae illi pro-

prie aequiualebit et proprietate praescripta erit praedita. Iam quum etiam F et $(a'm, b'm, c'm)$ proprie aequiualeant, facile perspicietur, sufficere eum casum considerare vbi a ad $2dm$ sit primus. Tunc (a, bm, cmm) erit forma proprie primitiua (si enim a, $2bm$, cmm diuisorem communem haberent, hunc etiam $2dm = 2bbm - 2acm$ implicaret) eiusdem determinantis vt F, confirmaturque facile, F transmutari in productum e forma $(m, 0, -dm)$, quae, nisi F est forma negatiua, erit simplicissima ordinis O, in (a, bm, cmm) per substitutionem $1, 0, -b; -cm$; $0, m, a, bm$, vnde per criterium in obs. 4. art. 235 concluditur, F ex $(m, 0, -dm)$ et (a, bm, cmm) esse compositam. Quando autem F est forma negatiua, transibit in productum e forma simplicissima eiusdem ordinis $(-m, 0, dm)$ in positiuam $(-a, bm, -cmm)$ per substitutionem $1, 0, b, -cm$; $0, -m, -a, bm$, adeoque ex ipsis erit composita.

Secundo, si f est forma improprie primitiua, supponere licebit $\frac{1}{2}a$ ad $2dm$ esse primum; si enim haec proprietas in forma f locum nondum habet, inueniri potest forma ipsi f proprie aequiualens et hac proprietate praedita. Hinc autem sequitur facile, $(\frac{1}{2}a, bm, 2cmm)$ esse formam proprie primitiuam eiusdem determinantis vt F; aeque facile confirmatur, F transire in productum e formis $(\pm 2m, \pm m \pm \frac{1}{2}(m - dm))$, $(\pm \frac{1}{2}a, bm, \pm 2cmm)$ per substitutionem $1, 0, \frac{1}{2}(1 \mp b), -cm$; $0, \pm 2m, \pm \frac{1}{2}a, (b \pm 1)m$, vbi signa inferiora accipienda sunt quando F est forma negatiua, superiora in casibus reliquis, adeo-

que ex his duabus formis esse compositam, quarum prior erit simplicissima ordinis O, posterior forma proprie primitiua (positiua).

251. Problema. *Propositis duabus formis F, f eiusdem determinantis D et ad eundem ordinem O pertinentibus: inuenire formam proprie primitiuam determinantis D, quae cum f composita producat F.*

Sol. Sit φ forma simplicissima ordinis O; $\mathfrak{F}$, $\mathfrak{f}$ formae proprie primitiuae det. D, quae cum φ compositae producant ipsas F, f resp.; denique f' forma proprie primitiua quae cum $\mathfrak{f}$ composita producat $\mathfrak{F}$. Tunc forma F composita erit e tribus formis φ, $\mathfrak{f}$, f', siue e duabus f, f'. *Q. E. I.*

Quaeuis itaque classis ordinis dati considerari potest tamquam composita ex quacunque classe data eiusdem ordinis et aliqua classe proprie primitiua eiusdem determinantis.

252. Theorema. *Pro determinante dato in singulis generibus eiusdem ordinis contentae sunt classes aeque multae.*

Dem. Pertineant genera G et H ad eundem ordinem, constet G ex n classibus K, K', K'' ... K^{n-1}, sitque L classis aliqua e genere H. Inuestigetur per art. praec. classis proprie primitiua M eiusdem determinantis, ex cuius compositione cum K prodeat L, designenturque classes quae oriuntur ex compositione classis M cum K', K'' ... K^{n-1} resp. per L', L'' ... L^{n-1}. Tunc ex

obs. vltima art. 249 sequitur, omnes classes L, L', $L'' \dots L^{n-1}$ esse diuersas, et per art. 248 omnes pertinebunt ad genus idem, i. e. ad genus H. Denique perspicietur facile, H alias classes praeter has continere non posse, quum quaeuis classis generis H tamquam composita considerari possit ex M et alia classe eiusdem determinantis quae necessario semper erit e genere G. Quocirca H perinde vt G continet n classes diuersas. *Q. E. D.*

253. Theorema praecedens supponit ordinis identitatem neque ad ordines diuersos est extendendum. Ita e. g. pro determinante — 171 dantur 20 classes positiuae, quae reducuntur ad quatuor ordines: in ordine proprie primitiuo duo continentur genera, vtrumque sex classes complectitur; in ordine impr. primitiuo duo genera quatuor classes possident, singula binas; in ordine deriuato ex O. proprie prim. det. — 19 vnicum est genus quatuor classes complectens; denique O. deriuatus ex impr. prim. det. — 19 vnicum genus habet ex vna classe constans; perinde se habent classes negatiuae. Operae itaque pretium est, in principium generale inquirere, a quo nexus inter multitudines classium in diuersis ordinibus pendeat. Supponamus, K, L esse duas classes ex eodem ordine (positiuo) O determinantis D, atque M classem proprie primitiuam eiusdem det., ex cuius compositione cum K oriatur L, qualis per art. 251 semper potest assignari. Iam in quibusdam casibus fieri potest, vt M sit *vnica* classis pr. primitiua quae cum K composita producat L; in aliis plures classes diuersae pr. primitiuae exstare pos-

sunt hac proprietate praeditae. Supponamus generaliter, dari r huiusmodi classes pr. primitiuas, M, M', M'' ... $M^{(r-1)}$, quae singulae cum K compositae producant eandem classem L, designemusque illarum complexum per $\mathfrak{M}$. Porro sit L' alia classis ordinis O (a classe L diuersa), atque N' classis pr. prim. det. D quae cum L composita efficiat L', designeturque complexus classium $N' + M$, $N' + M'$, $N' + M''$ ... $N' + M^{(r-1)}$ (quae omnes erunt proprie primitiuae et inter se diuersae) per $\mathfrak{M}'$. Tunc perspicietur facile, K cum classe quacunque ex $\mathfrak{M}$ compositam producere L', vnde concluditur, $\mathfrak{M}$ et $\mathfrak{M}'$ nullam classem communem habere; praeterea nullo negotio comprobatur, nullam classem pr. primitiuam in complexu $\mathfrak{M}'$ non contentam dari, quae cum K composita producat ipsam L'. Eodem modo patet, si L'' sit alia classis ordinis O a classibus L, L' diuersa, dari r formas pr. primitiuas tum inter se tum a formis $\mathfrak{M}$, $\mathfrak{M}'$ diuersas, quae singulae cum K compositae ipsam L'' producant, et perinde res se habebit pro omnibus reliquis classibus ordinis O. Quoniam vero quaeuis classis pr. prim. (positiua) determinantis D cum K composita classem ordinis O producit, facile hinc colligitur, si multitudo omnium classium ordinis O sit n, multitudinem omnium classium proprie primitiuarum (positiuarum) eiusdem determinantis fore rn. Habemus itaque regulam generalem: Denotantibus K, L classes quascunque ordinis O, atque r multitudinem classium proprie primitiuarum diuersarum eiusdem determinantis, quae singulae cum K compositae ipsam L producunt, multitudo omnium classium in ordine proprie

primitiuo (positiuo) r vicibus maior erit quam multitudo classium ordinis O.

Quum classes K, L in ordine O omnino ad libitum assumi possint, etiam classes identicas accipere licebit, et quidem e re erit ea classe vti, in qua continetur forma huius ordinis simplicissima. Quam itaque pro K et L assumendo, res eo reducta et, vt omnes classes proprie primitiuae assignentur, quae cum K compositae ipsam K reproducant. Huc via sternitur per sequens

254. Theorema. *Si* $F = (A, B, C)$ *est forma simplicissima ordinis* O *determinantis* D, *atque* $f = (a, b, c)$ *forma proprie primitiua eiusdem determinantis: per hanc formam* f *repraesentari poterit numerus* AA, *si* F *oritur per compositionem formarum* f, F; *et vice versa* F *ex se ipsa atque* f *composita erit, si* AA *per* f *repraesentari potest.*

Dem. I. Si F in productum fF transit per substitutionem p, p', p'', p'''; q, q', q'', q'''; ex art. 235 habemus $A\,(aq''q'' - 2bqq'' + cqq) = A^3$, vnde $AA = aq''q'' - 2bqq'' + cqq$. *Q. E. P.*

II. Si *supponitur*, A per f repraesentari posse, designentur valores indeterminatarum per quos hoc efficitur per q'', $-q$, siue sit $AA = aq''q'' - 2bqq'' + cqq$, ponaturque $q''a - q(b+B) = Ap$, $-qC = Ap'$, $q''(b-B) - qc = Ap''$, $-q''C = Ap'''$, $q''a - q(b-B) = Aq'$, $q''(b+B) - qc = Aq'''$. Quo facto, facile confirmatur, F

transire in productum fF per substitutionem p, p', p'', p'''; q, q', q'', q''', atque adeo ex f et F compositam esse, si modo omnes numeri p, p' etc. sint integri. Iam per descriptionem formae simplicissimae, A est vel o vel $\frac{1}{2}B$, adeoque $\frac{2B}{A}$ integer; ibinde patet, $\frac{C}{A}$ semper esse integrum. Hinc $q' - p$, p', $q''' - p''$, p''' erunt integri, superestque adeo tantummodo, vt probetur p et p'' esse integros. Fit autem $pp + \frac{2pqB}{A} = a$, $p''p'' + \frac{2p''q''B}{A} = c$; quamobrem si $B = 0$, fit $pp = a$, $p''p'' = c$, et proin p, p'' integri; si vero $B = \frac{1}{2}A$, fit $pp + pq = a$, $p''p'' + p''q'' = c$, vnde aeque facile concluditur, p et p'' in hoc quoque casu esse integros. Ex his colligitur, F ex f et F esse compositam. *Q. E. S.*

255. Problema itaque eo reductum est, vt omnes classes proprie primitiuas determinantis D assignare oporteat, per quarum formas repraesentari potest AA. Manifesto AA repraesentari potest per quamuis formam cuius terminus primus est vel AA vel quadratum partis aliquotae ipsius A; vice versa autem, si AA repraesentari potest per formam f, tribuendo ipsius indeterminatis valores αe, γe quorum diuisor communis maximus e, forma f per substitutionem α, $\mathfrak{C}$, γ, $\mathfrak{d}$ transibit in formam cuius terminus primus $\frac{A}{ee}$, formaque haec proprie aequiualebit formae f, si $\mathfrak{C}$, $\mathfrak{d}$ ita accipiuntur vt fiat $\alpha\mathfrak{d} - \mathfrak{C}\gamma = 1$; vnde

patet, in quauis classe, per cuius formas repraesentari possit AA, inueniri formas, quarum terminus primus sit AA vel quadratum partis aliquotae ipsius A. Res itaque in eo versatur, vt omnes classes proprie primitiuae det. D eruantur, in quibus huiusmodi formae occurrant, quod obtinetur sequenti modo: Sint a, a', a'' etc. omnes diuisores (positiui) ipsius A; inuestigentur omnes valores expr. $\sqrt{D}$ (mod. aa) inter o et $aa - 1$ incl. siti, qui sint b, b', b'' etc. statuaturque $bb - D = aac$, $b'b' - D = aac'$, $b''b'' - D = aac''$ etc.; complexus formarum (aa, b, c), (aa, b', c') etc. designetur per V. Tunc facile perspicitur, in quauis classe det. D, in qua occurrat forma cuius terminus primus aa, etiam aliquam formam ex V contentam esse debere. Simili modo eruantur omnes formae det. D, quarum terminus primus $a'a'$, medius inter o et $a'a' - 1$ incl. situs, designeturque ipsarum complexus per V'; eademque ratione sit V'' complexus similium formarum quarum terminus primus $a''a''$ etc. Eiiciantur ex V, V', V'' etc. omnes formae quae non sunt proprie primitiuae, reducantur reliquae in classes, et, si forte plures adsint ad eandem classem pertinentes, in singulis classibus vna tantum retineatur. Hoc modo omnes classes quaesitae habebuntur, eritque harum multitudo ad vnitatem, vt multitudo omnium classium proprie primitiuarum (positiuarum) ad multitudinem classium in ordine O.

Ex. Sit $D = -531$, atque O ordo positiuus deriuatus ex ordine improprie primitiuo det. -59, in quo forma simplicissima $(6, 3, 90)$

siue $A = 6$. Hic a, a', a'', a''' erunt 1, 2, 3, 6; V continebit formam (1, 0, 531); V' has (4, 1, 133), (4, 3, 135); V'' has (9, 0, 59), (9, 3, 60), (9, 6, 63); denique V''' has (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35), (36, 33, 45): sed ex his duodecim formis sex sunt reiiciendae, puta ex V'' secunda et tertia, ex V''' prima, tertia, quarta et sexta, quae omnes sunt formae deriuatae; sex reliquae omnes ad classes diuersas pertinere inueniuntur. Reuera multitudo classium proprie primitiuarum (positiuarum) det. — 531 est 18, multitudoque classium impr. primitiuarum (pos.) det. — 59 (siue multitudo classium det. — 531 ex his deriuatarum) 3, adeoque illa ad hanc vt 6 ad 1.

256. Solutio haec per obseruationes sequentes generales adhuc magis illustrabitur.

I. Si ordo O est deriuatus ex ordine proprie primitiuo, metietur AA ipsum D; si vero O est impr. primitiuus vel ex impr. prim. deriuatus, erit A par, D per $\frac{1}{4}AA$ diuisibilis et quotiens $\equiv 1 \pmod 4$. Hinc quadratum cuiusuis diuisoris ipsius A metietur vel ipsum D, vel saltem ipsum $4D$, et in casu posteriori quotiens semper erit $\equiv 1 \pmod 4$.

II. Si aa ipsum D metitur, omnes valores expr. $\sqrt{D} \pmod{aa}$, qui quidem inter 0 et $aa - 1$ iacent, erunt $0, a, 2a \ldots aa - a$, adeoque a multitudo formarum in V; sed inter has tot tantummodo erunt proprie primitiuae, quot numerorum $\frac{D}{aa}, \frac{D}{aa} - 1, \frac{D}{aa} - 4 \ldots \frac{D}{aa} - (a-1)^2$

cum a diuisorem communem non habent. Quando $a = 1$, V ex vnica forma constabit, $(1, 0, -D)$, quae semper erit proprie primitiua. Quando a est 2 vel potestas quaecunque ipsius 2, semissis illorum a numerorum par erunt, semissis impar; quare in V aderunt $\frac{1}{2}a$ formae proprie primitiuae. Quando a est alius numerus primus p vel potestas numeri primi p, tres casus sunt distinguendi: scilicet, omnes illi a numeri ad a primi erunt, adeoque omnes formae in V pr. primitiuae, si $\frac{D}{aa}$ per p non est diuisibilis simulque non residuum quadraticum ipsius p; si vero p ipsum $\frac{D}{aa}$ metitur, in V erunt $\frac{(p-1)a}{p}$ formae pr. primitiuae; denique si $\frac{D}{aa}$ est res. quadr. ipsius p per p non diuisibile, in V erunt $\frac{(p-2)a}{p}$ formae pr. primitiuae. Haec omnia nullo negotio demonstrantur. Generaliter autem posito $a = 2^\nu p^\pi q^\chi r^\varrho \ldots$, designantibus p, q, r etc. numeros primos impares diuersos, multitudo formarum pr. primitiuarum in V erit $NPQR\ldots$, vbi statui debet $N = 1$ (si $\nu = 0$) vel $N = 2^{\nu-1}$ (si $\nu > 0$); $P = p^\pi$ (si $\frac{D}{aa}$ est non residuum quadr. ipsius p) vel $P = (p-1)\, p^{\pi-1}$ (si $\frac{D}{aa}$ per p est diuisibilis) vel $P = (p-2)\, p^{\pi-1}$ (si $\frac{D}{aa}$ est res. qu. ipsius p per p non diuisibile); Q, R etc. autem eodem modo ex q, r etc. sunt definiendi vt P ex p.

III. Si aa ipsum D non metitur, erit $\frac{4D}{aa}$ integer et $\equiv 1 \pmod 4$, valoresque expr. $\sqrt{D} \pmod{aa}$ hi $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a \ldots aa - \frac{1}{2}a$, vnde multitudo formarum in V erit a, tot autem inter ipsas erunt proprie primitiuae quot ex numeris $\frac{D}{aa} - \frac{1}{4}, \frac{D}{aa} - \frac{9}{4}, \frac{D}{aa} - \frac{25}{4} \ldots \frac{D}{aa} - (a - \frac{1}{2})^2$ ad a sunt primi. Quoties $\frac{4D}{aa} \equiv 1 \pmod 8$, omnes hi numeri erunt pares, adeoque in V nulla forma pr. primitiua; quando autem $\frac{4D}{aa} \equiv 5 \pmod 8$, omnes illi numeri erunt impares, adeoque omnes formae in V pr. primitiuae, si a est 2 vel potestas ipsius 2, generaliter autem in hoc casu tot formae pr. primitiuae in V erunt, quot illorum numerorum per nullum diuisorem primum imparem ipsius a sunt diuisibiles. Multitudo haec erit $NPQR \ldots$, si $a = 2^\nu p^\pi q^\chi r^\varrho \ldots$, vbi statuere oportet $N = 2^\nu$, ipsos P, Q, R etc. autem eodem modo ex p, q, r etc. deriuare vt in casu praecedente.

IV. Hoc itaque modo multitudines formarum pr. primitiuarum in V, V', V'' etc. definiri possunt; pro aggregato omnium harum multitudinum haud difficulter eruitur sequens regula generalis: Si $A = 2^\varrho \mathfrak{A}^\alpha \mathfrak{B}^\beta \mathfrak{C}^\gamma \ldots$, designantibus $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. numeros primos impares diuersos, multitudo totalis omnium formarum pr. primitiuarum in V, V', V'' etc. erit $= Anabc \ldots$, vbi statui debet $n = 1$ (tum si $\nu = 0$, tum si $\frac{4D}{AA}$

$\equiv 1$, mod. 8), vel $n = 2$ (si $\nu > 0$ simulque $\frac{D}{AA}$ integer), vel $n = 3$ (si $\nu > 0$ simulque $\frac{4D}{AA} \equiv 5$, mod. 8); porro $a = \mathfrak{A}$ (si $\mathfrak{A}$ ipsum $\frac{4D}{AA}$ metitur), vel $a = \mathfrak{A} \pm 1$ (si $\mathfrak{A}$ ipsum $\frac{4D}{AA}$ non metitur, accipiendo signum superius vel inferius prout $\frac{4D}{AA}$ est non- residuum vel res. qu. ipsius $\mathfrak{A}$), denique b, c etc. eodem modo ex $\mathfrak{B}$, $\mathfrak{C}$ deriuari vt a ex $\mathfrak{A}$. Demonstrationem fusius hic explicare, breuitas non permittit.

V. Iam quod attinet ad multitudinem classium, quas suppeditant formae pr. primitiuae in V, V', V'' etc., tres casus sequentes sunt distinguendi.

Primo, quando D est numerus negatiuus, singulae formae pr. primitiuae in V, V' etc. constituent classem peculiarem, siue multitudo ipsa classium quaesitarum exprimetur per formulam in obseru. praec. traditam, duobus casibus exceptis, scilicet vbi $\frac{4D}{AA}$ vel $= -4$ vel $= -3$, siue vbi D vel $= -AA$ vel $= -\frac{3}{4}AA$. Ad demonstrationem huius theorematis manifesto ostendi tantummodo debet, fieri non posse, vt duae formae diuersae ex V, V', V'' etc. sint proprie aequiualentes. Supponamus itaque, (hh, i, k), $(h'h', i', k')$ esse duas formas diuersas pr. primitiuas ex V, V', V'' etc. ad eandem classem pertinentes, transeatque prior in posteriorem per substitutionem propriam $\alpha, \mathfrak{G}, \gamma, \delta$; vnde habe-

buntur aequationes $\alpha\delta - \beta\gamma = 1$, $hh\alpha\alpha + 2i\alpha\gamma + k\gamma\gamma = h'h'$, $hh\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i'$. Hinc facile concluditur, *primo* γ certo non esse $= 0$ (vnde sequeretur, esse $\alpha = \pm 1$, $hh = h'h'$, $i' \equiv i \pmod{hh}$ adeoque formas propositas identicas, contra hyp.); *secundo*, γ diuisibilem esse per diuisorem maximum communem numerorum h, h'; (ponendo enim hunc diuisorem $= r$, hic manifesto etiam metietur ipsos $2i$, $2i'$, ad k vero erit primus; praeterea rr metietur ipsum $hhk - h'h'k' = ii - i'i'$; vnde facile deducitur, r etiam metiri ipsum $i - i'$; habetur autem $\alpha i' - \beta h'h' = \alpha i + \gamma k$, vnde γk et proin etiam γ diuisibilis erit per r); *tertio*, esse $(\alpha hh + \gamma i)^2 - D\gamma\gamma = hhh'h'$. Ponendo itaque $\alpha hh + \gamma i = rp$, $\gamma = rq$, p et q erunt integri quorum posterior non $= 0$, atque $pp - Dqq = \frac{hhh'h'}{rr}$. Sed $\frac{hhh'h'}{rr}$ erit numerus minimus per hh et $h'h'$ simul diuisibilis adeoque ipsum AA et proin etiam ipsum $4D$ metietur, quare $\frac{4Drr}{hhh'h'}$ erit integer (negatiuus), quem statuendo $= -e$, erit $pp - Dqq = -\frac{4D}{e}$ siue $4 = (\frac{2rp}{hh'})^2 + eqq$, in qua aequatione pars $(\frac{2rp}{hh'})^2$ tamquam quadratum ipso 4 minus necessario erit vel 0 vel 1. In casu priori erit $eqq = 4$, et $D = -(\frac{hh'}{rq})^2$, vnde sequitur, $\frac{4D}{AA}$ esse quadratum signo negatiuo affectum adeoque certo non $\equiv 1 \pmod{4}$, neque adeo O ordinem improprie primitiuum neque ex improprie pri-

mitiuo deriuatum. Hinc $\frac{D}{AA}$ erit integer, vnde facile deducitur, e per 4 esse diuisibilem, $qq = 1$, $D = -(\frac{hh'}{r})^2$ atque etiam $\frac{AA}{D}$ integrum. Hinc necessario erit $D = -AA$ siue $\frac{D}{AA} = -1$, quae est exceptio prima. In casu posteriori erit $eqq = 3$, vnde $e = 3$ et $4D = -3(\frac{hh'}{r})^2$; hinc $3(\frac{hh'}{rA})^2$ erit integer, qui, quoniam per quadratum integrum $(\frac{rA}{hh'})^2$ multiplicatus producit 3, non poterit esse alius quam 3; hinc $4D = -3AA$ siue $D = -\frac{3}{4}AA$, quae est exceptio secunda. In omnibus igitur reliquis casibus omnes formae pr. primitiuae in V, V', V'' etc. ad classes diuersas pertinebunt. — Pro casibus exceptis ea, quae ex disquisitione haud difficili sed hic breuitatis caussa supprimenda resultauerunt, apposuisse sufficiat. Scilicet in priori, ex formis pr. primitiuis in V, V', V'' etc. binae semper ad eandem classem pertinebunt, in posteriori ternae, ita vt multitudo omnium classium quaesitarum in illo casu fiat semissis, in hoc triens valoris expressionis in obs. praec. traditae.

Secundo quando D est numerus positiuus quadratus: singulae formae pr. primitiuae in V, V', V'' etc. sine exceptione classem peculiarem constituunt. Supponamus enim, (hh, i, k), $(h'h', i', k')$ esse duas tales formas diuersas proprie aequiualentes, transeatque prior in posteriorem per substitutionem propriam $\alpha, \beta, \gamma, \delta$. Tum

patet, omnia ratiocinia pro casu praec. adhibita, in quibus non supponatur D esse negatiuum, etiam hic valere. Designantibus itaque p, q, r idem vt illic, etiam hic erit $\frac{4Drr}{hnh'h'}$ integer, at non amplius negatiuus sed positiuus insuperque quadratus, quo posito $= gg$, erit $(\frac{2rp}{hh'})^2 - ggqq = 4$, *Q. E. A.*, quia differentia duorum quadratorum nequit esse 4, nisi quadratum minus fuerit 0; quamobrem suppositio consistere nequit.

Pro casu *tertio* autem, vbi D est numerus positiuus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitiuarum in V, V', V'' etc. cum multitudine classium diuersarum inde resultantium hucusque non habemus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi $tt - Duu = AA$ satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (vt in casibus praecc.), de hac re nihil certi pronunciare possumus. Ecce quaedam exempla, quorum numerum quisque facile augere poterit. Pro $D = 13$, $A = 2$, multitudo formarum pr. prim. in V etc. est 3, quae omnes sunt aequiualentes siue vnicam classem efficiunt; pro $D = 37$, $A = 2$, etiam tres formae pr. prim. in V etc. habentur, quae ad tres classes diuersas pertinent; pro $D = 588$,

$A = 7$, habentur octo formae pr. prim. in V etc. quae efficiunt quatuor classes; pro $D = 869$, $A = 17$ in V etc. sunt 18 formae pr. primitiuae, totidem pro $D = 1445$, $A = 17$, sed quae pro illo determinante in duas classes discedunt, pro hoc in sex.

VI. Ex applicatione huius theoriae generalis ad eum casum, vbi O est ordo improprie primitiuus, colligitur, multitudinem classium in hoc ordine contentarum fore ad multitudinem omnium classium in ordine proprie primitiuo, vt 1 ad multitudinem classium diuersarum quas hae tres formae $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ efficiunt. Et quidem hinc resultabit vnica classis, quando $D \equiv 1 \pmod 8$, quia in hoc casu forma secunda et tertia sunt improprie primitiuae; quando vero $D \equiv 5 \pmod 8$, illae tres formae omnes erunt proprie primitiuae totidemque classes diuersas producent si D est negatiuus, vnico casu excepto, vbi $D = -3$, in quo vnicam classem constituunt; denique casus vbi D est positiuus (formae $8n + 5$) ad eos pertinet, pro quibus regula generalis hactenus desideratur. Id tamen asserere possumus, illas tres formas in hoc casu vel ad tres classes diuersas pertinere vel ad vnicam, numquam ad duas; facile enim perspicitur, si formae $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ resp. pertineant ad classes K, K', K'' fore

$K + K' = K'$, $K' + K' = K''$, adeoque, si K et K', identicae esse supponantur, etiam K' et K'' identicas fore; simili ratione si K et K'' supponuntur esse identicae, etiam K' et K'' erunt; denique quum sit $K' + K'' = K$, ex suppositione, K' et K'' identicas esse, sequitur, etiam K et K'' coincidere; vnde colligitur, vel omnes tres classes K, K', K'' esse diuersas, vel omnes tres identicas. E. g. infra 600 dantur 75 numeri formae $8n + 5$, inter quos sunt 17 determinantes pro quibus casus prior locum habet siue multitudo classium in ordine pr. primitiuo ter maior est quam in impr. primitiuo, puta 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 397, 405, 485, 557, 573; pro 58 reliquis casus posterior valet, siue multitudo classium in vtroque ordine est aequalis.

VII. Vix opus erit, obseruare, per disquisitionem praecedentem non solum multitudines classium in ordinibus diuersis eiusdem determinantis comparari posse, sed illam etiam ad quosuis determinantes diuersos qui rationem quadratorum inter se teneant esse applicabilem. Scilicet designante O ordinem quemcunque det. dmm, O' ordinem det. $dm'm'$, O comparari poterit cum ordine proprie primitiuo det. dmm, atque hic cum ordine deriuato ex ordine pr. prim. det. d, siue, quod respectu multitudinis classium eodem redit, cum hoc ordine ipso; et cum eodem prorsus simili ratione comparari poterit ordo O'.

257. Inter omnes classes in ordine dato determinantis dati imprimis classes ancipites disqui-

sitionem vberiorem postulant, determinatioque multitudinis harum classium ad multa alia viam nobis aperiet. Sufficit autem, hanc multitudinem in solo ordine pr. primitiuo assignare, quum casus reliqui ad hunc facile reduci possint. Hoc negotium ita absoluemus, vt primo omnes formas ancipites pr. primitiuas (A, B, C) determinantis propositi D, in quibus vel $B = 0$ vel $B = \frac{1}{2}A$, eruere, tunc ex harum multitudine multitudinem omnium classium ancipitum pr. primitiuarum det. D inuenire doceamus.

I. Omnes formae pr. primitiuae $(A, 0, C)$ determinantis D manifesto inueniuntur, accipiendo pro A singulos diuisores ipsius D (tum positiue tum negatiue) pro quibus $C = -\frac{D}{A}$ fit primus ad A. Quando itaque $D = 1$, duae huiusmodi formae dantur $(1, 0, -1)$, $(-1, 0, 1)$; totidem quando $D = -1$, puta $(1, 0, 1)$, $(-1, 0, -1)$; quando D est numerus primus aut numeri primi potestas (siue signo positiuo siue negatiuo), quatuor dabuntur $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. Generaliter autem, quando D per n numeros primos diuersos est diuisibilis (inter quos hoc loco etiam 2 in computum ingredi debet): dabuntur omnino 2^{n+1} huiusmodi formae; scilicet posito $D = \pm PQR \ldots$, designantibus P, Q, R etc. numeros primos diuersos aut numerorum primorum diuersorum potestates quorum multitudo $= n$, valores ipsius A erunt $1, P, Q, R$ etc. atque producta ex quotcunque horum numerorum; horum valorum multitudo fit per theo-

riam combinationum 2^n, sed duplicanda est, quoniam singulis valoribus tum signum positiuum tum negatiuum tribuere oportet.

II. Simili modo patet, omnes formas pr. primitiuas $(2B, B, C)$ determinantis D obtineri, si pro B accipiantur omnes diuisores ipsius D (positiue et negatiue), pro quibus $C = \frac{1}{2}(B - \frac{D}{B})$ fit integer et ad $2B$ primus. Quum itaque C necessario debeat esse impar, adeoque $CC \equiv 1 \pmod 8$, ex $D = BB - 2BC = (B - C)^2 - CC$ sequitur, D esse vel $\equiv 3 \pmod 4$, quando B impar, vel $\equiv 0 \pmod 8$, quando B par; quoties itaque D alicui numerorum $1, 2, 4, 5, 6$ sec. mod. 8 est congruus, nullae huiusmodi formae dabuntur. Quando $D \equiv 3 \pmod 4$, C fit integer et impar, quicunque diuisor ipsius D pro B accipiatur; ne vero C diuisorem communem cum $2B$ habeat, B ita accipi debebit, vt $\frac{D}{B}$ ad B fiat primus; hinc pro $D = -1$ duae formae habentur $(2, 1, 1)$, $(-2, -1, -1)$, generaliterque facile perspicitur, si multitudo omnium numerorum primorum ipsum D metientium sit n, omnino emergere 2^{n+} formas. — Quando D per 8 est diuisibilis, C fit integer, accipiendo pro B diuisorem quemcunque parem ipsius $\frac{1}{2}D$; conditioni alteri autem, vt $C = \frac{1}{2}B - \frac{D}{2B}$ ad $2B$ sit primus, satisfit *primo*, accipiendo pro B omnes diuisores impariter pares ipsius D, pro quibus $\frac{D}{B}$ cum B diuisorem communem non habet, quorum multitudo (habita ratione diuersitatis signorum) erit

2^{n+1}, si D per n numeros primos impares diuersos diuisibilis esse supponitur; *secundo*, accipiendo pro B omnes diuisores pariter pares ipsius $\frac{1}{2}D$, pro quibus $\frac{D}{2B}$ fit primus ad B, quorum multitudo quoque erit 2^{n+1}, ita vt in hoc casu omnino habeantur 2^{n+2} huiusmodi formae. Scilicet ponendo $D = \pm 2^{\mu} PQR\ldots$, designante μ exponentem maiorem quam 2; P, Q, R numeros primos impares diuersos aut talium numerorum primorum potestates quorum multitudo n: *tum* pro $\frac{1}{2}B$, *tum* pro $\frac{D}{2B}$ accipi possunt valores 1, P, Q, R etc. productaque ex quotcunque horum numerorum, signo et positiuo et negatiuo.

Ex his omnibus colligitur, si D per n numeros primos impares diuersos diuisibilis supponatur (statuendo $n = 0$, quando $D = \pm 1$ aut ± 2 aut potestas binarii), multitudinem omnium formarum pr. primitiuarum (A, B, C), in quibus B vel 0 vel $\frac{1}{2}A$, fore 2^{n+1} quando D aut $\equiv 1$ aut $\equiv 5 \pmod 8$; 2^{n+2} quando $D \equiv 2, 3, 4, 6$ aut $7 \pmod 8$; denique 2^{n+3} quando $D \equiv 0 \pmod 8$. Quam comparando cum iis quae in art. 231 pro multitudine omnium characterum possibilium formarum primitiuarum det. D tradidimus, obseruamus, illam in omnibus casibus praecise esse duplo hac maiorem. Ceterum manifestum est, quando D sit negatiuus, inter illas formas totidem positiuas affore quot negatiuas.

258. Omnes formae in art. praec. erutae manifesto pertinent ad classes ancipites, et vice

versa in quauis classe ancipite pr. primitiua det. D saltem vna illarum formarum contenta esse debet; in tali enim classe certo adsunt formae ancipites et cuiuis formae ancipiti pr. primitiuae (a, b, c) det. D aliqua formarum art. praec. aequiualet, scilicet vel $(a, 0, -\frac{D}{a})$ vel $(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a})$, prout b vel $\equiv 0$ vel $\equiv \frac{1}{2}a \pmod{a}$. Problema itaque eo reductum est, vt quot classes diuersas illae formae constituant inuestigemus.

Si forma $(a, 0, c)$ est inter formas art. praec., forma $(c, 0, a)$ inter easdem occurret et ab illa semper erit diuersa, vnico casu excepto vbi $a = c = \pm 1$ adeoque $D = -1$, quem aliquantisper seponemus. Quoniam vero hae formae manifesto ad eandem classem pertinent, sufficit vnam retinere, et quidem reiiciemus eam, cuius terminus primus est maior quam tertius; eum casum vbi $a = -c = \pm 1$ siue $D = 1$ quoque seponemus. Hoc modo omnes formas $(A, 0, C)$ ad semissem reducere possumus, retinendo e binis semper vnam; et in omnibus remanentibus erit $A < \sqrt{\pm D}$.

Simili modo si inter formas art. praec. occurrit forma $(2b, b, c)$, inter easdem reperietur $(4c - 2b, 2c - b, c) = (-\frac{2D}{b}, -\frac{D}{b}, c)$, quae illi proprie aequiualens et ab ipsa diuersa erit, vnico quem seponimus casu excepto vbi $c = b = \pm 1$ siue $D = -1$. Ex his

duabus formis eam retinere sufficit, cuius terminus primus est minor quam terminus primus alterius (magnitudine aequales, signis diuersi in hoc casu esse nequeunt); vnde patet, etiam omnes formas $(2B, B, C)$ ad semissem reduci posse, e binis vnam semper eiiciendo; et in remanentibus esse $B < \frac{D}{B}$ siue $B < \sqrt{\pm D}$. Hoc modo ex omnibus formis art. praec. semissis tantum remanet, quarum complexum per W designabimus, nihilque superest, nisi vt ostendamus, quot classes diuersae ex his formis oriantur. Ceterum manifestum est, in eo casu vbi D sit negatiuus totidem formas positiuas in W affore quot negatiuas.

I. Quando D est negatiuus, singulae formae in W pertinebunt ad classes diuersas. Nam omnes formae $(A, 0, C)$ erunt reductae; similiter omnes formae $(2B, B, C)$ reductae erunt, praeter eas in quibus $C < 2B$; in tali vero forma erit $2C < 2B + C$; vnde (quoniam $B < \frac{D}{B}$ i. e. $B < 2C - B$, adeoque $2B < 2C$, siue $B < C$), $2C - 2B < C$ et $C - B < \frac{1}{2}C$ et proin $(C, C - B, C)$, quae manifesto illi aequiualet, forma reducta. Hoc modo totidem formae reductae habentur, quot formae habentur in W, et quum facile perspiciatur, inter illas neque identicas neque oppositas occurrere posse, vnico casu excepto vbi $C - B = 0$, in quo erit $B = C = \pm 1$, adeoque $D = -1$, quem iam seposuimus): omnes ad classes diuersas pertinebunt. Hinc colligitur, multitudinem omnium classium ancipitum pr. primitiuarum det. D multitudini formarum in W

seu semissi multitudinis formarum art. praec. aequalem esse; in casu excepto autem $D = -1$ per compensationem idem euenit, scilicit duae classes habentur, ad quarum alteram pertinent formae $(1, 0, 1)$, $(2, 1, 1)$, ad alteram hae $(-1, 0, -1)$, $(-2, -1, -1)$. Generaliter itaque pro determinante negatiuo multitudo omnium classium ancipitum pr. prim. aequalis est multitudini omnium characterum assignabilium formarum primitiuarum huius determinantis; multitudo classium ancipitum pr. prim. positiuarum autem semissis erit.

II. Quando D est positiuus quadratus $= hh$, haud difficile demonstratur, singulas formas in W ad classes diuersas pertinere; sed pro hoc casu ad problematis solutionem adhuc breuius sequenti modo peruenire possumus. Quum per art. 210 in quauis classe ancipite pr. prim. det. hh, neque in vlla alia, contineatur forma reducta vna $(a, h, 0)$, in qua a est valor expr. $\sqrt{1}$ (mod. $2h$) inter 0 et $2h - 1$ incl. situs: perspicuum est, totidem classes ancipites pr. prim. det. hh dari, quot valores expressos illa habeat. Ex art. 105 autem nullo negotio deducitur, multitudinem horum valorum esse 2^n vel 2^{n+1} vel 2^{n+2}, prout h sit impar vel impariter par vel pariter par, siue prout $D \equiv 1$ vel $\equiv 4$ vel $\equiv 0$ (mod. 8), designante n multitudinem diuisorum primorum imparium ipsius h siue ipsius D. Hinc colligitur, multitudinem classium ancipitum pr. prim. semper esse semissem multitudinis omnium formarum in art. praec. erutarum, siue multitudini formarum in W vel omnium characterum possibilium aequalem.

III. Quando D est positiuus non quadratus, ex singulis formis (A, B, C) in W contentis alias deducamus (A, B', C'), accipiendo $B' \equiv B \pmod{A}$ et inter limites $\sqrt{D}$ et $\sqrt{D} \mp A$ (vbi signum superius vel inferius adhibendum, prout A est pos. vel neg.) atque $C' = \frac{B'B' - D}{A}$; designemusque harum complexum per W'. Manifesto hae formae erunt proprie primitiuae ancipites det. D, atque omnes inter se diuersae: praeterea vero omnes erunt formae reductae. Quando enim $A < \sqrt{D}$, B' manifesto erit $< \sqrt{D}$ atque positiuus; praeterea $B' > \sqrt{D} \mp A$ adeoque $A > \sqrt{D} - B'$ et proin A, positiue acceptus, certo inter $\sqrt{D} + B'$ et $\sqrt{D} - B'$ situs. Quando vero $A > \sqrt{D}$, non poterit esse $B = 0$ (quippe quas formas eiecimus), sed erit necessario $B = \frac{1}{2}A$; hinc B' magnitudine ipsi $\frac{1}{2}A$ aequalis, signo positiuus (quoniam enim $A < 2\sqrt{D}$, $\pm \frac{1}{2} A$ iacebit inter limites ipsi B' assignatos, ipsique B sec. mod. A erit congruus; quare $B' = \pm \frac{1}{2} A$), proin $B' < \sqrt{D}$, vnde $2B' < \sqrt{D} + B'$ siue $A < \sqrt{D} + B'$, quamobrem $\pm A$ necessario inter limites $\sqrt{D} + B'$ et $\sqrt{D} - B'$ iacebit. Denique W' omnes formas reductas pr. prim. ancipites det. D continebit; si enim (a, b, c) est huiusmodi forma, erit vel $b \equiv 0$, vel $b \equiv \frac{1}{2} a \pmod{a}$. In casu priori manifesto non poterit esse $b < a$ neque adeo $a > \sqrt{D}$, quapropter forma $(a, 0, -\frac{D}{a})$ certo contenta erit in W, et respondens (a, b, c) in W'; in posteriori certo erit $a < 2\sqrt{D}$, adeoque $(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a})$ in W contenta, atque

respondens (a, b, c) in W'. Ex his colligitur, multitudinem formarum in W aequalem esse multitudini omnium formarum reductarum ancipitum pr. prim. det. D; quoniam vero in singulis classibus ancipitibus *binae* formae reductae ancipites continentur (artt. 187, 194), multitudo omnium classium ancipitum pr. prim. det. D erit semissis multitudinis formarum in W, siue semissis omnium characterem assignabilium.

259. Multitudo classium ancipitum improprie primitiuarum determinantis dati D multitudini proprie primitiuarum eiusdem det. semper est aequalis. Sit K classis principalis, atque K', K'' etc. reliquae classes ancipites pr. primitiuae huius determinantis; L aliqua classis anceps improprie primitiua eiusdem det., e. g. ea in qua est forma $(2, 1, \frac{1}{2} - \frac{1}{2}D)$. Prodibit itaque ex compositione classis L cum K classis L ipsa; ex compositione classis L cum K', K'' etc. prouenire supponamus classes L', L'' etc. resp., quae manifesto omnes ad eundem determinantem D pertinebunt, atque improprie primitiuae et ancipites erunt. Patet itaque, theorema demonstratum fore, simulac probatum fuerit, omnes classes L, L', L'' etc. esse diuersas, aliasque ancipites impr. prim. det. D praeter illas non dari. Ad hunc finem sequentes casus distinguimus:

I. Quando multitudo classium impr. primitiuarum multitudini pr. primitiuarum aequalis est, quaeuis illarum oritur ex compositione classis L cum classe determinata proprie primitiua, vnde necessario omnes L, L', L'' etc. erunt diuersae.

Designante autem $\mathfrak{L}$ classem quamcunque ancipitem impr. prim. det. D, dabitur classis proprie primitiua $\mathfrak{K}$ talis vt sit $\mathfrak{K} + L = \mathfrak{L}$; si classi $\mathfrak{K}$ opposita est classis $\mathfrak{K}'$, erit etiam (quoniam classes L, $\mathfrak{L}$ sibi ipsae oppositae sunt) $\mathfrak{K}' + L = \mathfrak{L}$, vnde necessario $\mathfrak{K}$ cum $\mathfrak{K}'$ identica, erit, adeoque classis anceps: hinc $\mathfrak{K}$ reperietur inter classes K, K', K'' etc. atque $\mathfrak{L}$ inter has L, L', L'' etc.

II. Quando multitudo classium improprie primitiuarum ter maior est quam multitudo classium pr. primitiuarum, sit H classis in qua est forma $(4, 1, \frac{1-D}{4})$, H' ea in qua est forma $(4, 3, \frac{9-D}{4})$, eruntque H, H' proprie primitiuae et tum inter se tum a classe principali K diuersae, atque $H + H' = K$, $2H = H'$, $2H' = H$; et si $\mathfrak{L}$ est classis quaecunque improprie primitiua det. D, quae oritur ex compositione classis L cum proprie primitiua $\mathfrak{K}$, erit etiam $\mathfrak{L} = L + \mathfrak{K} + H$ et $\mathfrak{L} = L + \mathfrak{K} + H'$; praeter tres classes (pr. prim. atque diuersas) $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ aliae non dabuntur, quae cum L compositae ipsam $\mathfrak{L}$ producant. Quoniam igitur, si $\mathfrak{L}$ est anceps atque $\mathfrak{K}'$ ipsi $\mathfrak{K}$ opposita, etiam $L + \mathfrak{K}' = \mathfrak{L}$, necessario $\mathfrak{K}'$ cum aliqua illarum trium classium identica erit. Si $\mathfrak{K}' = \mathfrak{K}$, erit $\mathfrak{K}$ anceps; si $\mathfrak{K}' = \mathfrak{K} + H$, erit $K = \mathfrak{K} + \mathfrak{K}' = 2\mathfrak{K} + H = 2(\mathfrak{K} + H')$ adeoque $\mathfrak{K} + H'$ anceps; similiterque si $\mathfrak{K}' = \mathfrak{K} + H'$ erit $\mathfrak{K} + H$ anceps, vnde concluditur, $\mathfrak{L}$ inter classes L, L', L'' etc. necessario reperiri. Facile autem perspicitur, inter

tres classes $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ plures ancipites esse non posse; si enim tum $\mathfrak{K}$ tum $\mathfrak{K} + H$ ancipites essent siue cum oppositis suis $\mathfrak{K}'$, $\mathfrak{K}' + H'$ resp. identicae, foret $\mathfrak{K} + H = \mathfrak{K} H'$; eadem conclusio resultat ex suppositione, $\mathfrak{K}$ et $\mathfrak{K} + H'$ esse ancipites; denique si $\mathfrak{K} + H$, $\mathfrak{K} + H'$ ancipites siue cum oppositis suis $\mathfrak{K}' + H'$, $\mathfrak{K}' + H$ identicae essent, fieret $\mathfrak{K} + H + \mathfrak{K}' + H = \mathfrak{K}' + H' + \mathfrak{K} + H'$, vnde $2H = 2H'$, siue $H' = H$. Quamobrem vnica tantum classis anceps pr. prim. dabitur, quae cum L composita ipsam $\mathfrak{L}$ producit, adeoque omnes L, L', L'' etc. erunt diuersae.

Multitudo classium ancipitum in ordine *deriuato* manifesto aequalis est multitudini classium ancipitum in ordine primitiuo ex quo est deriuatus, adeoque per praecedentia semper poterit assignari.

260. Problema. *Classis proprie primitiua K determinantis D oritur ex duplicatione classis proprie primitiuae k eiusdem determinantis: quaeruntur omnes similes classes, ex quarum duplicatione classis K oritur.*

Sol. Sit H classis principalis det. D atque H', H'', H''' etc. reliquae classes ancipites pr. primitiuae eiusdem determinantis; classes quae ex harum compositione cum k oriuntur, $k + H'$, $k + H''$, $k + H'''$ etc. designentur per k', k'', k''' etc. Tunc omnes classes k, k', k'' etc. erunt pr. primitiuae det. D et inter se diuersae; aeque facile perspicitur, ex singularum duplicatione oriri classem K. Denotante autem $\mathfrak{K}$ classem quamcunque pr. prim. det. D, quae duplicata

producit classem K, necessario inter classes k, k', k'' etc. contenta erit. Ponatur enim $\mathfrak{K} = k + \mathfrak{H}$, ita vt $\mathfrak{H}$ sit classis pr. prim. det. D (art. 249), eritque $2k + 2\mathfrak{H} = 2\mathfrak{K} = K = 2k$, vnde facile concluditur, $2\mathfrak{H}$ coincidere cum classe principali, $\mathfrak{H}$ esse ancipitem siue inter H, H', H'' etc. contentam, atque $\mathfrak{K}$ inter k, k', k'' etc.; quamobrem hae classes completam problematis solutionem exhibent.

Ceterum manifestum est, in eo casu, vbi D sit negatiuus, e classibus k, k', k'' etc. semissem fore classes positiuas, semissem negatiuas.

Quum igitur quaeuis classis pr. prim. det. D, quae ex vllius classis similis duplicatione oriri potest, omnino ex totidem classium similium duplicatione proueniat, quot classes ancipites pr. prim. det. D dantur: perspicuum est, si multitudo cunctarum classium pr. prim. det. D sit r, multitudo omnium classium ancipitum pr. prim. huius det. n, multitudinem omnium classium pr. prim. eiusdem det. quae ex duplicatione similis classis produci possint fore $\frac{r}{n}$. Eadem formula resultat, si, pro det. negatiuo, characteres r, n multitudinem classium *positiuarum* designant, ille *omnium* pr. prim., hic solarum ancipitum. Ita e. g. pro $D = -161$ multitudo omnium classium pr. pr. positiuarum est 16, multitudo ancipitum 4, vnde multitudo omnium classium quae per duplicationem alicuius classis oriri possunt debebit esse 4. Et reuera inuenitur,

omnes classes in genere principali contentas hac proprietate esse praeditas; scilicet classis principalis (1, 0, 161) oritur ex duplicatione quatuor classium ancipitum; (2, 1, 18) ex duplicatione classium (9, 1, 18), (9, — 1, 18), (11, 2, 15), (11, — 2, 15); (9, 1, 18) ex dupl. classium (3, 1, 54), (6, 1, 27), (5, — 2, 33), (10, 3, 17); denique (9, — 1, 18) ex duplicatione classium (3, — 1, 54), (6, — 1, 27), (5, 2, 33), (10, — 3, 17).

261. THEOREMA. *Semissi omnium characterum assignabilium pro determinante positiuo non quadrato nulla genera proprie primitiua respondere possunt; pro determinante negatiuo autem nulla genera proprie primitiua positiua.*

Dem. Sit m multitudo omnium generum proprie primitiuorum (positiuorum) determinantis D; k multitudo classium in singulis generibus contentarum, ita vt km sit multitudo omnium classium proprie primitiuarum (positiuarum); n multitudo omnium characterum diuersorum pro hoc det. assignabilium. Tunc per art. 258 multitudo omnium classium ancipitum (positiuarum) pr. primitiuarum erit $\frac{1}{2}n$; hinc per art. praec. multitudo omnium classium pr. prim. quae ex duplicatione similis classis oriri possunt erit $\frac{2km}{n}$. Sed per art. 247 hae classes omnes pertinent ad genus principale, in quo continentur k classes; si itaque omnes classes generis principalis ex duplicatione alicuius classis prouenire possunt (quod reuera semper locum habere in sequentibus de-

monstrabitur), erit $\frac{2km}{n} = k$, siue $m = \frac{1}{2}n$; certo autem nequit esse $\frac{2km}{n} > k$ neque adeo $m > \frac{1}{2}n$. Quoniam itaque multitudo omnium generum pr. prim. (positiuorum) certo non est maior quam semissis omnium characterum assignabilium: ad minimum horum semissi talia genera respondere nequeunt. *Q. E. D.* — Ceterum probe notandum est, hinc nondum sequi, semissi omnium characterum assignabilium reuera respondere genera pr. prim. (positiua), sed huius propositionis grauissimae veritas infra demum e reconditissimis numerorum mysteriis enodari poterit.

Quum pro determinante negatiuo totidem genera negatiua semper exstent quot positiua, manifesto ex omnibus characteribus assignabilibus non plures quam semissis generibus pr. prim. negatiuis competere possunt, de qua re vt et de generibus impr. prim. infra loquemur. Denique obseruamus, theorema ad determinantes positiuos quadratos non extendi, pro quibus nullo negotio perspicitur singulis characteribus assignabilibus genera reuera respondere.

262. In eo itaque casu, vbi pro determinante non-quadrato dato D duo tantummodo characteres diuersi assignari possunt, vnico tantum genus pr. primitiuum (positiuum) respondebit, (quod non poterit esse aliud quam genus principale), alter nulli formae pr. prim. (pos.) illius determinantis competet. Hoc euenit pro determinantibus -1, 2, -2, -4, numeris primis formae $4n + 1$

positiue, iisque formae $4n + 3$ negatiue acceptis, denique pro omnibus numerorum primorum formae $4n + 1$ potestatibus exponentis imparis positiue sumtis, et pro potestatibus numerorum primorum formae $4n + 3$ positiue vel negatiue sumtis prout exponentes sunt pares vel impares. Ex hoc principio methodum nouam haurire possumus, non modo theorema fundamentale, sed etiam reliqua theoremata sect. praec. ad residua -1, $+2$, -2 pertinentia demonstrandi, quae a methodis in sect. praec. adhibitis omnino est diuersa, elegantiaque his neutiquam inferior aestimanda videtur. Determinantem -4 autem, et qui sunt numerorum primorum potestates, quum nihil noui doceant, praeteribimus.

Pro determinante -1 itaque nulla forma positiua datur cuius character sit $3, 4$; pro determinante $+2$, nulla omnino forma cuius character sit 3 *et* $5, 8$; pro determinante -2 nulli formae positiuae competet character 5 et $7, 8$; pro determinante $+p$, si p est numerus primus formae $4n + 1$, vel pro determinante $-p$, si p est numerus primus formae $4n + 3$, nulli formae pr. pr. (positiuae in casu post.) competet character Np. Hinc theoremata sect. praec. sequenti modo demonstramus:

I. Est -1 non residuum cuiusuis numeri (positiui) formae $4n + 3$. Si enim -1 residuum talis numeri A esset, faciendo $-1 = BB - AC$, foret (A, B, C) forma positiua det. -1 cuius character $3, 4$.

II. Est — 1 residuum cuiusuis numeri primi p formae $4n + 1$. Nam character formae $(-1, 0, p)$, sicuti omnium proprie primitiuarum det. p, erit Rp, adeoque $-1Rp$.

III. Tum + 2 tum — 2 est residuum cuiusuis numeri primi p formae $8n + 1$. Nam vel formae $(8, 1, \frac{1-p}{8})$, $(-8, 1, \frac{p-1}{8})$, vel hae $(8, 3, \frac{9-p}{8})$, $(-8, 3, \frac{p-9}{8})$ erunt proprie primitiuae (prout n impar vel par), adeoque ipsarum character Rp; hinc $+8Rp$ et $-8Rp$, vnde etiam $2Rp$, $-2Rp$.

IV. Est + 2 non residuum cuiusuis numeri formae $8n + 3$ aut $8n + 5$. Si enim esset residuum talis numeri A, daretur forma (A, B, C) determinantis + 2, cuius character 3 *et* 5, 8.

V. Simili modo — 2 est non residuum cuiusuis numeri formae $8n + 5$ aut $8n + 7$, alioquin enim daretur forma (A, B, C) determinantis — 2 cuius character 5 *et* 7, 8.

VI. Est — 2 residuum cuiusuis numeri primi p formae $8n + 3$. Hanc propositionem per methodum duplicem demonstrare licet. *Primo*, quum per IV sit $+2Np$, atque per I, $-1Np$, necessario erit $+2Rp$. Demonstratio *secunda* petitur ex consideratione determinantis $+2p$, pro quo quatuor characteres sunt assignabiles, puta Rp, 1 *et* 3, 8; Rp, 5 *et* 7, 8; Np, 1 *et* 3, 8; Np, 5 *et* 7, 8, ex quibus igitur saltem duobus

nulla genera respondebunt. Iam formae $(1, 0, -2p)$ competit character primus; formae $(-1, 0, 2p)$ quartus; quare qui reiici debent sunt secundus atque tertius. Quum itaque character formae $(p, 0, -2)$ relatiue ad numerum 8 sit 1 *et* 3, 8, ipsius character relatiue ad p non poterit esse alius quam Rp, vnde $-2Rp$.

VII. Est $+2$ residuum cuiusuis numeri primi p formae $8n + 7$, quod per methodum duplicem demonstrare licet. *Primo*, quum ex I et V sit $-1Np$, $-2Np$, erit $+2Rp$. *Secundo* quum vel $(8, 1, \frac{1+p}{8})$ vel $(8, 3, \frac{9+p}{8})$ sit forma proprie primitiua determinantis p (prout n par vel impar), ipsius character erit Rp, adeoque $8Rp$ et $2Rp$.

VIII. Quilibet numerus primus p formae $4n + 1$ est non residuum cuiusuis numeri imparis q, qui ipsius p non residuum est. Patet enim, si p esset residuum ipsius q, dari formam proprie primitiuam determinantis p cuius character Np.

IX. Simili modo si numerus quicunque impar q est non residuum numeri primi p formae $4n + 3$, erit $-p$ non residuum ipsius q; alioquin enim daretur forma positiua pr. primitiua determinantis $-p$ cuius character Np.

X. Quiuis numerus primus p formae $4n + 1$ est residuum cuiusuis alius numeri primi q, qui ipsius p residuum est. Si etiam q est formae

$4n + 3$, erit etiam — q residuum ipsius p (propter II) adeoque pRq (ex IX).

XI. Si numerus quicunque primus q est residuum alius numeri primi p formae $4n + 3$, erit — p residuum ipsius q. Si enim q est formae $4n + 1$, ex VIII sequitur pRq, adeoque (per II), — pRq; casus autem vbi etiam q est formae $4n + 3$ huic methodo se subducit, attamen facile ex consideratione determinantis + pq absolui potest. Scilicet quum ex quatuor characteribus pro hoc determinante assignabilibus Rp, Rq; Rp, Nq; Np, Rq; Np, Nq duobus nulla genera respondere possint, atque formarum (1, 0, — pq), (— 1, 0, pq) characteres respectiue sint primus et quartus, character secundus et tertius nulli formae pr. prim. det. pq competere possunt. Quum itaque character formae (q, 0, — p) resp. numeri p per hyp. sit Rp, eiusdem formae character respectu numeri q debet esse Rq, adeoque — pRq. *Q. E. D.*

Si in proposs. VIII et IX, q supponitur designare numerum primum, hae cum X et XI iunctae theorema fundamentale sect. praec. exhibent.

263. Postquam theorema fundamentale demonstratione noua comprobauimus, eam characterum semissem, quibus nullae formae pr. primitiuae (positiuae) respondere possunt, pro determinante quocunque non quadrato dato discernere ostendemus, quod negotium eo breuius absoluere licebit, quum ipsius fundamentum iam

in disquisitione artt. 147 - 150 sit contentum. Sit ee quadratum maximum, determinantem propositum D metiens, atque $D = D'ee$, ita vt D' nullum factorem quadratum implicet; porro sint a, b, c etc. omnes diuisores primi impares ipsius D', adeoque D' sine respectu signi sui vel productum ex his numeris vel duplum huius producti. Designetur per Ω complexus characterum particularium Na, Nb, Nc etc., solus, quando $D' \equiv 1 \pmod 4$; adiuncto charactere 3, 4, quando $D' \equiv 3$ atque e impar aut impariter par; adiunctis his 3, 8 atque 7, 8, quando $D' \equiv 3$ atque e pariter par; adiuncto vel charactere 3 *et* 5, 8, vel duobus 3, 8 atque 5, 8, quando $D' \equiv 2 \pmod 8$ atque e vel impar vel par; denique adiuncto vel charactere 5 *et* 7, 8, vel duobus 5, 8 atque 7, 8, quando $D' \equiv 6 \pmod 8$ atque e vel par vel impar. His ita factis, omnibus characteribus integris, in quibus multitudo impar characterum particularium Ω continetur, nulla genera proprie primitiua (positiua) determinantis D respondere poterunt. In omnibus casibus characteres particulares, qui exprimunt relationem ad tales diuisores primos ipsius D qui ipsum D' non metiuntur, ad generum possibilitatem vel impossibilitatem nihil conferunt. — Ex theoria combinationum autem facillime perspicitur, hoc modo reuera semissem omnium characterum integrorum assignabilium excludi.

Demonstratio horum praeceptorum adornatur sequenti modo. E principiis sect. praec., siue theorematibus in art. praec. denuo demonstratis nullo negotio deducitur, si p sit numerus

primus (impar positiuus) ipsum D non metiens, cui aliquis e characteribus reiectis competat, D' implicare multitudinem imparem factorum qui sint non residua ipsius p, atque adeo D', et hinc etiam D, esse non residuum ipsius p; porro facile perspicitur, productum e numeris quotcunque imparibus ad D primis, quorum nulli aliquis characterum reiectorum competat, etiam cum tali charactere consentire non posse; hinc vice versa perspicuum est, quemuis numerum imparem positiuum ad D primum, cui aliquis characterum reiectorum conueniat, certe aliquem factorem primum eiusdem qualitatis implicare, adeoque D ipsius non residuum esse. Si itaque forma proprie primitiua (positiua) determinantis D daretur, alicui characterum reiectorum respondens, D foret non residuum cuiusuis numeri positiui imparis ad ipsum primi per talem formam repraesentabilis, quod manifesto cum theoremate art. 154 consistere nequit.

Tamquam exempla conferantur classificationes in artt. 230, 231 traditae, quarum numerum quisque pro lubitu augere poterit.

264. Hoc itaque modo pro quouis determinante non quadrato dato omnes determinantes assignabiles in duas species P, Q aequaliter distribuuntur, ita vt nulli characterum Q forma proprie primitiua positiua respondere possit, reliquis autem P, quantum quidem hucusque nouimus, nihil obstet, quominus ad tales formas pertineant. Circa has characterum species notetur imprimis propositio sequens, quae ex ipsarum

criterio facile deducitur: Si character ex P cum charactere ex Q componitur (ad normam art. 246 perinde ac si etiam huic genus responderet) prodibit character ex Q; si vero duo characteres ex P, vel duo ex Q componuntur, character resultans ad P pertinebit. Adiumento huius theorematis etiam pro generibus negatiuis atque improprie primitiuis semissis omnium characterum assignabilium excludi potest sequenti modo.

I. Pro determinante negatiuo D genera negatiua positiuis hoc respectu prorsus contraria erunt, scilicet nullus characterum P pertinebit ad genus proprie primitiuum negatiuum, sed haec genera omnia habebunt characteres ex Q. Quando enim $D' \equiv 1 \pmod 4$, erit $-D'$ numerus positiuus formae $4n + 3$, adeoque inter a, b, c etc. multitudo impar numerorum formae $4n + 3$, quorum singulorum non residuum erit -1, vnde patet, in characterem integrum formae $(-1, 0, D)$ in hoc casu ingredi multitudinem imparem characterum particularium ex Ω, siue illum pertinere ad Q; quando $D' \equiv 3 \pmod 4$, ex simili ratione inter a, b, c etc. vel nullus numerus formae $4n + 3$ reperietur, vel duo, vel quatuor etc., sed quum vel 3, 4 vel 7, 8 in hoc casu occurrat inter characteres particulares formae $(-1, 0, D)$, patet, characterem integrum huius formae etiam hic pertinere ad Q. Eadem conclusio aeque facile in casibus reliquis obtinetur, ita vt forma negatiua $(-1, 0, D)$ semper habeat characterem ex Q. Sed quoniam haec forma cum quacunque alia pr. primitiua negatiua eiusdem det. composita similem formam

positiuam producit, facile perspicitur, nullam formam pr. prim. negatiuam characterem ex P habere posse.

II. Pro generibus improprie primitiuis (positiuis) simili modo probatur, rem vel eodem modo se habere vt in proprie primitiuis, vel contrario, prout $D \equiv 1$ vel $\equiv 5 \pmod 8$. Nam in casu priori erit etiam $D' \equiv 1 \pmod 8$, vnde facile concluditur, inter numeros a, b, c etc. vel nullum numerum formae $8n + 3$ et $8n + 5$ reperiri vel duos vel quatuor etc. (scilicet productum ex quotcunque numeris imparibus inter quos numeri formae $8n + 3$ et $8n + 5$ coniunctim multitudinem imparem efficiunt semper euadit vel $\equiv 3$ vel $\equiv 5 \pmod 8$, productum autem ex omnibus a, b, c etc., aequale esse debet vel ipsi D' vel ipsi $-D'$); hinc patet, characterem integrum formae $(2, 1, \frac{1-D}{2})$ inuoluere vel nullum characterem particularem ex Ω, vel duos vel quatuor etc., adeoque pertinere ad P. Iam quum quaeuis forma improprie primitiua (positiua) determinantis D spectari possit tamquam composita ex $(2, 1, \frac{1-D}{2})$ atque proprie primitiua (positiua) eiusdem determinantis, perspicuum est, nullam formam improprie primitiuam (positiuam) characterem ex Q in hoc casu habere posse. In casu altero, $D \equiv 5 \pmod 8$, omnia contraria sunt, scilicet D', qui etiam erit $\equiv 5$, certo multitudinem imparem factorum-formae $8n + 3$ atque $8n + 5$ implicabit, vnde concluditur, characterem formae $(2, 1,$

$\frac{1-D}{2}$), atque hinc etiam characterem cuiusuis formae improprie primitiuae (pos.) det. D, pertinere ad Q, adeoque nulli characterum P genus impr. prim. pos. respondere posse.

III. Denique pro determinante negatiuo genera improprie primitiua negatiua rursus contraria sunt generibus improprie primitiuis positiuis, scilicet illa non poterunt habere characterem ex P vel ex Q, prout $D \equiv 1$ vel $\equiv 5 \pmod 8$, siue prout $-D$ est formae $8n+7$ vel $8n+3$. Hoc nullo negotio deducitur inde, quod ex compositione formae $(-1, 0, D)$, cuius character est ex Q, cum formis improprie primitiuis negatiuis eiusdem determinantis formae improprie primitiuae positiuae proueniunt, adeoque, quando ab his exclusi sunt characteres Q, necessario ab illis exclusi esse debent characteres P, et contra.

265. Ex disquisitionibus artt. 257, 258 supra multitudine classium ancipitum, quibus omnia praecedentia sunt superstructa, multae aliae conclusiones attentione perdignae deduci possunt, quas breuitatis caussa supprimere oportet; sequentem tamen, elegantia sua insignem, praeterire non possumus. Pro determinante positiuo p, qui est numerus primus formae $4n+1$, vnicam tantummodo classem ancipitem proprie primitiuam dari ostendimus; quapropter omnes formae ancipites proprie primitiuae talis determinantis proprie aequiualentes erunt. Si itaque b est numerus integer positiuus proxime minor quam

$\sqrt{p}$, atque $p - bb = a'$, formae $(1, b, -a')$, $(-1, b, a')$ proprie aequiualebunt, adeoque, quum vtraque manifesto sit forma reducta, altera in alterius periodo erit contenta. Tribuendo formae priori in periodo sua indicem 0, index posterioris necessario erit impar (quoniam termini primi harum duarum formarum signa opposita habent); ponatur itaque $= 2m + 1$. Porro facile perspicitur, si formae indicum 1, 2, 3 etc. resp. sint $(-a', b', a'')$, $(a'', b'', -a''')$, $(-a''', b''', a^{IV})$ etc.: indicibus $2m$, $2m - 1$, $2m - 2$, $2m - 3$ etc. resp. responsuras esse formas $(a', b, -1)$, $(-a'', b', a')$, $(a''', b'', -a'')$, $(-a^{IV}, b''', a''')$ etc. Hinc colligitur, si forma indicis m sit (A, B, C), eandem fore $(-C, B, -A)$, adeoque $C = -A$ et $p = BB + AA$. Quare quiuis numerus primus formae $4n + 1$ in duo quadrata decomponi potest (quam propositionem supra, art. 182, e principiis prorsus diuersis deduximus), et ad talem decompositionem peruenire possumus per methodum simplicissimam et omnino vniformem, scilicet per euolutionem periodi formae reductae, cuius determinans est ille numerus primus et cuius terminus primus 1, vsque ad formam, cuius termini externi magnitudine sunt aequales, signis oppositi. Ita e. g. pro $p = 233$ habetur $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$, atque $233 = 64 + 169$. Ceterum patet, A necessario fieri imparem (quoniam $(A, B, -A)$ debet esse forma proprie primitiua), et proin B parem. — Quum pro determinante positiuo p, qui est numerus primus formae $4n + 1$, etiam in ordine

improprie primitiuo vnica tantum classis anceps contineatur, perspicuum est si g sit numerus impar proxime minor quam $\sqrt{p}$, atque $p - gg = 4h$, formas reductas improprie primitiuas $(2, g, -2h)$, $(-2, g, 2h)$ proprie aequiualere, adeoque alteram in alterius periodo contentam esse. Hinc per ratiocinia praecedentibus omnino similia concluditur, in periodo formae $(2, g, -2h)$ reperiri formam, cuius termini externi magnitudine aequales sint, signa habeant opposita, ita vt discerptio numeri p in duo quadrata etiam hinc peti possit. Patet autem, terminos externos huius formae fore pares, adeoque medium imparem; et quum constet, numerum primum vnico tantum modo in duo quadrata decomponi posse, forma per hanc posteriorem methodum inuenta erit vel $(B, \pm A, -B)$, vel $(-B, \pm A, B)$. Ita in exemplo nostro pro $p = 233$ habetur $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$, et $233 = 169 + 64$ vt supra.

266. Hactenus disquisitionem nostram ad tales functiones secundi gradus restrinximus, quae *duas* indeterminatas implicant, neque opus fuit, denominationem specialem ipsis tribuere. Sed manifesto hoc argumentum tamquam sectionem maxime particularem disquisitionis generalissimae *de functionibus algebraicis rationalibus integris homogeneis plurium indeterminatarum et plurium dimensionum* considerare, talesque functiones secundum multitudinem dimensionum in *formas secundi, tertii, quarti gradus etc.*, secundum multitudinem indeterminatarum autem

in *formas binarias*, *ternarias*, *quaternarias* etc. commode distinguere possumus. Formae itaque, hactenus simpliciter sic dictae, vocabuntur *formae binariae secundi gradus;* tales autem functiones vt $Axx + 2Bxy + Cyy + 2Dxz + 2Eyz + Fzz$ (denotantibus A, B, C, D, E, F integros datos) dicentur *formae ternariae secundi gradus* et sic porro. Proxime quidem Sectio praesens solis formis binariis secundi gradus est dicata; sed quoniam complures veritates ad has spectantes, eaeque pulcherrimae, adhuc supersunt, quarum fons proprius in theoria formarum ternariarum secundi gradus est querendus, breuem ad hanc theoriam digressionem hic intercalamus, in qua ex primis eius elementis ea trademus, quae ad perfectionem theoriae formarum binariarum sunt necessaria, quod geometris acceptius fore speramus, quam si illas vel supprimeremus, vel per methodos minus genuinas erueremus. Exactiorem autem de hoc argumento grauissimo disquisitionem ad aliam occasionem nobis reseruare debemus, tum quod ipsius vbertas limites huius operis iam nunc longe egrederetur, tum quod spes est, luculentis adhuc incrementis eam in posterum locupletatum iri. Formae vero tum quaternariae, quinariae etc. secundi gradus, tum omnes superiorum graduum hoc quidem loco ab instituto nostro penitus excluduntur *), sufficiatque hunc campum vastissimum geometrarum attentioni commendauisse, in quo materiem ingen-

*) Propter hanc rationem formae binariae vel ternariae *secundi gradus* in sequentibus semper sunt intelligendae, quoties de talibus formis simpliciter loquemur.

tem vires suas exercendi, Arithmeticamque sublimiorem egregiis incrementis augendi inuenient.

267. Ad perspicuitatem multum proderit, inter tres indeterminatas, in formam ternariam ingredientes, simili modo vt in formis binariis, ordinem fixum stabilire, ita vt *indeterminata prima*, *secunda* et *tertia* ab inuicem distinguantur; in disponendis autem singulis formae partibus hunc ordinem semper obseruabimus, vt primum locum obtineat ea pars quae quadratum indeterminatae primae implicat, in sequentibus eae quae implicant quadratum indeterminatae secundae, quadratum tertiae, productum duplum secundae in tertiam, productum duplum primae in tertiam, productum duplum primae in secundam deinceps sequantur; denique numeros integros determinatos per quos haec quadrata et producta dupla multiplicata sunt eodem ordine *coëfficientem primum*, *secundum*, *tertium*, *quartum*, *quintum*, *sextum* vocabimus. Ita $axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$ erit forma ternaria rite ordinata, cuius indeterminata prima x, secunda x', tertia x'', coëfficiens primus a etc., quartus b etc. Sed quoniam ad breuitatem multum conferet, si non semper necesse est, indeterminatas formae ternariae per literas peculiares denotare, eandem formam, quatenus ad indeterminatas non respicimus, etiam hoc modo $\left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ designabimus.

Ponendo $bb - a'a'' = A$, $b'b' - aa'' = A'$, $b''b'' - aa' = A''$, $ab - b'b'' = B$, $a'b' - bb'' = B'$, $a''b'' - bb' = B''$, oritur alia forma

$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \ldots F$, quam *formae* $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \ldots f$, *adiunctam* dicemus. Hinc rursus inuenitur, denotando breuitatis caussa numerum $abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b''$ per D, $BB - A'A'' = aD$, $B'B' - AA'' = a'D$, $B''B'' - AA' = a''D$, $AB - B'B'' = bD$, $A'B' - BB'' = b'D$, $A''B'' - BB' = b''D$, vnde patet, formae F adiunctam esse formam $\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}$. Numerum D, a cuius indole proprietates formae ternariae f imprimis pendent, *determinantem* huius formae vocabimus; hoc modo determinans formae F fit $= DD$, siue aequalis quadrato determinantis formae f, cui adiuncta est.

Ita e. g. formae ternariae $\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix}$ adiuncta est $\begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{pmatrix}$, vtriusque determinans $= 1$.

Formae ternariae determinantis 0 ab inuestigatione sequente omnino excludentur, quippe quae, vt in formarum ternariarum theoria, alia occasione vberius tradenda, ostendetur, *specie* tantum sunt ternariae, reueraque binariis aequipollentes.

268. Si forma aliqua ternaria f determinantis D, cuius indeterminatae sunt x, x', x'' (puta prima $= x$ etc.) in formam ternariam g determinantis E, cuius indeterminatae sunt y, y', y'', transmutatur per substitutionem talem

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'' \\ x' &= \alpha' y + \beta' y' + \gamma' y'' \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \end{aligned}$$

vbi nouem coëfficientes α, $\mathfrak{G}$ etc. omnes supponuntur esse numeri integri, breuitatis caussa neglectis indeterminatis simpliciter dicemus, f transire in g per substitutionem (S)

$$\begin{array}{ccc} \alpha, & \mathfrak{G}, & \gamma \\ \alpha', & \mathfrak{G}', & \gamma' \\ \alpha'', & \mathfrak{G}'', & \gamma'' \end{array}$$

atque f *implicare* ipsam g, siue g *sub* f *contentam* esse. Ex tali itaque suppositione sponte sequuntur sex aequationes pro sex coëfficientibus in g, quas apponere non erit necessarium; hinc autem per calculum facilem sequentes conclusiones euoluuntur:

I. Designato breuitatis caussa numero $\alpha\mathfrak{G}'\gamma'' + \mathfrak{G}\gamma'\alpha'' + \gamma\alpha'\mathfrak{G}'' - \gamma\mathfrak{G}'\alpha'' - \alpha\gamma'\mathfrak{G}'' - \mathfrak{G}\alpha'\gamma''$ per k, inuenitur post debitas reductiones $E = kkD$, vnde patet, D metiri ipsum E et quotientem esse quadratum. Patet itaque, numerum k pro transformationibus formarum ternariarum simile quid esse, ac numerum $\alpha\delta - \mathfrak{G}\gamma$ in art. 157 pro transformationibus formarum binariarum, puta radicem quadratam ex quotiente determinantium, vnde coniectare possemus, diuersitatem signi ipsius k etiam hic stabilire differentiam essentialem inter transformationes atque implicationes proprias et improprias. Sed rem propius contemplando perspicuum est, f transire in g etiam per hanc substitutionem

$$\begin{array}{ccc} -\alpha, & -\mathfrak{G}, & -\gamma \\ -\alpha', & -\mathfrak{G}', & -\gamma' \\ -\alpha'', & -\mathfrak{G}'', & -\gamma'' \end{array}$$

ponendo autem in valore ipsius k pro α, $-\alpha$, pro $\mathfrak{G}$, $-\mathfrak{G}$ etc. prodebit $-k$, quare haec substitutio substitutioni S dissimilis foret, et quaeuis forma ternaria, aliam vno modo implicans, eandem etiam altero modo implicaret. Talis itaque distinctio, quoniam in formis ternariis nullum vsum habet, hic omnino proscribetur.

II. Denotando per F, G formas ipsis f, g resp. adiunctas, determinantur coëfficientes in F per coëfficientes in f, coëfficientesque in G per valores coëfficientium formae g ex aequationibus quas suppeditat substitutio S notos. Exprimendo coëfficientes formae f per literas, ex comparatione valorum coëfficientium formarum F, G nullo negotio confirmatur, F implicare formam G atque in eam transmutari per substitutionem (S')

$$\begin{array}{llll} \mathfrak{G}'\gamma'' - \mathfrak{G}''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\mathfrak{G}'' - \alpha''\mathfrak{G}' \\ \mathfrak{G}''\gamma - \mathfrak{G}\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\mathfrak{G} - \alpha\mathfrak{G}'' \\ \mathfrak{G}\gamma' - \mathfrak{G}'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\mathfrak{G}' - \alpha'\mathfrak{G} \end{array}$$

Calculum ipsum nullis difficultatibus obnoxium non adscribimus.

III. Forma g per substitutionem (S'')

$$\begin{array}{lll} \mathfrak{G}'\gamma'' - \mathfrak{G}''\gamma', & \mathfrak{G}''\gamma - \mathfrak{G}\gamma'', & \mathfrak{G}\gamma' - \mathfrak{G}'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\mathfrak{G}'' - \alpha''\mathfrak{G}', & \alpha''\mathfrak{G} - \alpha\mathfrak{G}'', & \alpha\mathfrak{G}' - \alpha'\mathfrak{G} \end{array}$$

manifesto in eandem formam transmutatur, in quam f transit per hanc

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{matrix}$$

siue in eam, quae oritur multiplicando singulos coëfficientes formae f per kk. Hanc formam designabimus per f'.

IV. Prorsus simili modo probatur, formam G per substitutionem (S''')

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

transire in formam, quae oritur ex F, multiplicando singulos coëfficientes per kk. Hanc formam exprimemus per F'.

Substitutionem S''' oriri dicemus *per transpositionem* substitutionis; Si tunc manifesto S rursus prodit ex transpositione substitutionis S'''; atque S', S'' altera ex alterius transpositione. — Substitutio S' commode appellari potest substitutioni S *adiuncta*, vnde substitutioni S''' adiuncta erit S''.

269. Si non modo forma f implicat ipsam g, sed etiam haec illam, formae f, g *aequiualentes* vocabuntur. In hoc itaque casu non modo D ipsum E metietur, sed etiam E ipsum D, vnde facile concluditur esse, debere $D = E$. Vice versa autem, si forma f implicat formam g eiusdem determinantis, hae duae for-

mae erunt aequiualentes. Erit enim (adhibendo eadem signa vt in art. praec. excipiendoque casum vbi $D = 0$) $k = \pm 1$, adeoque forma f', in quam transit g per substitutionem S'', cum f identica, siue f sub g contenta. Porro patet, in hoc casu etiam formas F, G, ipsius f, g adiunctas, inter se aequiualentes fore, posterioremque in priorem transire per substitutionem S'''. Denique vice versa, si formae F, G aequiualentes esse *supponuntur*, atque prior transit in posteriorem per substitutionem T, etiam formae f, g aequiualentes erunt, transibitque f in g per substitutionem ipsi T adiunctam, atque g in f per eam quae oritur ex transpositione substitutionis T. Nam per has duas substitutiones resp. transit forma ipsi F adiuncta in formam ipsi G adiunctam atque haec in illam; hae duae formae autem oriuntur ex f, g multiplicando singulos coëfficientes per D; vnde nullo negotio concluditur, per easdem substitutiones transire f in g, atque g in f resp.

270. Si forma ternaria f formam ternariam f' implicat, atque haec formam f'': implicabit etiam f ipsam f''. Facillime enim perspicietur, si transeat

f in f' per substitutionem.	f in f'' per substitutionem;
α, β, γ	$\delta, \varepsilon, \zeta$
α', β', γ'	$\delta', \varepsilon', \zeta'$
$\alpha'', \beta'', \gamma''$	$\delta'', \varepsilon'', \zeta''$

f transmutatum iri per substitutionem

$\alpha\delta + \beta\delta' + \gamma\delta''$, $\alpha\varepsilon + \beta\varepsilon' + \gamma\varepsilon''$, $\alpha\zeta + \beta\zeta' + \gamma\zeta''$
$\alpha'\delta + \beta'\delta' + \gamma'\delta''$, $\alpha'\varepsilon + \beta'\varepsilon' + \gamma'\varepsilon''$, $\alpha'\zeta + \beta'\zeta' + \gamma'\zeta''$
$\alpha''\delta + \beta''\delta' + \gamma''\delta''$, $\alpha''\varepsilon + \beta''\varepsilon' + \gamma''\varepsilon''$, $\alpha''\zeta + \beta''\zeta' + \gamma''\zeta''$

In eo itaque casu, vbi f aequiualet ipsi f', atque f' ipsi f'', forma f etiam formae f'' aequualebit. — Ceterum sponte manifestum est, quomodo haec theoremata ad plures formas sint applicanda.

271. Hinc iam patet, omnes formas ternarias, perinde ac binarias, in *classes* distribui posse, referendo ad classem eandem formas aequiualentes, non aequiualentes ad diuersas. Formae itaque determinantium diuersorum certo ad classes diuersas pertinebunt, et proin classes infinite multae formarum ternariarum dabuntur; formae autem ternariae eiusdem determinantis modo minorem modo maiorem classium numerum efficiunt; quod vero tamquam proprietas palmaris harum formarum est considerandum, *omnes formae eiusdem determinantis dati semper constituunt classium multitudinem finitam.* Euolutioni vberiori huius grauissimi theorematis praemittenda est explicatio sequentis differentiae essentialis, quae inter formas ternarias obtinet.

Quaedam formae ternariae ita sunt comparatae, vt per ipsas sine discrimine repraesentari possint numeri positiui et negatiui, *e. g* forma $xx + yy - zz$, quamobrem *formae indefinitae* vocabuntur. Contra per alias numeri negatiui repraesentari nequeunt, sed (praeter cifram quae

prodit, ponendo singulas indeterminatas = 0) positiui tantum, vt $xx + yy + zz$, quare *formae positiuae* dicentur; denique per alias numeri positiui repraesentari nequeunt, vt $- xx - yy - zz$, vnde appellabuntur *formae negatiuae*; formae positiuae et negatiuae nomine communi *formae definitae* dicentur. Ecce iam criteria generalia, per quae haec formarum indoles discerni poterit.

Multiplicando formam ternariam $f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$, determinantis D per a, denotandoque coëfficientes formae ipsi f adiunctae, perinde vt in art. 268 per A, A', A'', B, B', B'', prodit $(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = g$; multiplicando denuo per A', prouenit $A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'x' = h$. Hinc statim concluditur, si tum A', tum aD sint numeri negatiui, omnes valores ipsius h esse negatiuos, vnde manifesto per formam f tales tantummodo numeri repraesentari poterunt, quorum signum oppositum est signo ipsius aA', i. e. identicum cum signo ipsius a, siue oppositum signo ipsius D. In hoc itaque casu f erit forma definita, et quidem positiua vel negatiua, prout a est positiuus vel negatiuus, siue prout D est negatiuus vel positiuus.

Si vero vel vterque aD, A' est positiuus, vel alter positiuus alter negatiuus (neuter = 0), facile perspicietur, h per debitam quantitatum x, x', x'' determinationem valores tum positiuos tum negatiuos nancisci posse. Quare in hoc

casu f valores tum eodem signo affectos vt aA' tum opposito, obtinere poterit, eritque adeo forma indefinita.

Pro eo casu, vbi $A' = 0$, neque vero $a = 0$, fit $g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2Bx'')$. Tribuendo ipsi x' valorem arbitarium (qui tamen non $= 0$), accipiendoque x'' ita vt $\frac{A''x'}{2B} - x''$ signum idem obtineat vt Bx' (quod fieri posse facile perspicitur, quum B nequeat esse $= 0$, hinc enim foret $BB - A'A'' = aD = 0$, adeoque etiam $D = 0$, quem casum excludimus), erit $x'(A''x' - 2Bx'')$ quantitas positiua, vnde facile patet, x ita determinari posse, vt g obtineat valorem negatiuum. Manifesto hi valores etiam ita accipi poterunt, vt, si desideretur, omnes sint integri. Denique patet, si ipsis x', x'' valores quicunque tribuantur, ipsum x tam magnum accipi posse, vt g fiat positiuus. Hinc concluditur, in hoc casu formam f esse indefinitam.

Denique si $a = 0$, erit $f = a'x'x' + 2bx'x'' + a''x''x'' + 2x(b''x' + b'x'')$. Accipiendo itaque x', x'' ad lubitum, ita tamen vt $b''x' + b'x''$ non sit $= 0$ (quod manifesto fieri poterit, nisi simul b' et b'' sint $= 0$; tunc autem foret $D = 0$), nullo negotio perspicitur, x ita determinari posse, vt f obtineat valores tum positiuos, tum negatiuos. Quare etiam in hocce casu f erit forma indefinita.

Eodem modo, vt hic ex numeris aD, A' indolem formae f diiudicauimus, etiam aD et A''

adhiberi possunt, ita vt f sit forma definita, si tum aD tum A'' sit negatiuus; indefinita in omnibus reliquis casibus. Nec non prorsus simili modo eidem fini inseruire potest consideratio numerorum $a'D$ et A, vel horum $a'D$ et A'', vel horum $a''D$ et A, vel denique ipsorum $a''D$ et A'.

Ex his omnibus colligitur, in forma definita sex numeros A, A', A'', aD, $a'D$, $a''D$ esse negatiuos, et quidem in forma positiua a, a', a'' erunt positiui, D negatiuus; in negatiua autem a, a', a'' erunt negatiui, D positiuus. Hinc patet, omnes formas ternarias determinantis dati positiui distribui in negatiuas et indefinitas; omnes autem determinantis negatiui in positiuas et indefinitas; denique formas positiuas determinantis positiui, seu negatiuas determinantis negatiui omnino non dari. — Ibinde facile perspicitur, formae definitae semper adiunctam esse definitam et quidam *negatiuam*, indefinitae indefinitam.

Quum omnes numeri per formam ternariam datam repraesentabiles manifesto etiam per omnes formas huic aequiualentes repraesentari possint: formae ternariae in eadem classe contentae vel omnes erunt indefinitae, vel omnes positiuae, vel omnes negatiuae. Quamobrem has formarum denominationes etiam ad classes integras transferre licebit.

272. Theorema in art. praec. propositum, quod omnes formae ternariae determinantis dati

in multitudinem *finitam* classium distribuuntur, per methodum ei qua in formis binariis vsi sumus analogam tractabimus, scilicet ostendendo, primo, quo pacto quaeuis forma ternaria ad formam simpliciorem reduci possit, dein, formarum simplicissimarum (ad quas per tales reductiones perueniatur), multitudinem pro quouis determinante dato esse finitam. Supponamus generaliter, propositam esse formam ternariam $f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ determinantis D (a cifra diuersi), quae per substitutionem (S)

$$\begin{matrix} \alpha, & \mathfrak{G}, & \gamma \\ \alpha', & \mathfrak{G}', & \gamma' \\ \alpha'', & \mathfrak{G}'', & \gamma'' \end{matrix}$$

transeat in aequiualentem $g = \begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$; versabiturque negotium nostrum in eo, vt α, $\mathfrak{G}$, γ etc. ita definiantur, vt forma g simplicior euadat quam f. Sint formae ipsis f, g adiunctae resp. $\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$, $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$, quae designentur per F, G. Tunc per art. 269. F transibit in G per substitutionem ipsi S adiunctam, G autem in F per substitutionem ex transpositione ipsius S oriundam. Numerum $\alpha\mathfrak{G}'\gamma'' + \alpha'\mathfrak{G}''\gamma + \alpha''\mathfrak{G}\gamma' - \alpha''\mathfrak{G}'\gamma - \alpha\mathfrak{G}''\gamma' - \alpha'\mathfrak{G}\gamma''$, qui esse debebit vel $= +1$ vel $= -1$, denotabimus per k. Quibus ita factis, obseruamus

I. Si fiat $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\mathfrak{G}'' = 0$, $\gamma'' = 1$, fore

$$m = a\alpha\alpha + 2b''\alpha\alpha' + a'\alpha'\alpha'$$
$$m' = a\gamma\gamma + 2b''\gamma\gamma' + a'\gamma'\gamma'$$
$$m'' = a''; \; n = b\gamma' + b'\gamma; \; n' = b\alpha' + b'\alpha$$
$$n'' = a\alpha\gamma + b''(\alpha\gamma' + \gamma\alpha') + a'\alpha'\gamma'$$

Praeterea esse debebit $\alpha\gamma' - \gamma\alpha'$ vel $= +1$ vel $= -1$. Hinc manifestum est, formam binariam (a, b'', a'), cuius determinans est A'', transmutari per substitutionem $\alpha, \gamma; \alpha'; \gamma'$ in formam binariam (m, n'', m') determinantis M'', et proin ipsi aequiualere propter $\alpha\gamma' - \gamma\alpha' = \pm 1$, vnde erit $M'' = A''$, quod etiam directe facile confirmatur. Nisi itaque (a, b'', a') iam est forma simplicissima in classe sua, ipsos α, γ, α', γ' ita determinare licebit, vt (m, n'', m') sit forma simplicior; et quidem e theoria aequiualentiae formarum binariarum facile concluditur, hoc ita fieri posse, vt m non sit maior quam $\sqrt{-\frac{4}{3}A''}$, si A'' fuerit negatiuus, vel non maior quam $\sqrt{A''}$, si A'' fuerit positiuus, vel $m = 0$ si $A'' = 0$, ita vt in omnibus casibus valor (absolutus) ipsius m certe vel saltem vsque ad $\sqrt{\pm\frac{4}{3}A''}$ deprimi possit. Hoc itaque modo forma f ad aliam reducitur coëfficientem primum, si fieri potest, minorem habentem, et cuius forma adiuncta coëfficientem tertium eundem habet vt forma F ipsi f adiuncta. In hoc consistit *reductio prima.*

II. Si vero fit $\alpha = 1$, $\gamma = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, erit $k = \gamma'\gamma'' - \gamma''\gamma' = +1$; substitutio itaque ipsi S adiuncta erit

$$\pm \begin{matrix} 1, & 0, & 0 \\ 0, & \gamma'', & -\xi'' \\ 0, & -\gamma', & \xi' \end{matrix}$$

per quam F transibit in G. Habebitur itaque

$$m = a,\ n' = b'\gamma'' + b''\gamma',\ n'' = b'\xi'' + b''\xi'$$
$$m' = a'\xi'\xi' + 2b\xi'\xi'' + a''\xi''\xi''$$
$$m'' = a'\gamma'\gamma' + 2b\gamma'\gamma'' + a''\gamma''\gamma''$$
$$n = a'\xi'\gamma' + b(\xi'\gamma'' + \gamma'\xi'') + a''\xi''\gamma''$$
$$M' = A'\gamma''\gamma'' - 2B\gamma'\gamma'' + A''\gamma'\gamma'$$
$$N = -A'\xi''\gamma'' + B(\xi'\gamma'' + \gamma'\xi'') - A''\xi'\gamma'$$
$$M'' = A'\xi''\xi'' - 2B\xi'\xi'' + A''\xi'\xi'$$

Hinc patet, formam binariam (A'', B, A'), cuius determinans est Da, transire per substitutionem $\xi', -\gamma', -\xi'', \gamma''$ in formam (M'', N, M') determinantis Dm, adeoque (propter $\xi'\gamma'' - \gamma'\xi'' = \pm 1$, vel propter $Da = Dm$) ipsi aequiualere. Nisi itaque (A'', B, A') iam est forma simplicissima classis suae, coëfficientes $\xi', \gamma', \xi'', \gamma''$ ita determinari poterunt, vt (M'', N, M') sit simplicior, et quidem hoc semper poterit fieri ita, vt M'' sine respectu signi non sit maior quam $\sqrt{\pm \frac{4}{3} Da}$. Hoc itaque modo forma f reducitur ad aliam coëfficientem primum eundem habentem, sed cuius forma adiuncta coëfficientem tertium si fieri potest minorem habeat quam forma F ipsi f adiuncta. In hoc consistit *reductio secunda.*

III. Si itaque f est forma ternaria, ad quam neque reductio prima neque secunda est applica-

bilis, i. e. quae per neutram in formam simpliciorem transmutari potest: necessario erit tum $aa < \text{vel} = \frac{4}{3}A$, tum $AA < \text{vel} = \frac{4}{3}aD$ sine respetu signi. Hinc a^4 erit $< \text{vel} = \frac{16}{9}AA$, adeoque $a^4 < \text{vel} = \frac{64}{27}aD$, $a^3 < \text{vel} = \frac{64}{27}D$, et $a < \text{vel} = \frac{4}{3}\sqrt[3]{D}$; hinc rursus $AA < \text{vel} = \frac{16}{9}\sqrt[3]{D^4}$ atque $A < \text{vel} = \frac{4}{3}\sqrt[3]{D^2}$. Quamobrem quamdiu a vel A hos limites adhuc superant, necessario vna aut altera reductionum praecedentium ad formam f applicari poterit. — Ceterum haec conclusio non est conuertenda, quum vtique saepius accidat, vt forma ternaria, cuius coëfficiens primus, atque coëfficiens tertius formae adiunctae iam sunt infra illos limites, nihilominus per vnam alteramue reductionem adhuc simplicior reddi possit.

IV. Quodsi vero ad formam ternariam quamcunque datam determinantis D alternis vicibus reductio prima et secunda applicantur, i. e. ad ipsam prima vel secunda, ad eam quae hinc resultat secunda vel prima, ad eam quae hinc prouenit iterum prima vel secunda etc., manifestum est, tandem necessario ad formam peruentum iri, ad quam neutra amplius applicari possit. Quum enim magnitudo absoluta tum coëfficientium primorum formarum hoc modo prodeuntium, tum coëfficientium tertiorum formarum illis adiunctarum continuo alternis vicibus eadem maneat atque decrescat, hic progressus necessario tandem alicubi finietur, quia alioquin duae series infinitae numerorum continuo decrescentium haberentur. Hinc iam nacti sumus egregium theorema: *Quaeuis forma ternaria deter-*

minantis D reduci potest ad aliam aequiualentem, cuius coëfficiens primus non sit maior quam $\frac{4}{3}\sqrt[3]{D}$, *atque coëfficiens tertius formae ipsi adiunctae non maior quam* $\frac{4}{3}\sqrt[3]{D^2}$ *sine respectu signi, siquidem forma proposita his proprietatibus ipsa nondum est praedita.* — Ceterum loco coëfficientis primi formae f atque tertii formae ipsi f adiunctae prorsus simili modo tractare potuissemus vel coëfficientem primum formae ipsius et secundum adiunctae; vel secundum formae ipsius et primum vel tertium adiunctae; vel tertium formae ipsius et primum vel secundum adiunctae, quibus viis perinde ad finem nobis propositum peruenieremus: sed e re est, methodo vni constanter adhaerere, quo facilius operationes huc pertinentes ad algorithmum fixum reduci possint. Denique obseruamus, duobus coëfficientibus, quos infra limites fixos deprimere docuimus, limites adhuc minores constitui posse, si formae definitae ab indefinitis separentur; hoc vero ad institutum praesens non est necessarium.

273. Ecce iam quaedam exempla, per quae praecepta praecedentia magis illustrabuntur.

Ex. 1. Sit $f = \begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$, eritque $F = \begin{pmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{pmatrix}$, $D = -1$. Quum (19, 1, 21) sit forma binaria reducta, cui alia, termini primi minoris quam 19, non aequiualet, reductio prima hic non est applicabilis; forma binaria $(A'', B, A') = (-398, 257, -166)$ autem per theoriam aequiualentiae formarum binariarum

in simpliciorem aequiualentem $(-2, 1, -10)$ transmutabilis inuenitur, in quam transit per substitutionem 2, 7, 3, 11. Faciendo itaque $\beta' = 2$, $\gamma' = -7$, $\beta'' = -3$, $\gamma'' = 11$, applicanda erit ad formam f substitutio

$$\begin{matrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11 \end{matrix}$$

per quam inuenitur transire in hanc $\begin{pmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{pmatrix} \ldots f'$. Coëfficiens tertius formae, huic adiunctae, est -2, quo respectu f' simplicior est censenda quam f.

Ad formam f' applicari potest reductio prima. Scilicet quum forma binaria $(19, -82, 354)$ transmutetur in $(1, 0, 2)$ per substitutionem 13, 4, 3, 1: applicanda erit ad formam f substitutio

$$\begin{matrix} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}$$

per quam transit in hanc $\begin{pmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{pmatrix} \ldots f''$

Ad formam f'', cui adiuncta est $\begin{pmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{pmatrix}$, denuo applicari potest reductio secunda. Scilicet $(-2, -95, -4513)$ transit per substitutionem $47, 1, -1, 0$ in $(-1, 1, -2)$; quamobrem ad f'' applicanda erit substitutio

$$\begin{matrix} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0 \end{matrix}$$

per quam transit in $\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}$ . . . f'''. Huius coëfficiens primus per reductionem primam amplius diminui non potest, neque formae, ipsi adiunctae, tertius per secundam.

Ex. 2. Proposita sit forma $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ ... f, cui adiuncta est $\begin{pmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{pmatrix}$ et cuius determinans $= 2$. Hic successiue reperiuntur, applicando alternatim reductionem secundam et primam,

substitutiones	per quas transit	in
$\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{matrix}$	f	$\begin{pmatrix} 10, & 2, & 2 \\ -1, & 0, & 4 \end{pmatrix} = f'$
$\begin{matrix} 0, & -1, & 0 \\ 1, & -2, & 0 \\ 0, & 0, & 1 \end{matrix}$	f'	$\begin{pmatrix} 2, & 2, & 2 \\ 2, & -1, & 0 \end{pmatrix} = f''$
$\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 2, & -1 \end{matrix}$	f''	$\begin{pmatrix} 2, & 2, & 2 \\ -2, & 1, & -2 \end{pmatrix} = f'''$
$\begin{matrix} 1, & 0, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}$	f'''	$\begin{pmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{pmatrix} = f^{IV}$

Forma f^{IV} per reductionem primam vel secundam vlterius deprimi nequit.

274. Quando forma ternaria habetur, cuius coëfficiens primus, atque formae adiunctae tertius, quantum fieri potest per methodos praecedentes sunt depressi: methodus sequens reductionem vlteriorem suppeditat.

Adhibendo signa eadem vt in art. 272, et ponendo $\alpha = 1$, $\alpha' = 0$, $\xi' = 1$, $\alpha'' = 0$, $\xi'' = 0$, $\gamma'' = 1$, i. e. adhibendo substitutionem

$$\begin{matrix} 1, & \xi, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1 \end{matrix}$$

erit $m = a$, $m' = a' + 2b''\xi + a\xi\xi$, $m'' = a'' + 2b\gamma' + 2b'\gamma + a\gamma\gamma + 2b''\gamma\gamma' + a'\gamma'\gamma'$, $n = b + a'\gamma' + b'\xi + b''(\gamma + \xi\gamma') + a\xi\gamma$, $n' = b' + a\gamma + b''\gamma'$, $n'' = b'' + a\xi$; praeterea $M'' = A''$, $N = B - A''\gamma'$, $N' = B' - N\xi - A''\gamma$. Per talem itaque substitutionem coëfficientes a, A'', qui per reductiones praecedentes diminuti sunt, non mutantur; quamobrem negotium in eo versatur, vt per idoneam determinationem ipsorum ξ, γ, γ' depressiones in coëfficientibus reliquis obtineantur. Ad hunc finem obseruamus primo, si fuerit $A'' = 0$, supponi posse, esse etiam $a = 0$; si enim a non $= 0$, reductio prima adhuc semel applicabilis foret, quum cuiuis formae binariae determinantis 0 aequiualeat forma talis $(0, 0, h)$, siue cuius terminus primus $= 0$ (V. art. 215). Prorsus simili ratione supponere licet,

esse etiam $A'' = 0$, si fuerit $a = 0$, ita vt vel neuter numerorum a, A'' sit 0 vel vterque.

In casu priori manifestum est, ipsos ξ, γ, γ' ita determinari posse, vt sine respectu signi n'', N, N' resp. non sint maiores quam $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$. Ita in exemplo primo art. praec. transibit forma postrema $\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}$, cui adiuncta est $\begin{pmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{pmatrix}$, per substitutionem

$$\begin{matrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{matrix}$$

in hanc $\begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ ... f^{IV}, cui adiuncta est $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$.

In casu posteriori, vbi $a = A'' = 0$, adeoque etiam $b'' = 0$, erit $m = 0$, $m' = a'$, $m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'\gamma'$, $n = b + a'\gamma' + b'\xi$, $n' = b'$, $n'' = 0$. Erit itaque $D = -a'b'b' = -m'n'n'$; perspicieturque facile, ξ et γ' ita determinari posse, vt n fiat aequalis residuo absolute minimo ipsius b secundum modulum qui est diuisor communis maximus ipsorum a', b', i. e. vt n fiat non maior quam semissis huius diuisoris sine respectu signi, adeoque $n = 0$, quoties a', b' inter se sunt primi. Ipsis ξ, γ' in hunc modum determinatis, valor ipsius γ ita accipi poterit, vt m'' non sit maior quam b' sine respectu signi; hoc quidem impossibile esset

quando $b' = 0$; tunc vero foret $D = 0$, quem casum exclusimus. Ita fit pro forma postrema in ex. 2 art. praec. $n = -2 - \zeta + 2\gamma'$, vnde statuendo $\zeta = -2$, $\gamma' = 0$, fit $n = 0$, porro $m'' = 2 - 2\gamma$, et ponendo $\gamma = 1$, $m'' = 0$. Habemus itaque substitutionem

$$\begin{matrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}$$

per quam forma illa transit in $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix} \ldots f^{V}$.

275. Si habetur series formarum ternariarum aequiualentium f, f', f'', f'''. etc., atque transformationes cuiusuis harum formarum in sequentem: ex transformationibus formae f in f', formaeque f' in f'' per art. 270 deducitur transformatio formae f in f''; ex hac atque transf. formae f'' in f''' sequitur transf. formae f in f''' etc., manifestoque hoc pacto transformatio formae f in quamcunque aliam seriei inueniri poterit. Et quum ex transformatione formae f in quamcunque aliam aequiualentem g deduci possit transformatio formae g in f (S'' ex S artt. 268, 269), hoc modo erui poterit transformatio cuiuslibet formae seriei f', f'' etc. in primam f. — Ita pro formis exempli primi art. praec inueniuntur substitutiones

$$\begin{matrix} 13, & 4, & 0 \\ 6, & 2, & -7 \\ -9, & -3, & 11 \end{matrix} \quad \begin{matrix} 13, & 188, & -4 \\ 6, & 87, & -2 \\ -9, & -130, & 3 \end{matrix} \quad \begin{matrix} 13, & -20, & 16 \\ 6, & -9, & 7 \\ -9, & 14, & -11 \end{matrix}$$

per quas f transit in f'', f''' f^{IV} resp., et ex subst. vltima haec

$$\begin{matrix} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3 \end{matrix}$$

per quam f^{IV} transit in f. Simili modo pro ex. 2 art. praec. prodeunt substitutiones

$$\begin{matrix} 1, & -1, & 1 \\ -3, & 4, & -3 \\ 10, & -14, & 11 \end{matrix} \quad \left| \quad \begin{matrix} 2, & -3, & -1 \\ 3, & 1, & 0 \\ 2, & 4, & 1 \end{matrix} \right.$$

per quas resp. transit forma $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0 & 4 \end{pmatrix}$ in $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$, atque haec in illam.

276. Theorema. *Classium, in quas omnes formae ternariae determinantis dati distribuuntur, multitudo semper est finita.*

Dem. I. Multitudo omnium formarum $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ determinantis dati D, in quibus $a = 0$, $b'' = 0$, b non maior quam semissis diuisoris comm. max. numerorum a', b'; a'' non maior quam b', manifesto est finita. Quoniam enim esse debet $a'b'b' = D$, pro b' alii valores accipi nequeunt, quam $+1$, -1 atque radices quadratorum ipsum D metientium (si quae alia praeter 1 dantur) signo positiuo et negatiuo affectae, quorum valorum multitudo finita est. Pro singulis autem valoribus ipsius b' valor ipsius

a' est determinatus, ipsorumque b, a'' valores manifesto limitantur ad multitudinem finitam.

II. Simili modo finita est multitudo omnium formarum $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ determinantis D, in quibus a non $= 0$, neque maior quam $\frac{4}{3}\sqrt[3]{\pm D}$; $b''b'' - aa' = A''$ non $= 0$ neque maior quam $\frac{4}{3}\sqrt[3]{D^2}$; b'' non maior quam $\frac{1}{2}a$; $ab - b'b'' = B$ et $a'b' - bb'' = B'$ non maiores quam $\frac{1}{2}A''$. Nam multitudo omnium combinationum valorum ipsorum a, b'', A'', B, B' finita erit; his vero singulis determinatis, etiam formae coëfficientes reliqui a', b, b', a'', coëfficientesque formae adiunctae $bb - a'a'' = A$, $b'b' - aa'' = A'$, $a''b'' - bb' = B''$ determinati erunt per aequationes hasce: $a' = \frac{b''b'' - A''}{a}$, $A' = \frac{BB - aD}{A''}$, $A = \frac{B'B' - a'D}{A''}$, $B'' = \frac{BB' + b''D}{A''}$, $b = \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}$, $b' = \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}$, $a'' = \frac{b'b' - A'}{a} = \frac{bb - A}{a'} = \frac{bb' + B''}{b''}$. Iam quum omnes illae formae obtineantur, eligendo e cunctis combinationibus valorum ipsorum a, b'', A'', B, B' eas, e quibus etiam a', a'', b, b' valores integros nanciscuntur, illarum multitudo manifesto erit finita.

III. Cunctae itaque formae in I et II multitudinem finitam classium constituunt, quae etiam formarum ipsarum multitudine minor esse poterit, si quae ex ipsis inter se sunt aequivalen-

tes. Iam quum per disquisitiones praecedentes quaeuis forma ternaria determinantis D alicui ex illis formis necessario aequiualeat, i. e. ad aliquam e classibus quas hae formae constituunt pertineat: hae classes omnes formas det. D complectentur, i. e. omnes formae ternariae det. D in multitudinem finitam classium distribuentur. *Q. E. D.*

277. Regulae, per quas omnes formae in I et II art. praec. erui possunt, ex ipsarum explicatione sponte defluunt; quare sufficiet quaedam exempla apposuisse. Pro $D = 1$, formae I hae sex (per ambiguitatem signorum) prodeunt $\begin{pmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$; in formis II a et A'' alios valores quam $+1$ et -1 habere nequeunt, pro singulis quatuor combinationum hinc oriundarum b'', B et B' poni debent $= 0$, vnde emergunt quatuor formae $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$. Simili modo pro $D = -1$ sex forma I quatuorque II habentur, $\begin{pmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & -1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$. Pro $D = 2$ sex formae I proueniunt $\begin{pmatrix} 0, & 2, & 0 \\ 0, & \pm 0 & \end{pmatrix}$, $\begin{pmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, octoque formae II, $\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 2 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{pmatrix}$.

Ceterum multitudo classium ex his formis in his tribus casibus prodeuntium formarum multitudine multo minor est. Scilicet facile confirmatur

I. Formam $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ transire in $\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}$, $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ resp. per substitutiones

$$\begin{array}{l|l|l|l} 1, 0, 0 & 0, 0, 1 & 0, 0, 1 & 1, 0, -1 \\ 0, 1, 0 & 0, 1, -1 & 0, 1, 1 & 1, 1, -1 \\ 0, 0, -1 & \pm 1, 1, 0 & \pm 1, -1, -1 & 0, -1, 1 \end{array}$$

formam $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ autem in $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ per solam indeterminatarum permutationem. Quare illae decem formae ternariae det. 1 ad has duas reducuntur $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$; pro priori, si magis arridet, etiam haec $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ accipi potest. Quum forma prior indefinita sit, posterior definita, manifestum et quamuis formam ternariam indefinitam det. 1 aequiualere formae $xx + 2yz$, quamuis definitam huic $-xx - yy - zz$.

II. Prorsus simili modo inuenitur, quamlibet formam ternariam indefinitam determinantis — 1 aequiualere formae — xx

$+ 2yz$, quamlibet definitam huic $xx + yy + zz$.

III. Pro determinante 2 ex octo formis (II) statim reiici possunt secunda, sexta et septima, quippe quae ex prima per solam indeterminatarum permutationem oriuntur, similique ratione etiam quinta quae e tertia, et octaua quae e quarta perinde proueniunt; tres reliquae, cum sex formis I, tres classes constituunt; scilicet $\begin{pmatrix} 0, 2, 0 \\ 0, 1, 0 \end{pmatrix}$ transit in $\begin{pmatrix} 0, 2, 0 \\ 0, -1, 0 \end{pmatrix}$ per substitutionem

$$\begin{matrix} 1, 0, 0 \\ 0, 1, 0 \\ 0, 0, -1 \end{matrix}$$

formaque $\begin{pmatrix} 1, 1, -2 \\ 0, 0, 0 \end{pmatrix}$ in $\begin{pmatrix} 0, 2, 1 \\ 0, 1, 0 \end{pmatrix}$, $\begin{pmatrix} 0, 2, 1 \\ 0, -1, 0 \end{pmatrix}$, $\begin{pmatrix} 0, 2, -1 \\ 0, 1, 0 \end{pmatrix}$, $\begin{pmatrix} 0, 2, -1 \\ 0, -1, 0 \end{pmatrix}$, $\begin{pmatrix} 1, -1, 2 \\ 0, 0, 0 \end{pmatrix}$ resp. per substitutiones

1, 0, 1	1, 0, −1	1, 0, 0	1, 0, 0	1, 0, 0
1, 2, 0	1, 2, 0	1, 2, −1	1, 2, 1	0, 1, 2
1, 1, 0	1, 1, 0	1, 1, −1	1, 1, 1	0, 1, 1

Quaeuis itaque forma ternaria determinantis 2 ad aliquam ex his tribus est reducibilis $\begin{pmatrix} 0, 2, 0 \\ 0, 1, 0 \end{pmatrix}$, $\begin{pmatrix} 1, 1, -2 \\ 0, 0, 0 \end{pmatrix}$, $\begin{pmatrix} -1, -1, -2 \\ 0, 0, 0 \end{pmatrix}$; loco primae si magis placet etiam $\begin{pmatrix} 2, 0, 0 \\ 1, 0, 0 \end{pmatrix}$ accipi potest. Ma-

nifesto autem quaeuis forma ternaria definita necessario aequiualebit tertiae $-xx-yy-2zz$, quum duae priores sint indefinitae; quaeuis indefinita primae vel secundae, et quidem primae $2xx+2yz$, si ipsius coëfficiens primus, secundus et tertius simul sunt pares (quoniam facile perspicitur, talem formam per substitutionem quamcunque in similem formam transire, adeoque formae secundae aequiualere non posse), secundae $xx+yy-2zz$ autem, si ipsius coëfficiens primus, secundus et tertius non simul pares sunt, sed vnus, duo omnesue impares (in talem enim formam ex simili ratione forma prima $2xx+2yz$ per nullam substitutionem transformabilis esse poterit).

Quod igitur in exemplis artt. 273, 274 euenit, vt forma definita $\begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$ determinantis -1 ad hanc $xx+yy+zz$, atque forma indefinita $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ determinantis 2 ad $2xx-2yz$ siue (quod eodem redit) ad $2xx+2yz$ reduceretur, per disquisitiones praecedentes a priori praeuideri potuisset.

278. Per formam ternariam, cuius indeterminatae sunt x, x', x'', *repraesentantur* tum numeri, tribuendo ipsis x, x', x'' valores determinatos, tum formae binariae per huiusmodi substitutiones $x = mt+nu$, $x' = m't+n'u$, $x'' = m''t+n''u$, designantibus m, n, m' etc. numeros determinatos; t, u indeterminatas formae repraesentatae. Ad theoriam itaque completam formarum ternariarum requireretur solutio se-

quentium problematum: I. Inuenire omnes repraesentationes numeri dati per formam ternariam datam. II. Inuenire omnes repraesentationes formae binariae datae per ternariam datam. III. Diiudicare, vtrum duae formae ternariae datae eiusdem determinantis aequiualentes sint, necne, et in casu priori omnes transformationes alterius in alteram inuenire. IV. Diiudicare, vtrum forma ternaria data aliam datam determinantis maioris implicet, necne, et in casu priori omnes transformationes illius in hanc assignare. De quibus problematibus longe difficilioribus quam analoga in formis binariis alio loco pluribus agemus: hic disquisitionem nostram restringimus ad ostendendum, quomodo problema primum ad secundum secundumque ad tertium reduci possit; tertium vero pro casibus quibusdam simplicissimis formarumque binariarum theoriam imprimis illustrantibus soluere docebimus; quartum hic omnino excludemus.

279. Lemma. *Propositis tribus numeris integris quibuscunque* a, a', a'' (*qui tamen non omnes simul* $= 0$): *inuenire sex alios* B, B', B'', C, C', C'' *ita comparatos vt fiat* $B'C'' - B''C' = a$, $B''C - BC'' = a'$, $BC' - B'C = a''$.

Sol. Sit α diu. comm. max. ipsorum a, a', a'', accipianturque integri A, A', A'' ita vt fiat $Aa + A'a' + A''a'' = \alpha$. Porro accipiantur tres integri $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$ ad lubitum ea sola conditione, vt tres numeri $\mathfrak{C}'A'' - \mathfrak{C}''A'$, $\mathfrak{C}''A - \mathfrak{C}A''$, $\mathfrak{C}A' - \mathfrak{C}'A$, quos resp. per b, b', b'' ipsorumque diuisorem communem maximum per $\mathfrak{G}$

designabimus, non fiant simul = 0. Tunc ponatur $a'b'' - a''b' = \alpha\mathfrak{E}C$, $a''b - ab'' = \alpha\mathfrak{E}C'$, $ab' - a'b = \alpha\mathfrak{E}C''$, patetque ipsos C, C', C'' fore integros. Denique accipiendo integros $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ ita vt fiat $\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \mathfrak{C}$, ponendo $\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = \alpha h$, et statuendo $B = \alpha\mathfrak{B} - hA$, $B' = \alpha\mathfrak{B}' - hA'$, $B'' = \alpha\mathfrak{B}'' - hA''$, hi valores ipsorum B, B', B'', C, C', C'' aequationibus praescriptis satisfacient.

Inuenitur enim $aB + a'B' + a''B'' = 0$, $bA + b'A' + b''A'' = 0$, vnde $bB + b'B' + b''B'' = \alpha\mathfrak{E}$. Iam ex valoribus ipsorum C', C'' fit $\alpha\mathfrak{E}(B'C'' - B''C') = ab'B' - a'bB' - a''bB'' + ab''B'' = a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\mathfrak{E}a$, adeoque $B'C'' - B''C' = a$; similique modo inuenitur $B''C - BC'' = a'$, $BC' - B'C = a''$. *Q. E. F.* — Ceterum analysis per quam haec solutio inuenta est, nec non methodus ex vna solutione omnes inueniendi, hic sunt supprimendae.

280. Supponamus, formam binariam $att + 2btu + cuu \ldots \Phi$, cuius determinans = D, repraesentari per formam ternariam f cuius indeterminatae x, x', x'', ponendo $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$, ipsique f adiunctam esse formam F, cuius indeterminatae X, X', X''. Tunc per calculum facile confirmatur (designando coëfficientes formarum f, F per literas peculiares) siue etiam ex art. 268. II. protinus deducitur, numerum D repraesentari per F ponendo $X = m'n'' - m''n'$, $X' = m''n - mn''$, $X'' = mn' - m'n$, quae repraesentatio numeri

D repraesentationi formae Φ per f *adiuncta* commode dici potest. Si valores ipsarum X, X', X'' diuisorem communem non habent, breuitatis caussa hanc repraesentationem ipsius D *propriam* vocabimus, sin secus *impropriam*, easdem denominationes etiam repraesentationi formae Φ per f, cui illa repraes. ipsius D adiuncta est, tribuemus. Iam inuentio omnium repraesentationum propriarum numeri D per formam F sequentibus momentis innititur:

I. Nulla repraesentatio ipsius D per F datur, quae non ex aliqua repraesentatione alicuius formae determinantis D per formam f deduci possit, i. e. tali repraesentationi adiuncta sit.

Sit enim repraesentatio quaecunque ipsius D per F haec: $X = L$, $X' = L'$, $X'' = L''$; accipiantur per lemma art. praec. m, m', m'', n, n', n'' ita vt fiat $m'n'' - m''n' = L$, $m''n - mn'' = L'$, $mn' - m'n = L''$, transeatque f per substitutionem $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$ in formam binariam $\Phi = att + 2btu + cuu$. Tunc facile perspicietur, D fore determinantem formae Φ ipsiusque repraesentationi per f repraesentationem propositam ipsius D per F adiunctam.

Ex. Sit $f = xx + x'x' + x''x''$, adeoque $F = -XX - X'X' - X''X''$; $D = -209$, ipsiusque repraesentatio per F haec $X = 1$, $X' = 8$, $X'' = 12$; hinc inueniuntur valores ipsorum m, m', m'', n, n', n'' hi -20, 1, 1, -12, 0, 1 resp., atque $\Phi = 402\,tt + 482\,tu + 145\,uu$.

II. Si Φ, χ sunt formae binariae proprie aequiualentes, quaeuis repraesentatio ipsius D per F alicui repraesentationi formae Φ per f adiuncta, etiam alicui repraesentationi formae χ per f adiuncta erit.

Sint p, q indeterminatae formae χ; transeat Φ in χ per substitutionem propriam $t = \alpha p + \gamma q$, $u = \beta p + \delta q$, sitque aliqua repraesentatio formae Φ per f haec $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u \ldots (R)$. Tunc nullo negotio perspicitur, si ponatur $\alpha m + \gamma n = g$, $\alpha m' + \gamma n' = g'$, $\alpha m'' + \gamma n'' = g''$, $\beta m + \delta n = h$, $\beta m' + \delta n' = h'$, $\beta m' + \delta n' = h'$, $\beta m'' + \delta n'' = h''$, formam χ repraesentatum iri per f statuendo $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q \ldots (R')$, calculoque facto inuenitur (propter $\alpha\delta - \beta\gamma = 1$) esse $g'h'' - g''h' = m'n'' - m''n'$, $g''h - gh'' = m''n - mn''$, $gh' - g'h = mn' - m'n$, i. e. repraesentationibus R, R' eadem repraesentatio ipsius D per F adiuncta est.

Ita in ex. praec. formae Φ aequiualere inuenitur inuenitur $\chi = 13pp - 10pq + 18qq$, in quam illa transit per substitutionem propriam $t = -3p + q$, $u = 5p - 2q$; hinc inuenitur repraesentatio formae χ per f haec $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$, ex qua eadem numeri -209 repraesentatio deducitur, a qua profecti eramus.

III. Denique si duae formae binariae Φ, χ determinantis D, quarum indeterminatae sunt t, u; p, q, per f repraesentari possunt, alicuique repraesentationi vnius eadem repraesentatio propria ipsius D

per F adiuncta est, atque alicui repraesentationi alterius, illae formae necessario erunt proprie aequivalentes. Supponamus Φ repraesentari per f ponendo $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$; χ vero statuendo $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''p$, atque esse $m'n'' - m''n' = g'h'' - g''h' = L$, $m''n - mn'' = g''h - gh'' = L'$, $mn' - m'n = gh' - g'h = L''$. Accipiantur integri l, l', l'' ita vt fiat $Ll + L'l' + L''l'' = 1$, ponaturque $n'l'' - n''l' = M$, $n''l - nl'' = M'$, $nl' - n'l = M''$, $l'm'' - l''m' = N$, $l''m - lm'' = N'$, $lm' - l'm = N''$; denique statuatur $gM + g'M' + g''M = \alpha$, $hM + h'M' + h''M'' = \mathfrak{G}$, $gN + g'N' + g''N'' = \gamma$, $hN + h'N' + h''N'' = \delta$. Hinc facile deducitur

$$\alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g$$
$$\mathfrak{G}m + \delta n = h - l(hL + h'L' + h''L'') = h$$

similique modo $\alpha m' + \gamma n' = g'$, $\mathfrak{G}m' + \delta n' = h'$, $\alpha m'' + \gamma n'' = g''$, $\mathfrak{G}m'' + \delta n'' = h''$. Hinc patet $mt + nu$, $m't + n'u$, $m''t + n''u$ transire per substitutionem $t = \alpha p + \mathfrak{G}q$, $u = \gamma p + \delta q$ ... (S) in $gp + hq$, $g'p + h'q$, $g''p + h''q$ resp., vnde manifestum est, Φ transire per substitutionem S in eandem formam, in quam f transeat ponendo $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q$, adeoque in formam χ, cui itaque aequivalet. Denique per substitutiones debitas facile inuenitur $\alpha\delta - \mathfrak{G}\gamma = Ll + L'l' + L''l'' = 1$, quocirca substitutio S est propria, formaeque Φ, χ proprie aequivalentes.

Ex his obseruationibus deriuantur regulae sequentes ad inueniendum omnes repraesentationes proprias ipsius D per F: Euoluantur omnes classes formarum binariarum determinantis D, et ex singulis vna forma ad libitum eligatur; quaerantur omnes repraesentationes propriae singularum harum formarum per f (reiectis iis quae forte per f repraesentari nequeunt), et ex singulis hisce repraesentationibus deducantur repraesentationes numeri D per F. Ex I et II manifestum est, hoc modo omnes repraesentationes proprias possibiles obtineri, adeoque solutionem esse completam; ex III, transformationes formarum e classibus diuersis certo producere repraesentationes diuersas.

281. Inuestigatio repraesentationum *improprìarum* numeri dati D per formam F ad casum praecedentem facile reducitur. Scilicet manifestum est, si D per nullum quadratum (praeter 1) diuisibilis sit, tales repraesentationes omnino non dari; sin secus, metientibus ipsum D quadratis $\lambda\lambda$, $\mu\mu$, $\nu\nu$ etc., omnes repraesentationes improprias ipsius D per F inueniri, si omnes repraesentationes propriae numerorum $\frac{D}{\lambda\lambda}$, $\frac{D}{\mu\mu}$, $\frac{D}{\nu\nu}$ etc. per eandem formam euoluantur, indeterminatarumque valores per λ, μ, ν etc. resp. multiplicentur.

Hoc itaque modo inuentio omnium repraesentationum numeri dati per formam ternariam datam, *quae alicui formae ternariae adiuncta est*, a problemate secundo pendet; ad hunc vero casum, qui primo aspectu minus late patere videri

posset, reliqui ita reducuntur. Sit D numerus repraesentandus per formam $\left(\begin{smallmatrix} g, g', g'' \\ h, h', h'' \end{smallmatrix}\right)$, cuius determinans Δ, et cui adiuncta est forma $\left(\begin{smallmatrix} G, G', G'' \\ H, H', H'' \end{smallmatrix}\right) = f$. Tunc huic rursus adiuncta erit $\left(\begin{smallmatrix} \Delta g, \Delta g', \Delta g'' \\ \Delta h, \Delta h', \Delta h'' \end{smallmatrix}\right) = F$, patetque, repraesentationes numeri ΔD per F (quarum inuestigatio a praecc. pendet) omnino identicas esse cum repraesentationibus numeri D per formam propositam. — Ceterum quando omnes coëfficientes formae f diuisorem communem μ habent, perspicuum est, omnes coëfficientes formae F diuisibiles esse per $\mu\mu$, quocirca etiam ΔD per $\mu\mu$ diuisibilis esse debebit (alioquin nullae repraesentationes darentur); repraesentationesque numeri D per formam propositam coincident cum repraesentationibus numeri $\frac{\Delta D}{\mu\mu}$ per formam quae oritur ex F, diuidendo singulos coëfficientes per $\mu\mu$, cui formae adiuncta erit ea, quae oritur ex f, diuidendo singulos coëfficientes per μ.

Denique obseruamus, hanc problematis primi solutionem in vnico casu, vbi $D = 0$, non esse applicabilem; hic enim omnes formae binariae determinantis D in multitudinem finitam classium non distribuuntur; infra autem hunc casum ex aliis principiis soluemus.

282. Inuestigatio repraesentationum formae binariae datae cuius determinans non $= 0$*) per

*) Hunc casum per methodum aliquantum diuersam tractandum hoc loco breuitatis caussa praeterimus.

ternariam datam pendet ab obseruationibus sequentibus:

I. Ex quauis repraesentatione propria formae binariae $(p, q, r) = \Phi$ determinantis D per ternariam f determinantis Δ deduci possunt integri B, B' tales vt sit $BB \equiv \Delta p$, $BB' \equiv -\Delta q$, $B'B' \equiv \Delta q \pmod{D}$, i. e. valor expressionis $\sqrt{\Delta}\,(p, -q, r) \pmod{D}$. Habeatur repraesentatio propria formae Φ per f haec $x = \alpha t + \mathfrak{C} u$, $x' = \alpha' t + \mathfrak{C}' u$, $x'' = \alpha'' t + \mathfrak{C}'' u$, (designantibus x, x', x''; t, u indeterminatas formarum f, Φ); accipiantur integri γ, γ', γ'' ita vt $(\alpha'\mathfrak{C}'' - \alpha''\mathfrak{C}')\gamma + (\alpha\mathfrak{C}'' - \alpha''\mathfrak{C})\gamma' + (\alpha\mathfrak{C}' - \alpha'\mathfrak{C})\gamma'' = k$ fiat vel $= +1$ vel $= -1$, transeatque f per substitutionem

$$\begin{matrix} \alpha, & \mathfrak{C}, & \gamma \\ \alpha', & \mathfrak{C}', & \gamma' \\ \alpha'', & \mathfrak{C}'', & \gamma'' \end{matrix}$$

in formam $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} = g$, cui adiuncta sit $\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} = G$. Tunc manifestum est, fore $a = p$, $b'' = q$, $a' = r$, $A'' = D$, atque Δ determinantem formae g; vnde $BB = \Delta p + A'D$, $BB' = -\Delta q + B''D$, $B'B' = \Delta r + AD$. — Ita *e. g.* forma $19tt + 6tu + 41uu$ repraesentatur per $xx + x'x' + x''x''$ ponendo $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$; vnde statuendo $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$, eruitur $B = -171$, $B' = 27$, siue valor $(-171, 27)$ expr. $\sqrt{-1}\,(19, -3, 41) \pmod{770}$.

Hinc iam sequitur, si $\Delta\ (p, -q, r)$ non sit residuum quadratum ipsius D, φ per nullam formam ternariam determinantis Δ proprie repraesentabilem esse posse; in eo itaque casu vbi Δ, D inter se primi sunt, Δ numerus characteristicus formae φ esse debebit.

II. Quum γ, γ', γ'' infinite multis modis diuersis determinari possint, etiam alii atque alii valores ipsorum B, B' inde prodibunt, qui quem nexum inter se habeant videamus. Ponamus, etiam δ, δ', δ'' ita comparatos esse, vt $(\alpha'\mathfrak{C}'' - \alpha''\mathfrak{C}')\,\delta + (\alpha''\mathfrak{C} - \alpha\mathfrak{C}'')\,\delta' + (\alpha\mathfrak{C}' - \alpha'\mathfrak{C})\,\delta'' = \mathfrak{k}$ fiat vel vel $= +1$ vel $= -1$, formamque f transire per substitutionem

$$\begin{matrix} \alpha, & \mathfrak{C}, & \delta \\ \alpha', & \mathfrak{C}', & \delta' \\ \alpha'', & \mathfrak{C}'', & \delta'' \end{matrix}$$

in $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} = \mathfrak{g}$, cui adiuncta $\begin{pmatrix} \mathfrak{A}, & \mathfrak{A}', & \mathfrak{A}'' \\ \mathfrak{B}, & \mathfrak{B}', & \mathfrak{B}'' \end{pmatrix} = \mathfrak{G}$. Tunc g, $\mathfrak{g}$ erunt aequiualentes, adeoque etiam G et $\mathfrak{G}$, et per applicationem praeceptorum in artt. 269, 270 traditorum *) inuenitur, si statuatur $(\mathfrak{C}'\gamma'' - \mathfrak{C}''\gamma')\,\delta + (\mathfrak{C}''\gamma - \mathfrak{C}\gamma'')\,\delta' + (\mathfrak{C}\gamma' - \mathfrak{C}'\gamma)\,\delta'' = \zeta$, $(\gamma'\alpha'' - \gamma''\alpha')\,\delta + (\gamma''\alpha - \gamma\alpha'')\,\delta' + (\gamma\alpha' - \gamma'\alpha)\,\delta'' = \eta$, formam $\mathfrak{G}$ transire in G per substitutionem

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k} \end{matrix}$$

*) Eruendo ex transf. formae f in g, transformationem formae g in f; ex hac atque transf. formae f in $\mathfrak{g}$, transf. formae g in $\mathfrak{g}$; denique ex hac, per transpositionem, transf. formae $\mathfrak{G}$ in G.

Hinc erit $B = {}_n t D + t k \mathfrak{B}$, $B' = \zeta t D + t k \mathfrak{B}'$, adeoque, propter $tk = \pm 1$, vel $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$, vel $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). In casu priori valores (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ aequiualentes vocamus, in posteriori oppositos; repraesentationem formae Φ autem ad quemlibet valorem expr. $\sqrt{\Delta}(p, -q, r)$ (mod. D), qui ex ipsa per methodum in I deduci potest, *pertinere* dicemus. Hinc omnes valores, ad quos eadem repraesentatio pertinet, vel aequiualentes erunt vel oppositi.

III. Vice versa autem, si vt ante in I repraesentatio formae Φ per f haec $x = \alpha t + \gamma u$ etc. ad valorem (B, B') pertinet, qui inde deducitur adiumento transformationis

$$\begin{matrix} \alpha, & \gamma, & \gamma \\ \alpha', & \gamma', & \gamma' \\ \alpha'', & \gamma'', & \gamma'' \end{matrix}$$

eadem quoque ad quemuis alium valorem $(\mathfrak{B}, \mathfrak{B}')$ pertinebit, qui illi vel aequiualens est vel oppositus; i. e. loco ipsorum γ, γ', γ'' alios integros δ, δ', δ'' accipere licebit, pro quibus aequatio (Ω) haec $(\alpha'\gamma'' - \alpha''\gamma')\delta + (\alpha''\gamma - \alpha\gamma'')\delta' + (\alpha\gamma' - \alpha'\gamma)\delta'' = \pm 1$ locum habeat, et qui ita comparati sint, vt coëfficiens 4 et 5 in forma ei adiuncta, in quam f per substitutionem (S)

$$\begin{matrix} \alpha, & \gamma, & \delta \\ \alpha', & \gamma', & \delta' \\ \alpha'', & \gamma'', & \delta'' \end{matrix}$$

transit, resp. fiant $= \mathfrak{B}, \mathfrak{B}'$. Statuatur enim $\pm B = \mathfrak{B} + {}_n D$, $\pm B' = \mathfrak{B}' + \zeta D$ (accipiendo

hic et postea signa superiora vel inferiora, prout valores (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ aequiualentes sunt vel oppositi), vnde ζ, η erunt integri, transeatque g per substitutionem

$$\begin{matrix} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{matrix}$$

in formam $\mathfrak{g}$, cuius determinantem esse Δ, in forma adiuncta vero coëfficientes 4 et 5 resp. $= \mathfrak{B}$, $\mathfrak{B}'$ fieri facile perspicietur. Faciendo autem $\alpha\zeta + \mathfrak{C}\eta \pm \gamma = \delta$, $\alpha'\zeta + \mathfrak{C}'\eta \pm \gamma' = \delta'$, $\alpha''\zeta + \mathfrak{C}''\eta \pm \gamma'' = \delta''$, nullo negotio patebit, f per substitutionem (S) transire in $\mathfrak{g}$, atque aequationi (Ω) satisfactum esse. *Q. E. D.*

283. Ex his principiis deducitur methodus sequens, omnes repraesentationes proprias formae binariae $\Phi = ptt + 2qtu + ruu$ determinantis D per ternariam f determinantis Δ inueniendi.

I. Eruantur omnes valores diuersi (i. e. non aequiualentes) expressionis $\sqrt{\Delta}(p, -q, r)$ (mod. D). Hoc problema pro eo casu, vbi Φ est forma primitiua atque Δ ad D primus, supra (art. 233) solutum est, casusque reliqui ad hunc facillime reducuntur, quam tamen rem fusius hic explicare breuitas non permittit. Obseruamus tantummodo, quoties Δ ad D primus sit, expressionem $\Delta(p, -q, r)$ residuum quadraticum ipsius D esse non posse, nisi Φ fuerit forma primitiua. Supponendo enim $\Delta p = BB - DA'$, $-\Delta q = BB' - DB''$, $\Delta r = B'B' - DA$, fit $(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$; hinc, per euolutionem et substituendo $qq - pr$ pro D, fit $(qq -$

$pr)\ (B''B'' - AA') - \Delta\ (Ap + 2B''q + A'r) + \Delta\Delta = 0$, vnde facile concluditur, si p, q, r diuisorem communem haberent, hunc etiam ipsum $\Delta\Delta$ metiri; tunc vero Δ ad D primus esse non posset. Quare p, q, r diuisorem communem habere nequeunt, siue φ erit forma primitiua.

II. Designemus multitudinem horum valorum per m, supponamusque, inter eos reperiri n valores, qui sibi ipsis oppositi sint (statuendo $n = 0$ quando tales non adsunt). Tunc manifestum est, ex $m - n$ reliquis valoribus binos semper oppositos fore (quoniam cuncti valores complete haberi supponuntur); reiiciatur e binis quibusque valoribus oppositis vnus ad libitum, remanebuntque omnino valores $\frac{1}{2}(m + n)$. Ita e. g. ex octo valoribus expr. $\sqrt{-1} \times (19, 3, 41)$ (mod. 770) his (44, 237), (171, — 27), (269, — 83), (291, — 127), (— 44, — 237), (— 171, 27), (— 269, 83), (— 291, 127), quatuor posteriores sunt reiiciendi, tamquam quatuor prioribus oppositi. Ceterum perspicuum est, si (B, B') sit valor sibi ipsi oppositus, $2B$, $2B'$, et proin etiam $2\Delta p$, $2\Delta q$, $2\Delta r$ per D diuisibiles fore; quodsi itaque Δ, D inter se primi sunt, etiam $2p$, $2q$, $2r$ per D diuisibiles erunt, et quum, per I, in hoc casu etiam p, q, r diuisorem communem habere nequeant, etiam 2 per D diuisibilis esse debebit, quod fieri nequit nisi D vel $= \pm 1$, vel $= \pm 2$. Quamobrem pro omnibus valoribus ipsius D maioribus quam 2 semper erit $n = 0$, si Δ ad D est primus.

III. His ita factis manifestum est, quamuis repraesentationem propriam formae φ per f ne-

cessario ad aliquem e valoribus remanentibus pertinere debere, et quidem ad vnicum tantum. Quare hi valores successiue sunt percurrendi, repraesentationesque ad singulos pertinentes inuestigandae. Vt inueniantur repraesentationes ad valorem *datum* (B, B') pertinentes, primo determinanda est forma ternaria $g = \left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$, cuius determinans $= \Delta$ et in qua $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$; valores ipsorum a'', b, b' hinc inueniuntur adiumento aequationum in II art. 276, ex quibus facile perspicitur, in eo casu vbi Δ, D inter se primi sint, b, b', a'' necessario fieri integros (nempe quoniam hi tres numeri, multiplicati tum per D tum per Δ integros producunt). Iam si vel aliquis coëfficientium b, b', b'' fractus est, vel formae f, g non sunt aequiualentes: nullae repraesentationes formae φ per f ad (B, B') pertinentes dari possunt; si vero b, b', a'' sunt integri, formaeque f, g aequiualentes, quaeuis transformatio illius in hanc, vt

$$\begin{matrix} \alpha, & \mathfrak{G}, & \gamma \\ \alpha', & \mathfrak{G}', & \gamma' \\ \alpha'', & \mathfrak{G}'', & \gamma'' \end{matrix}$$

talem repraesentationem suppeditat, puta $x = \alpha t + \mathfrak{G} u$, $x' = \alpha' t + \mathfrak{G}' u$, $x'' = \alpha'' t + \mathfrak{G}'' u$; manifestoque nulla huiusmodi repraesentatio exstare poterit, quae non ex aliqua transformatione deduci posset. Hoc itaque modo ea problematis secundi pars, quae inuestigat repraesentationes *proprias*, ad problema tertium iam est reducta.

IV. Ceterum transformationes diuersae formae f in g semper producunt repraesentationes diuersas, eo solo casu excepto, vbi valor (B, B') sibi ipsi oppositus est, in quo binae transformationes vnicam semper repraesentationem suppeditant. Supponendo enim, f transire in g etiam per substitutionem

$$\begin{matrix} \alpha, & \mathfrak{C}, & \delta \\ \alpha', & \mathfrak{C}', & \delta' \\ \alpha'', & \mathfrak{C}'', & \delta'' \end{matrix}$$

(quae eandem repr. praebet vt transf. praec.), denotandoque per k, $\mathfrak{k}$, ζ, η numeros eosdem vt in II art. praec., erit $B = k\mathfrak{k}B + \eta\mathfrak{k}D$, $B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$; si itaque vel vterque k, $\mathfrak{k}$ supponitur $= +1$, vel vterque $= -1$, erit (quia casum $D = 0$ exclusimus) $\zeta = 0$, $\eta = 0$, vnde facile sequitur $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$; quare illae duae transformationes in eo solo casu diuersae esse possunt, vbi alter numerorum k, $\mathfrak{k}$ est $+1$, alter -1; tunc erit $B \equiv -B$, $B' \equiv -B'$ (mod. D), siue valor (B, B') sibi ipsi oppositus.

V. Ex iis, quae supra (art. 271) de criteriis formarum definitarum et indefinitarum tradidimus, facile sequitur, si Δ sit positiuus, D negatiuus, atque Φ forma negatiua, g fieri formam definitam negatiuam; si vero Δ sit positiuus, atque vel D positiuus, vel D negatiuus et Φ forma positiua, g euadere formam indefinitam. Iam quum f, g certo aequiualentes esse nequeant, nisi respectu huius qualitatis similes sint, manifestum est, formas binarias determinantis positiui nec non po-

sitiuas, per ternariam negatiuam proprie repraesentari non posse, neque formas binarias negatiuas per ternariam indefinitam determinantis positiui; sed per formam ternariam prioris posterioriseue speciei vnice binarias posterioris priorisue resp. Simili modo concluditur, per formam ternariam determinantis negatiui definitam (i. e. positiuam) vnice repraesentari binarias positiuas, per indefinitam vnice negatiuas et formas det. positiui.

284. Quum repraesentationes *impropriae* formae binariae φ determinantis D per ternariam f, cui adiuncta est F, eae sint, ex quibus repraesentationes impropriae numeri D per formam F sequuntur, φ per f manifesto nequit improprie repraesentari, nisi D factores quadratos implicet. Ponamus, omnia quadrata ipsum D metientia (praeter 1) esse ee, $e'e'$, $e''e''$ etc. (quorum multitudo finita erit, quia supponimus, non esse $D = 0$), praebebitque quaelibet repr. impr. formae φ per f repraesentationem numeri D per F, in qua valores indeterminatarum aliquem e numeris e, e', e'' etc. pro diuisore communi maximo habebunt; hoc respectu breuitatis caussa quamuis repr. impr. formae φ ad diuisorem quadratum ee vel $e'e'$ vel $e''e''$ etc. *pertinere* dicemus. Iam omnes repr. formae φ ad eundem diuisorem quadratum *datum* ee (cuius radicem e positiue acceptam supponimus) pertinentes per regulas sequentes inueniuntur, ex quarum demonstratione synthetica, propter breuitatem hic praeferenda, analysis per quam euolutae sunt facile restitui poterit.

Primo eruantur omnes formae binariae determinantis $\frac{D}{ee}$, quae in formam φ transeunt per substitutionem propriam talem $T = \varkappa t + \lambda u$, $U = \mu u$, designantibus T, U indeterminatas talis formae; t, u indet. formae φ; $\varkappa$, μ integros positiuos (quorum productum itaque $= e$); λ integrum positiuum minorem quam μ (siue etiam cifram). Hae formae, cum transformationibus respondentibus, ita inueniuntur:

Aequetur $\varkappa$ successiue singulis diuisoribus ipsius e positiue acceptis (inclusis etiam 1 et e), fiatque $\mu = \frac{e}{\varkappa}$; pro singulis valoribus determinatis ipsorum $\varkappa$, μ tribuantur ipsi λ omnes valores integri a 0 vsque ad $\mu - 1$, quo pacto omnes transformationes certo habebuntur. Iam forma, quae per quamuis substitutionem $T = \varkappa t + \lambda u$, $U = \mu u$ in φ transit, inuenitur inuestigando formam in quam φ transit per hanc $t = \frac{1}{\varkappa} T - \frac{\lambda}{e} U$, $u = \frac{1}{\mu} U$; sic formae singulis transformationibus respondentes obtinebuntur; sed ex omnibus his formis eae tantum retinendae sunt, in quibus omnes tres coëfficientes euadunt integri *).

*) Si de hoc problemate fusius agere hic liceret, solutionem admodum contrahere possemus. Id statim obuium est, pro $\varkappa$ alios diuisores ipsius e accipere non esse necessarium, nisi quorum quadratum metiatur coëfficientem primum formae φ. Ceterum hoc problema, ex qua etiam solutiones simpliciores probl. artt. 213, 214 deduci possunt, alia occasione idonea resumere nobis reseruamus.

Secundo ponamus Φ esse aliquam ex hisce formis, quae in φ transeat per subst. $T = \varkappa t + \lambda u$, $U = \mu u$; inuestigentur omnes repraesentationes *propriae* formae Φ per f (si quae dantur), exhibeanturque indefinite per $x = \mathfrak{A}T + \mathfrak{B}U$, $x' = \mathfrak{A}'T + \mathfrak{B}'U$, $x'' = \mathfrak{A}''T + \mathfrak{B}''U \ldots (\mathfrak{R})$; denique ex singulis $(\mathfrak{R})$ deducatur repraesentatio $(\varrho) \ldots x = \alpha t + \mathfrak{C}u$, $x' = \alpha' t + \mathfrak{C}' u$, $x'' = \alpha'' t + \mathfrak{C}'' u$ per aequationes $(R) \ldots \alpha = \varkappa\mathfrak{A}$, $\alpha' = \varkappa\mathfrak{A}'$, $\alpha'' = \varkappa\mathfrak{A}''$, $\mathfrak{C} = \lambda\mathfrak{A} + \mu\mathfrak{B}$, $\mathfrak{C}' = \lambda\mathfrak{A}' + \mu\mathfrak{B}'$, $\mathfrak{C}'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}''$. Eodem prorsus modo, vt forma Φ, tractentur formae reliquae per regulam primam inuentae (si plures adsunt), ita vt ex singulis cuiusque repraesentationibus propriis aliae repraesentationes deriuentur, dicoque, hoc modo prodire cunctas repraesentationes formae Φ ad diuisorem *ee* pertinentes, et quidem quamlibet semel tantum.

Dem. I. Formam ternariam f per quamuis substitutionem (ϱ) reuera transire in φ, tam obuium est, vt explicatione ampliori non opus sit; quamlibet autem repr. (ϱ) esse impropriam et ad diuisorem *ee* pertinere, inde patet, quod numeri $\alpha'\mathfrak{C}'' - \alpha''\mathfrak{C}'$, $\alpha''\mathfrak{C} - \alpha\mathfrak{C}''$, $\alpha\mathfrak{C}' - \alpha'\mathfrak{C}$ resp. fiunt $= e(\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B})$, vnde illorum diuisor comm. max. manifesto erit e (quoniam $\mathfrak{R}$ est repraesentatio propria).

II. Ostendemus, ex quauis repraesentatione data (ϱ) formae φ, inueniri posse repraesentationem propriam formae determinantis $\frac{D}{ee}$, inter formas per regulam primam inuentas conten-

tae, siue ex valoribus datis ipsorum α, α', α'', $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$ deduci posse valores integros ipsorum $\varkappa$, λ, μ, conditionibus praescriptis, atque valores ipsorum $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$, aequationibus (R) satisfacientes, et quidem vnico tantum modo. Primo statim patet ex tribus aequ. primis in (R), pro $\varkappa$ accipi debere diuisorem communem maximum ipsorum α, α', α'' signo positiuo (quum enim $\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B}$ diuisorem communem non habere debeant, etiam $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ diu. comm. habere nequeunt); hinc etiam $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ determinati erunt, nec non $\mu = \frac{e}{\varkappa}$ (quem necessario integrum fieri facile perspicitur). Ponamus, tres integros a, a', a'' ita acceptos esse, vt fiat $a\mathfrak{A} + a'\mathfrak{A}' + a''\mathfrak{A}'' = 1$, scribamusque breuitatis caussa k pro $a\mathfrak{B} + a'\mathfrak{B}' + a''\mathfrak{B}''$. Tunc ex tribus vltimis aeq. (R) sequitur, esse debere $a\mathfrak{C} + a'\mathfrak{C}' + a''\mathfrak{C}'' = \lambda + \mu k$, vnde statim patet pro λ vnicum tantummodo valorem inter limites 0 et $\mu - 1$ situm dari. Quo facto quum etiam $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ valores determinatos nanciscantur, nihil superest, nisi vt demonstremus hos semper hinc integros euadere. Fiet autem $\mathfrak{B} = \frac{1}{\mu}(\mathfrak{C} - \lambda\mathfrak{A}) = \frac{1}{\mu}(\mathfrak{C}(1 - a\mathfrak{A}) - \mathfrak{A}(a'\mathfrak{C}' + a''\mathfrak{C}''))$ $- \mathfrak{A}k = \frac{1}{\mu}(a''(\mathfrak{A}''\mathfrak{C} - \mathfrak{A}\mathfrak{C}'') - a'(\mathfrak{A}\mathfrak{C}' - \mathfrak{A}'\mathfrak{C}))$ $- \mathfrak{A}k = \frac{1}{e}(a''(\alpha''\mathfrak{C} - \alpha\mathfrak{C}'') - a'(\alpha\mathfrak{C}' - \alpha'\mathfrak{C})) - \mathfrak{A}k$, eritque adeo manifesto integer, similiterque facile confirmatur, etiam ipsos $\mathfrak{B}'$, $\mathfrak{B}''$ valores integros nancisci. — Ex his ratiociniis colligitur, nullam repraesentationem impropriam formae Φ per f, ad diuisorem ee pertinentem, exstare posse,

quae per methodum traditam vel non vel pluries obtineatur.

Quodsi iam eodem modo reliqui diuisores quadrati ipsius D tractantur, repraesentationesque ad singulos pertinentes eruuntur, cunctae repraesentationes impropriae formae φ per f habebuntur.

Ceterum ex hac solutione facile deducitur, theorema, ad finem art. praec. pro repraess. propriis traditum etiam ad improprias patere, scilicet generaliter nullam formam binariam positiuam det. negatiui per ternariam negatiuam repraesentari posse etc.; patet enim, si φ sit forma talis binaria, quae propter illud theorema per f proprie repraesentari nequeat, etiam omnes formas determinantium $\frac{D}{ee}$, $\frac{D}{e'e'}$ etc., ipsam φ implicantes per f proprie repraesentari non posse, quum hae formae omnes determinantem eodem signo affectum habeant vt φ, et, quoties hi determinantes negatiui sunt, vel omnes euadant formae positiuae vel negatiuae, prout φ ad illas vel ad has pertinet.

285. De quaestionibus problema tertium nobis propositum constituentibus (ad quod duo priora in praecc. sunt reducta), scilicet propositis duabus formis ternariis eiusdem determinantis, diiudicare, vtrum aequiualentes sint necne, et in casu priori omnes transformationes alterius in alteram inuenire, pauca tantum hoc loco inserere possumus, quum solutio completa, qualem

pro problematibus analogis in formis binariis tradidimus, hic adhuc maioribus difficultatibus sit obnoxia. Quamobrem ad quosdam casus particulares, propter quos praecipue haecce digressio instituta est, disquisitionem nostram limitabimus.

I. Pro determinante + 1 supra ostensum est, omnes formas binarias in duas classes distribui, quarum altera omnes formas indefinitas, altera omnes definitas (negatiuas) contineat. Hinc statim concluditur, duas formas ternarias quascunque det. 1 aequiualentes esse, si vel vtraque sit definita vel vtraque indefinita; si vero altera sit definita, altera indefinita, aequiualentiam locum non habere (propositionis pars posterior manifesto valet generaliter pro formis determinantis cuiuscunque). — Simili modo duae formae quaecunque determinantis — 1 certo aequialebunt, si vel vtraque definita est, vel vtraque indefinita. — Duae formae definitae determinantis 2 semper aequialebunt; duae indefinitae non aequialebunt; si in altera tres coëfficientes primi omnes pares sunt, in altera vero non omnes sunt pares; in casibus reliquis (si vel vtraque tres coëfficientes primos simul pares habet, vel neutra) aequialebunt. — Hoc modo adhuc multo plures propositiones speciales exhibere possemus, si supra (art. 277) plura exempla euoluta fuissent.

II. Pro omnibus hisce casibus poterit etiam, designantibus f, f' formas ternarias aequiualentes, transformatio vna alterius in alteram inueniri. Nam pro omnibus casibus in quauis classe formarum ternariarum multitudo satis parua forma-

rum supra assignata est, ad quarum aliquam per methodos vniformes quaeuis forma eiusdem classis reduci possit; has omnes ad vnicam reducere ibidem docuimus. Sit F haec forma in ea classe in qua sunt f, f', poteruntque per praecepta supra tradita inueniri transformationes formarum f, f' in F, nec non formae F in f, f'. Hinc per art. 270 deduci poterunt transformationes formae f in f' formaeque f' in f.

III. Superesset itaque tantummodo, ostendere, quo pacto ex vna transformatione formae ternariae f in aliam f' omnes transformationes possibiles deriuari possint. Hoc problema pendet ab alio simpliciori, scilicet inuenire omnes transformationes formae ternariae f in se ipsam. Nimirum si f per plures substitutiones (γ), (γ'), (γ'') etc. in se ipsam et per substitutionem (t) in f' transit, patet si ad normam art. 270. combinetur transformatio (t) cum (γ), $\gamma')$, (γ'') etc., prodire transformationes per quas omnes f in f' transeat; praeterea per calculum facile probatur, quamuis transformationem formae f in f' hoc modo deduci posse e combinatione transformationis datae t formae f in f' cum aliqua (et quidem *vnica*) transformatione formae f in se ipsam, adeoque ex combinatione transformationis datae formae f in f' cum *omnibus* transformationibus formae f in se ipsam oriri *omnes* transformationes formae f in f', et quidem singulas semel tantum.

Inuestigationem omnium transformationum formae f in se ipsam ad eum casum hic restrin-

gimus, vbi f est forma definita cuius coëfficientes 4, 5, 6 omnes $= 0$ *). Sit itaque $f = \begin{pmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{pmatrix}$, exhibeanturque omnes substitutiones, per quas f in se ipsam transit, indefinite per

$$\begin{matrix} \alpha, & \mathfrak{b}, & \gamma \\ \alpha', & \mathfrak{b}', & \gamma' \\ \alpha'', & \mathfrak{b}'', & \gamma'' \end{matrix}$$

ita vt satisfieri debeat aequationibus (Ω) ... $a\alpha\alpha + a'\alpha'\alpha' + a''\alpha''\alpha'' = a$, $a\mathfrak{b}\mathfrak{b} + a'\mathfrak{b}'\mathfrak{b}' + a''\mathfrak{b}''\mathfrak{b}'' = a'$, $a\gamma\gamma + a'\gamma'\gamma' + a''\gamma''\gamma'' = a''$, $a\alpha\mathfrak{b} + a'\alpha'\mathfrak{b}' + a''\alpha''\mathfrak{b}'' = 0$, $a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' = 0$, $a\mathfrak{b}\gamma + a'\mathfrak{b}'\gamma' + a''\mathfrak{b}''\gamma'' = 0$. Iam tres casus sunt distinguendi:

I. Quando a, a', a'' (qui idem signum habebunt) omnes sunt inaequales, supponamus $a < a'$, $a' < a''$ (si alius magnitudinis ordo adest, eaedem conclusiones prorsus simili modo eruentur). Tunc aequ. prima in (Ω) manifesto requirit vt sit $\alpha' = \alpha'' = 0$, adeoque $\alpha = \pm 1$; hinc per aequ. 4, 5 erit $\mathfrak{b} = 0$, $\gamma = 0$; similiter ex aequ. 2 erit $\mathfrak{b}'' = 0$, et proin $\mathfrak{b}' = \pm 1$; hinc fit, per aequ. 6, $\gamma' = 0$, et per 3, $\gamma'' = \pm 1$, ita vt (ob signorum ambiguitatem independentem) omnino habeantur 8 transformationes diuersae.

II. Quando e numeris a, a', a'' duo sunt aequales, *e. g.* $a' = a''$, tertius inaequalis, sup-

*) Casus reliqui vbi f est forma definita ad hunc reduci possunt; si vero f est forma indafinita, methodus omnino diuersa adhibenda, transformationumque multitudo infinita erit.

ponamus *primo* $a < a'$. Tunc eodem modo vt in casu praec. erit $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\mathfrak{C} = 0$, $\gamma = 0$; ex aequ. 2, 3, 6 autem facile deducitur, esse debere vel $\mathfrak{C}' = \pm 1$, $\gamma' = 0$, $\mathfrak{C}'' = 0$, $\gamma'' = \pm 1$, vel $\mathfrak{C}' = 0$, $\gamma' = \pm 1$, $\mathfrak{C}'' = \pm 1$, $\gamma'' = 0$. Si vero, *secundo*, $a > a'$, eaedem conclusiones sic obtinentur: ex aequ. 2, 3 necessario erit $\mathfrak{C} = 0$, $\gamma = 0$, et vel $\mathfrak{C}' = \pm 1$, $\gamma' = 0$, $\mathfrak{C}'' = 0$, $\gamma'' = \pm 1$, vel $\mathfrak{C}' = 0$, $\gamma' = \pm 1$, $\mathfrak{C}'' = \pm 1$, $\gamma'' = 0$; pro suppositione vtraque ex aequ. 4, 5 erit $\alpha' = 0$, $\alpha'' = 0$, atque ex 1, $\alpha = \pm 1$. Habentur itaque, pro vtroque casu, 16 transformationes diuersae. — Duo casus reliqui, vbi vel $a = a''$, vel $a = a'$, prorsus simili modo absoluuntur, si modo characteres α, α', α'' in priori cum $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$, in posteriori cum γ, γ', γ'' resp. commutantur.

III. Quando omnes a, a', a'' aequales sunt, aequationes 1, 2, 3 requirunt, vt e tribus numeris α, α', α'', nec non ex $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$, vt et ex γ, γ', γ'' bini sint $= 0$, tertius $= \pm 1$. Per aequ. 4, 5, 6 autem facile intelligitur, e tribus numeris α, $\mathfrak{C}$, γ vnum tantummodo $= \pm 1$ esse posse, similiterque ex α', $\mathfrak{C}'$, γ', nec non ex α'', $\mathfrak{C}''$, γ''. Quamobrem sex tantummodo combinationes dantur

$$\left.\begin{array}{cccccc|c} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \mathfrak{C}' & \mathfrak{C}'' & \mathfrak{C} & \mathfrak{C}'' & \mathfrak{C} & \mathfrak{C}' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array}\right\} \text{ Coëfficientes seni reliqui} = 0$$

ita vt ob signorum ambiguitatem omnino 48 transformationes habeantur. — Idem typus etiam

casus praecedentes complectitur: sed e sex columnis primis prima sola accipi debet, quando a, a', a'' omnes sunt inaequales; columna prima et secunda, quando $a' = a''$; prima et tertia, quando $a = a'$; prima et sexta, quando $a = a''$.

Hinc colligitur, si forma $f = axx + a'x'x' + a''x''x''$ in aliam aequiualentem f' transeat per substitutionem $x = \delta y + \varepsilon y' + \zeta y''$, $x' = \delta' y + \varepsilon' y' + \zeta' y''$, $x'' = \delta'' y + \varepsilon'' y' + \zeta'' y''$, omnes transf. formae f in f' contineri sub schemate sequente:

$$\begin{array}{|c|c|c|c|c|c|}
x & x & x' & x' & x'' & x'' \\
x' & x'' & x & x'' & x & x' \\
x'' & x' & x'' & x & x' & x
\end{array} = \pm \begin{array}{l}
(\delta y + \varepsilon y' + \zeta y'') \\
(\delta' y + \varepsilon' y' + \zeta' y'') \\
(\delta'' y + \varepsilon'' y' + \zeta'' y'')
\end{array}$$

eo discrimine, vt sex columnae primae omnes adhibendae sint, quando $a = a' = a''$; columna 1 et 2, quando a', a'' aequales, a inaequalis; 1 et 3, quando $a = a'$; 1 et 6, quando $a = a''$; denique columna prima sola, quando a, a', a'' omnes inaequales. In casu primo transformationum multitudo erit 48, in secundo, tertio et quarto 16, in quinto 8.

* * *

Ab hac succincta primorum elementorum theoriae formarum ternariarum expositione ad quasdem applicationes speciales progredimur, inter quas primum locum meretur sequens

286. Problema. *Proposita forma binaria* $F = (A, B, C)$ *determinantis* D *ad genus principale pertinente: inuenire formam binariam* f, *e cuius duplicatione illa oriatur.*

Sol. I. Quaeratur repraesentatio propria formae ipsi F oppositae $F' = ATT - 2BTU + CUU$ per formam ternariam $xx - 2yz$, quae sit $x = \alpha T + \gamma U$, $y = \alpha' T + \gamma' U$, $z = \alpha'' T + \gamma'' U$, quod fieri posse e theoria praec. formarum ternariarum facile colligitur. Quum enim F per hyp. sit e genere principali, dabitur valor expr. $\sqrt{(A, B, C)}$ (mod. D), vnde inueniri poterit forma ternaria Φ determinantis 1, in quam $(A, -B, C)$ tamquam pars ingrediatur, cuius formae coëfficientes omnes fore integros nullo negotio perspicietur. Aeque facile intelligitur, Φ fore formam indefinitam (quoniam per hyp. F certo non est forma negatiua); vnde necessario formae $xx - 2yz$ aequiualens erit. Assignari poterit itaque transformatio huius in illam, quae repraesentationem propriam formae F' per $xx - 2yz$ suppeditabit. — Tunc igitur erit $A = \alpha\alpha - 2\alpha'\alpha''$, $-B = \alpha\gamma - \alpha'\gamma'' - \alpha''\gamma'$, $C = \gamma\gamma - 2\gamma'\gamma''$; porro designatis numeris $\alpha\gamma' - \alpha'\gamma$, $\alpha'\gamma'' - \alpha''\gamma'$, $\alpha''\gamma - \alpha\gamma''$ per a, b, c resp., hi diuisorem communem non habebunt, eritque $D = bb - 2ac$.

II. Hinc adiumento obseruationis vltimae art. 235 facile concluditur, F transire per substitutionem $2\gamma'$, γ, γ, γ''; $2\alpha'$, α, α, α'' in productum formae $(2a, -b, c)$ in se ipsam, nec non per substitutionem γ', γ, γ, $2\gamma''$; α', α, α, $2\alpha''$ in productum formae

$(a, -b, 2c)$ in se ipsam. Iam diuisor communis maximus numerorum $2a$, $2b$, $2c$ est 2; si itaque c est impar, $2a$, $2b$, c diuisorem communem non habebunt, siue $(2a, -b, c)$ erit forma proprie primitiua; similiter, si a est impar, $(a, -b, 2c)$ forma proprie primitiua erit; in casu priori F oritur ex duplicatione formae $(2a, -b, c)$, in posteriori ex duplicatione formae $(a, -b, 2c)$, (V. concl. 4, art. 235); vnus vero horum casuum certo semper locum habebit. Si enim vterque a, c esset par, b necessario foret impar; iam facile confirmatur, esse $\gamma''a + \gamma b + \gamma'c = 0$, $\alpha''a + \alpha b + \alpha'c = 0$, vnde sequeretur, γb, αb, adeoque etiam α et γ esse pares. Hinc autem A et C forent pares, quod esset contra hypothesin, secundum quam F est forma e genere principali adeoque ex ordine proprie primitiuo. — Ceterum fieri etiam potest, vt tum a tum c pares sint, in quo itaque casu duae statim formae habebuntur, e quarum duplicatione F oritur.

Ex. Proposita sit forma $F = (5, 2, 31)$, det. -151. Valor expressionis $\sqrt{(5, 2, 31)}$ hic inuenitur $(55, 22)$; hinc forma ternaria $\Phi = \begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix}$; huic per praecepta art. 272 aequiualens inuenitur forma $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, quae in Φ transit per substitutionem

$$\begin{matrix} 2, & 2, & -1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{matrix}$$

Hinc adiumento transformationum in art. 277 traditarum inuenitur, $\begin{pmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{pmatrix}$ transire in φ per substitutionem

$$\begin{matrix} 3, & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3 \end{matrix}$$

Fit itaque $a = 11$, $b = -17$, $c = 20$; quare quum a sit impar, F oritur ex duplicatione formae $(11, -17, 40)$ transitque in productum huius formae in se ipsam per substitutionem $-1, -7, -7, -9;\ 2, 3, 3, 1$.

287. Circa problema in art. praec. solutum sequentes adhuc annotationes adiicimus.

I. Si forma F per substitutionem $p, p', p'', p'''; q, q', q'', q'''$ in productum e duabus formis (h, i, k), (h', i', k') transformatur, (vtraque vti semper supponimus proprie accepta), habebuntur aequationes, ex concl. 3 art. 235 facile deducendae: $p''hn' - p'h'n - p(in' - i'n) = 0$, $(p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0$, $p'kn' - p''k'n - p'''(in' - i'n) = 0$, tresque aliae ex his per commutationem numerorum p, p', p'', p''' cum q, q', q'', q''' oriundae; n, n' sunt radices quadratae positiuae e quotientibus prodeuntibus, si determinantes formarum (h, i, k), (h', i', k') per det. formae F diuiduntur. Si itaque hae formae sunt identicae, siue $n = n'$, $h = h'$, $i = i'$, $k = k'$, illae aequationes transeunt in has: $(p'' - p')hn = 0$, $(p'' - p)in$

$= 0$, $(p'' - p')\,kn = 0$, vnde erit *necessario* $p' = p''$, prorsusque simili modo $q' = q''$. — Tribuendo itaque formis (h, i, k), (h', i', k') *easdem* indeterminatas t, u, designandoque indeterminatas formae F per T, U, transibit F per substitutionem $T = ptt + 2p'tu + p''uu$, $U = qtt + 2q'tu + q''uu$ in $(htt + 2itu + kuu)^2$.

II. Si forma F oritur e duplicatione formae f, orietur etiam e duplicatione cuiusuis aliae formae cum f in eadem classe contentae siue classis formae F e duplicatione classis formae f (V. art. 238). Ita in ex. art. praec. (5, 2, 31) orietur etiam e duplicatione formae (11, 5, 16), ipsi (11, — 17, 40) proprie aequiualentis. Ex vna classe, per cuius dupl. classis formae F oritur, *omnes* (si plures dantur) inueniuntur adiumento probl. 260; in exemplo nostro alia huiusmodi classis positiua non dabitur, quia vna tantummodo classis anceps proprie primitiua positiua det. — 151 exstat (puta principalis); quum e compositione classis vnicae ancipitis negatiuae (— 1, 0, — 151), cum classe (11, 5, 16) oriatur classis (— 11, 5, — 16), haec erit vnica negatiua, e cuius duplicatione classis (5, 2, 31) oritur.

III. Quum per solutionem ipsam probl. art. praec. euictum sit, quamuis classem formarum binariarum proprie primitiuam (positiuam) ad genus principale pertinentem ex alicuius classis pr. prim. eiusdem det. duplicatione oriri posse: theorema art. 261, per quod certi eramus, *ad minimum* semissi omnium characterum pro determinante non quadrato dato D assignabilium

genera proprie primitiua (positiua) respondere non posse, eo iam ampliatur, vt *praecise* semissi omnium horum characterum talia genera reuera respondeant, alterique ideo semissi nulla respondere possint (V. demonstr. illius theor.). Quare quum in art. 263 omnes illi characteres assignabiles in duas species P, Q aequaliter distributi sint, e quibus posteriores Q formis pr. prim. (positiuis) respondere non posse probatum erat, de reliquis autem P incertum maneret, an singulis genera semper reuera responderent: nunc hoc dubium penitus est sublatum, certique sumus, in toto characterum complexu P nullum adesse cui genus non respondeat. — Hinc facile quoque deducitur, pro determinante negatiuo in ordine pr. prim. *negatiuo*, in quo omnes P impossibiles *solosque* Q possibiles esse in art. 264, I ostensum est, *omnes* Q reuera possibiles esse. Designante enim K characterem quemcunque ex Q, f formam arbitrariam ex ordine pr. prim. neg. formarum det. D, atque K' ipsius characterem, hic erit ex Q; vnde facile perspicitur, characterem ex K, K' compositum (ad normam art. 246) ad P pertinere, adeoque formas pr. primitiuas positiuas det. D exstare quae ei respondeant; ex compositione talis formae cum f manifesto orietur forma pr. prim. neg. det. D cuius character erit K. — Prorsus simili ratione probatur, in ordine improprie primitiuo eos characteres qui per praecepta art. 274 II, III *sali* possibiles inueniuntur *omnes* possibiles esse, siue sint P siue Q. — Haecce theoremata, ni vehementer fallimur, ad pulcherrima in theoria formarum binariarum sunt referenda, eo magis quod licet summa sim-

plicitate gaudeant, tamen tam recondita sint vt ipsarum demonstrationem rigorosam absque tot aliarum disquisitionum subsidio condere non liceat.

Transimus iam ad aliam applicationem digressionis praecedentis, ad discerptionem tum numerorum tum formarum binariarum in terna quadrata, cui praemittimus sequens

288. Problema. *Designante M numerum positiuum, inuenire conditiones sub quibus formae binariae primitiuae negatiuae determinantis — M dari possint, quae sint residua quadratica ipsius M siue pro quibus* 1 *sit numerus characteristicus.*

Sol. Designemus per Ω complexum omnium characterum particularium quos praebent relationes numeri 1 tum ad singulos diuisores primos (impares) ipsius M tum ad numerum 8 vel 4 quando ipsum M metitur; manifesto hi characteres erunt Rp, Rp', Rp'' etc., denotantibus p, p', p'' etc., illos diuisores primos; atque 1, 4 quando 4; 1, 8 quando 8 ipsum M metitur. Praeterea vtamur literis P, Q in eadem significatione vt in art. praec. siue vt in 263. Iam distinguamus casus sequentes.

I. Quando M per 4 diuisibilis est, Ω erit character integer, patetque ex art. 233 V, 1 talium tantummodo formarum numerum characteristicum esse posse, quarum character sit Ω. Sed manifestum est, Ω fore characterem formae principalis (1, 0, M), adeoque ad P pertinere et proin formae proprie primitiuae negatiuae competere non posse; quare quum formae impro-

prie primitiuae pro tali det. non dentur, nullae omnino formae prim. neg. in hoc casu dantur, quae sint residua ipsius *M*.

II. Quando $M \equiv 3 \pmod 4$, prorsus eadem ratiocinia valent ea sola exceptione vt in hoc casu ordo *improprie* primitiuus negatiuus exstet, in quo characteres *P* vel possibiles erunt, vel impossibiles, prout $M \equiv 3$ vel $\equiv 7 \pmod 8$, V. art. 264, III. In casu igitur priori in hoc ordine genus dabitur, cuius character sit Ω, vnde 1 erit numerus characteristicus omnium formarum in ipso contentarum; in casu posteriori nullae omnino formae negatiuae hac proprietate praeditae dari poterunt.

III. Quando $M \equiv 1 \pmod 4$, Ω nondum est character completus, sed iusuper accedere debet relatio ad numerum 4; patet autem, Ω necessario in characterem formae cuius num. char. sit 1 ingredi debere, et vice versa, formam quamuis, cuius character sit vel Ω; 1, 4, vel Ω; 3, 4, habere numerum char. 1. Iam Ω; 1, 4 manifesto est character generis principalis, qui ad *P* pertinet adeoque in ordine pr. prim. negatiuo impossibilis est; ex eadem ratione Ω; 3, 4 ad *Q* pertinebit (art. 263), vnde ipsi in ordine pr. prim. negatiuo genus respondebit, cuius formae omnes habebunt num. char. 1. Ordo improprie primitiuus in hoc casu, vt in sequente, non datur.

IV. Quando $M \equiv 2 \pmod 4$, ad Ω accedere debet relatio ad 8, quo fiat character completus, puta vel 1 *et* 3, 8, vel 5 *et* 7, 8, quando $M \equiv 2 \pmod 8$; et vel 1 *et* 7, 8, vel 3 *et*

5, 8, quando $M \equiv 6 \pmod 8$. Pro casu priori character Ω; 1 *et* 3, 8 manifesto pertinet ad P, adeoque Ω; 5 *et* 7, 8, ad Q, vnde ipsi respondebit genus pr. prim. neg.; similique ratione pro posteriori vnum genus in ordine pr. prim. negatiuo dabitur, cuius formae proprietate praescripta praeditae sint, puta cuius character Ω; 3 *et* 5, 8.

Ex his colligitur, formas primitiuas negatiuas det. — M quarum numerus characteristicus sit 1 dari, quando M alicui numerorum 1, 2, 3, 5, 6 secundum modulum 8 congruus sit et quidem in vnico semper genere, quod improprium erit quando $M \equiv 3$; tales formas omnino non dari, quando $M \equiv 0$, 4 vel 7 (mod. 8). Ceterum manifestum est, si $(-a, -b, -c)$ sit sit forma primitiua negatiua cuius num. char. $+1$, (a, b, c) esse formam primitiuam positiuam cuius num. char. -1; hinc perspicuum est, in quinque casibus prioribus (quando $M \equiv 1, 2, 3, 5, 6$) dari genus vnum primitiuum positiuum cuius formae habeant num. char. -1, et quidem, pro $M \equiv 3$, *improprium*, in tribus reliquis vero (quando $M \equiv 0, 4, 7$) tales formas positiuas omnino dari non posse.

289. Circa repraesentationes proprias formarum binariarum per ternariam $xx + yy + zz = f$, e theoria generali in art. 282 tradita colliguntur haec:

I. Forma binaria Φ per f proprie repraesentari nequit, nisi fuerit forma positiua primitiua, atque -1 (i. e. det. formae f) ipsius numerus characteristicus. Quare pro determinante positiuo, nec non pro negatiuo — M quando M est

vel per 4 diuisibilis vel formae $8n + 7$, nullae formae binariae per f proprie repraesentabiles dantur.

II. Si vero $\Phi = (p, q, r)$ est forma positiua primitiua determinantis $-M$, atque -1 numerus characteristicus formae Φ, adeoque etiam oppositae $(p, -q, r)$: dabuntur repraesentationes propriae formae Φ per f ad quemlibet valorem datum expr. $\sqrt{-(p, -q, r)}$ pertinentes. Scilicet omnes coëfficientes formae ternariae g det. -1 (art. 283) necessario fient integri, g vero forma definita, adeoque ipsi f certo aequiualens (art. 285. I).

III. Multitudo omnium repraesentationum ad eundem valorem expr. $\sqrt{-(p, -q, r)}$ pertinentium in omnibus casibus, praeter $M = 1$ et $M = 2$, per art. 283, III aeque magna est ac multitudo transformationum formae f in g, adeoque, per art. 285, $= 48$; ibinde patet, si vna repraesentatio ad valorem datum pertinens habeatur, 47 reliquas inde deriuari, valores ipsorum x, y, z, omnibus quibus fieri potest modis tum inter se permutando tum signis oppositis afficiendo; quare omnes 48 repraesentationes *vnicam* decompositionem formae Φ in tria quadrata producunt, si ad quadrata ipsa tantum, neque ad ipsorum ordinem radicumue signa respicitur.

IV. Posita multitudine omnium numerorum primorum imparium diuersorum ipsum M metientium $= \mu$, haud difficile ex art. 233 concluditur, multitudinem omnium valorum diuersorum expressionis $\sqrt{-(p, -q, r)}$ (mod. M) fore $= 2^{\mu}$, e quibus per art. 283 semissem tantum considerare oportet (quando $M > 2$). Qua-

re multitudo omnium repraesentationum propriarum formae φ per f erit $= 48.2^{\mu-1} = 3.2^{\mu+3}$; multitudo autem discerptionum diuersarum in terna quadrata $= 2^{\mu-1}$.

Ex. Sit $\varphi = 19tt + 6tu + 41uu$, adeoque $M = 770$; hic quatuor valores sequentes expr. $\sqrt{\ }-(19, -3, 41)$ (mod. 770) considerare oportet (art. 283): $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$. Vt inueniantur repraesentationes ad valorem $(39, 237)$ pertinentes, primo eruitur forma ternaria $\begin{pmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{pmatrix} = g$, in quam per praecepta art. 272, 275 f transire inuenitur per substitutionem

$$\begin{matrix} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{matrix}$$

vnde habetur repraesentatio formae φ per f haec: $x = t - 6u$, $y = -3t - 2u$, $z = -3t - u$; repraesentationes 47 reliquas ad eundem valorem pertinentes, quae ex horum valorum permutatione signorumque conuersione oriuntur, breuitatis caussa non adscribimus. Omnes vero 48 repraesentationes eandem discerptionem formae φ in tria quadrata $tt - 12tu + 36uu$, $9tt + 12tu + 4uu$, $9tt + 6tu + uu$ producunt.

Prorsus simili modo valor $(171, -27)$ suppeditat discerptionem in quadrata $(3t + 5u)^2$, $(3t - 4u)^2$, tt; valor $(269, -83)$ hanc $(t + 6u)^2 + (3t + u)^2 + (3t - 2u)^2$; denique valor $(291, -127)$ hanc $(t + 3u)^2 + (3t + 4u)^2 + (3t - 4u)^2$; singulae hae decompositiones

48 repraesentationibus aequipollent. — Praeter has 192 repraesentationes autem, siue quatuor discerptiones, aliae non dabuntur, quum 770 per nullum quadratum diuisibilis sit, adeoque repraesentationes impropriae exstare non possint.

290. De formis determinantis — 1 et — 2, quae quibusdam exceptionibus obnoxiae erant, paucis seorsim agemus. Praemittimus obseruationem generalem, si φ, φ' sint formae binariae aequiualentes quaecunque, (Θ) transformatio data illius in hanc, ex combinatione repraesentationis cuiusuis formae φ per aliquam ternariam f cum substitutione (Θ) prodire repraesentationem formae φ' per f; porro ex repraesentationibus propriis ipsius φ hoc modo oriri repraesentationes proprias formae φ', e diuersis diuersas, denique e cunctis cunctas. Haec omnia per calculum facillime comprobantur. Quare vna formarum φ, φ' totidem modis per f repraesentari poterit ac altera.

I. Sit primo $\varphi = tt + uu$, atque φ' forma quaecunque alia binaria positiua det. — 1, cui itaque φ aequiualebit; transeat φ in φ' per substitutionem $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. Forma φ repraesentatur per ternariam $f = xx + yy + zz$ ponendo $x = t$, $y = u$, $z = 0$; permutando x, y, z hinc emergunt *sex* repraesentationes, et e singulis rursus quatuor, mutando signa ipsorum t, u, ita vt omnino 24 repraesentationes diuersae habeantur, quibus vnica discerptio in tria quadrata aequipollet et praeter quas alias dari non posse facile perspicitur. Hinc concluditur,

etiam formam φ' vnico tantum modo in tria quadrata decomponi posse, puta in $(\alpha t' + \epsilon u')^2$, $(\gamma t' + \delta u')^2$ et 0, quae discerptio 24 repraesentationibus aequiualet.

II. Sit $\varphi = tt + 2uu$, φ' quaecunque alia forma binaria positiua det. — 2, in quam φ transeat per substitutionem $t = \alpha t' + \epsilon u'$, $u = \gamma t' + \delta u'$. Tunc simili modo vt in casu praec. concluditur, φ, et proin etiam φ', vnico tantum modo in tria quadrata discerpi posse, puta φ in $tt + uu + uu$, atque φ' in $(\alpha t' + \epsilon u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$; talem decompositionem 24 repraesentationibus aequipollere facile perspici potest.

Hinc colligitur, formas binarias determinantium — 1 et — 2 respectu multitudinis repraesentationum per ternariam $xx + yy + zz$ cum aliis formis binariis omnino conuenire; quum enim in vtroque casu fiat $\mu = 0$, formula in art. praec. IV. tradita vtique producit 24 repraesentationes. Ratio huius rei est, quod duae exceptiones, quibus tales formae obnoxiae erant, se mutuo compensant.

Theoriam generalem repraesentationum impropriarum in art. 284 explicatam ad formam $xx + yy + zz$ applicare, breuitatis gratia supersedemus.

291. Quaestio de inueniendis omnibus repraesentationibus propriis *numeri* positiui dati M per formam $xx + yy + zz$ primo per art. 281.

reducitur ad inuestigationem repraesentationum propriarum numeri $-M$ per formam $-xx - yy - zz = f$; hae vero per praecepta art. 280 ita eruuntur:

I. Euoluantur omnes classes formarum binariarum determinantis $-M$, quarum formae per $XX + YY + ZZ = F$ (cui formae ternariae adiuncta est f) proprie repraesentari possunt. Quando $M \equiv 0$, 4 vel 7 (mod. 8), tales classes per art. 288 non dantur, adeoque M in tria quadrata quae diuisorem communem non habeant discerpi nequit *). Quando vero $M \equiv 1$, 2, 5 vel 6, dabitur genus positiuum proprie primitiuum, et quando $M \equiv 3$, improprie primitiuum, quod omnes illas classes complectetur: designemus multitudinem harum classium per k.

II. Eligantur iam ex hisce classibus k formae ad lubitum, e singulis vna, quae sint ϕ, ϕ', ϕ'' etc.; inuestigentur omnes omnium repraesentationes propriae per F, quarum itaque multitudo erit $3.2^{\mu+3}k = K$, designante μ multitudinem factorum primorum (imparium) ipsius M; denique e quauis huiusmodi repraesentatione vt $X = mt + nu$, $Y = m't + n'u$, $Z = m''t + n''u$

*) Haec impossibilitas etiam inde manifesta, quod summa trium quadratorum imparium necessario fit $\equiv 3 \pmod 8$; summa duorum imparium cum vno pari vel $\equiv 2$ vel $\equiv 6$; summa vnius imparis cum duobus paribus vel $\equiv 1$ vel $\equiv 5$; denique summa trium parium vel $\equiv 0$ vel $\equiv 4$; sed in casu postremo repraesentatio manifesto est impropria.

deriuetur repraesentatio ipsius M per $xx + yy + zz$ haec $x = m'n'' - m''n'$, $y = m''n - mn''$, $z = mn' - m'n$. In complexu harum K repraesentationum, quem per Ω designemus, omnes repraesentationes ipsius M necessario contentae erunt.

III. Superest itaque tantummodo, vt inquiramus, num in Ω repraesentationes *identicae* occurrere possint; et quum ex art. 280, III iam constet, eas repraesentationes in Ω, quae e formis diuersis *e. g.* ex φ et φ' deriuatae sint, necessario diuersas esse, sola disquisitio restat, an repraesentationes diuersae eiusdem formae, *e. g.* ipsius φ, per F, repraesentationes identicas numeri M per $xx + yy + zz$ producere possint. Iam statim manifestum est, si inter repraesentationes ipsius φ reperiatur haec $(r) \ldots X = mt + nu$, $Y = m't + n'u$, $Z = m''t + n''u$, inter easdem fore hanc $(r') \ldots X = -mt - nu$, $Y = -m't - n'u$, $Z = -m''t - n''u$, atque ex vtraque deriuari eandem repraesentationem ipsius M, quae designetur per (R); examinemus itaque, num eadem (R) ex aliis adhuc repraesentationibus formae φ sequi possit. Ex art. 280, III facile deducitur, statuendo ibi $\chi = \varphi$, si omnes transformationes propriae formae φ in se ipsam exhibeantur per $t = \alpha t + \beta u$, $u = \gamma t + \delta u$, omnes eas repraesentationes formae φ, e quibus R sequatur, expressum iri per $x = (\alpha m + \gamma n)t + (\beta m + \delta n)u$, $y = (\alpha m' + \gamma n')t + (\beta m' + \delta n')u$, $z = (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u$. At e theoria transformationum formarum binariarum det. negatiui in art. 179 explicata sequitur,

in omnibus casibus praeter $M = 1$ et $M = 3$, duas tantummodo transformationes proprias formae φ in se ipsam dari, puta $\alpha, \beta, \gamma, \delta = 1, 0, 0, 1$ et $= -1, 0, 0, -1$ resp. (quum enim φ sit forma primitiua, id quod in art. 179 designabatur per m erit vel 1 vel 2, et proin, praeter casus exceptos, certo (1) locum ibi habebit). Quare (R) e solis r, r' prouenire poterit, adeoque quaeuis repraesentatio propria numeri M bis et non pluries in Ω reperietur, et multitudo omnium repraess. propriarum diuersarum ipsius M erit $\frac{1}{2}K = 3.2^{\mu+1}k$.

Quod attinet ad casus exceptos, multitudo transformationum propriarum formae φ in se ipsam per art. 179 erit 4 pro $M = 1$, et 6 pro $M = 3$; reueraque facile confirmatur, multitudinem repraesentationum propriarum numerorum 1, 3 esse $\frac{1}{4}K$, $\frac{1}{6}K$ resp.; scilicet vterque numerus vnico tantum modo in tria quadrata discerpi potest, 1 in $1 + 0 + 0$, 3 in $1 + 1 + 1$, discerptio ipsius 1 suppeditat sex, discerptio ipsius 3 octo repraesentationes diuersas; K vero fit $= 24$ pro $M = 1$ (vbi $\mu = 0, k = 1$) et $= 48$ pro $M = 3$ (vbi $\mu = 1, k = 1$).

Ceterum obseruamus, si h designet multitudinem classium in genere principali, cui multitudo classium in quouis alio genere proprie primitiuo per art. 252 aequalis est, fore $k = h$ pro $M \equiv 1, 2, 5$ vel 6 (mod. 8), sed $k = \frac{1}{3}h$ pro $M \equiv 3$ (mod. 8), vnico casu $M = 3$ excepto vbi $k = h = 1$. Pro numeris itaque formae $8n + 3$ multitudo repraesentationum *generaliter*

est $= 2^{\mu+\nu}h$, quum in numero 3 duae exceptiones sese compensent.

292. Discerptiones numerorum (vt formarum binariarum supra) in tria quadrata a repraesentationibus per formam $xx + yy + zz$ ita distinguimus, vt in illis ad solam quadratorum magnitudinem, in his vero insuper ad ipsorum ordinem radicumque signa respiciamus, adeoque repraesentationes $x = a$, $y = b$, $z = c$, et $x = a'$, $y = b'$, $z = c'$ pro diuersis habeamus nisi simul $a = a'$, $b = b'$, $c = c'$; discerptiones autem in $aa + bb + cc$ et in $a'a' + b'b' + c'c'$ pro vna, si nullo ordinis respectu habito haec quadrata illis aequalia sunt. Hinc patet,

I. Discerptionem numeri M in quadrata $aa + bb + cc$ aequipollere 48 repraesentationibus, si nullum sit $= 0$ omniaque inaequalia; 24 autem, si *vel* vnum $= 0$ reliqua inaequalia, *vel* nullum $= 0$ atque duo inter se aequalia. Si vero in discerptione numeri dati in tria quadrata duo ex his sunt $= 0$, *aut* vnum $= 0$ reliqua aequalia, *aut* omnia aequalia, repraesentationibus 6, *aut* 8, *aut* 12 aequiualens erit; sed haec euenire nequeunt nisi in casibus singularibus vbi $M = 1$ aut 2 aut 3 resp., siquidem repraesentationes esse debent propriae. His exclusis supponamus, multitudinem omnium discerptionum numeri M in terna quadrata (diuisoris communis expertia) esse E, atque inter has reperiri e in quibus vnum quadratum 0, et e' in quibus duo quadrata aequalia; illae etiam tamquam discerptiones in bina quadrata, hae tamquam discerptio-

nes in quadratum et quadratum duplum spectari possunt. Tunc multitudo omnium repraesentationum propriarum numeri M per $xx + yy + zz$ erit $= 24\,(e + e') + 48\,(E - e - e') = 48\,E - 24\,(e + e')$. At e theoria formarum binariarum facile deducitur, e fore vel $= 0$ vel $= 2^{\mu-1}$, prout -1 sit non-residuum vel residuum quadraticum ipsius M, nec non $e' = 0$ vel $= 2^{\mu-1}$, prout -2 non-residuum vel residuum ipsius M, denotante μ multitudinem factorum primorum (imparium) ipsius M (v. art. 182; expositionem vberiorem hic supprimimus). Hinc facile colligitur, fore $E = 2^{\mu-2}k$, si tum -1 tum -2 sit *N.R.* ipsius M; $E = 2^{\mu-2}(k+2)$, si vterque numerus sit residuum; denique $E = 2^{\mu-2}(k+1)$, si alter residuum sit alter non-residuum. In casibus exclusis $M = 1$ et $M = 2$, haec formula praeberet $E = \frac{3}{4}$, quum esse debeat $E = 1$; pro $M = 3$ autem recte prouenit $E = 1$, exceptionibus se mutuo compensantibus.

Si itaque M est numerus primus, fit $\mu = 1$, adeoque $E = \frac{1}{2}(k+2)$ quando $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k+1)$ quando $M \equiv 3$ aut $\equiv 5$. Haecce theoremata specialia ab ill. Le Gendre per inductionem dedecta et in commentatione egregia iam saepius laudata *Hist. de l'Ac. de Paris* 1785 *p.* 530 *sqq.* prolata fuerunt, etsi sub forma aliquantum diuersa, cuius rei ratio imprimis in eo est sita, quod aequiualentiam propriam ab impropria non distinxit, et proin classes oppositas commiscuit.

II. Ad inuentionem omnium discerptionum numeri M in terna quadrata (sine diu. comm.)

non opus est, omnes repraesentationes proprias omnium formarum Φ, Φ', Φ'' eruere. Primo enim facile confirmatur, omnes (48) repraesentationes formae Φ ad eundem valorem expr. $\sqrt{\ }-(p, -q, r)$ pertinentes (statuendo $\Phi = (p, q, r)$) discerptionem eandem numeri M praebere, adeoque sufficere, si vna ex illis habeatur, siue quod eodem redit, si tantummodo omnes diuersae discerptiones *) formae Φ in terna quadrata conscriptae sint, et perinde de reliquis Φ', Φ'' etc. Dein si Φ est e classe non ancipite, eam formam quae e classe opposita electa est omnino praeterire licebit, siue e binis classibus oppositis vnicam considerare sufficit. Quum enim prorsus arbitrarium sit, quaenam forma e singulis classibus eligatur, supponamus e classe opposita ei in qua est Φ eligi formam ipsi Φ oppositam, quae sit $= \Phi'$. Tunc nullo negotio perspicitur, si discerptiones propriae formae Φ indefinite exhibeantur per $(gt + hu)^2 + (g't + h'u)^2 + (g''t + h''u)^2$, omnes discerptiones formae Φ' expressum iri per $(gt - hu)^2 + (g't - h'u)^2 + (g''t - h''u)^2$, nec non ex his easdem discerptiones numeri M deriuari vt ex illis. Denique pro eo casu vbi Φ est forma e classe ancipite, attamen neque e classe principali neque formae $(2, 0, \frac{1}{2}M)$ aut $(2, 1, \frac{1}{2}(M + 1))$ aequiualens (prout M par aut impar), e valoribus expr. $\sqrt{\ }-(p, -q, r)$ semissem omittere licet; sed breuitatis caussa hocce compendium fusius hic non explicamus. — Ceterum iisdem compendiis etiam vti possumus,

*) Semper subintelligendum *propriae*, si hanc expressionem a repraesentationibus ad discerptiones transferre lubet.

quando omnes repraesentationes propriae ipsius M per $xx + yy + zz$ desiderantur, quum hae e discerptionibus facillime euoluantur.

Exempli caussa inuestigabimus omnes discerptiones numeri 770 in terna quadrata, vbi $\mu = 3$, $e = e' = 0$, adeoque $E = 2k$. Per classificationem formarum binariarum positiuarum determinantis — 770, quam quoniam a quouis ad normam art. 231 facile condi potest breuitatis gratia non adscribimus, inuenitur classium positiuarum multitudo = 32, quae omnes sunt proprie primitiuae et inter 8 genera distribuuntur, ita vt sit $k = 4$, et proin $E = 8$. Genus, cuius numerus characteristicus — 1, respectu numerorum 5, 7, 11 manifesto characteres particulares $R5$; $N7$; $N11$ habere debet, vnde per art. 263 facile concluditur, ipsius characterem respectu numeri 8 esse debere 1 et 3, 8. Iam in eo genere cuius character 1 *et* 3, 8; $R5$; $N7$; $N11$, quatuor classes reperiuntur, pro quarum repraesentantibus eligimus formas (6, 2, 129), (6, — 2, 129), (19, 3, 41), (19, — 3, 41); classem secundam vero et quartam reiicimus, vtpote primae et tertiae oppositas. Quatuor discerptiones formae (19, 3, 41) iam in art. 289 tradidimus, e quibus sequuntur discerptiones numeri 770 in 9 + 361 + 400, 16 + 25 + 729, 81 + 400 + 289, 576 + 169 + 25. Simili ratione inueniuntur quatuor discerptiones formae $6tt + 4tu + 129uu$ in $(t - 8u)^2 + (2t + u)^2 + (t + 8u)^2$, $(t - 10u)^2 + (2t + 5u)^2 + (t + 2u)^2$, $(2t - 5u)^2 + (t + 10u)^2 + (t + 2u)^2$, $(2t + 7u)^2 + (t - 8u)^2 + (t - 4u)^2$, resp. e valori-

bus expressionis $\sqrt{} - (6, -2, 129)$ hisce oriundae $(48, 369)$, $(62, -149)$, $(92, -159)$, $(202, -61)$; vnde prodeunt discerptiones numeri 770 in $225 + 256 + 289$, $1 + 144 + 625$, $64 + 81 + 625$, $16 + 225 + 529$. Praeter has octo discerptiones aliae non dantur.

Quae ad discerptiones numerorum in terna quadrata diuisores communes habentia attinent, tam facile e theoria generali art. 281 sequuntur, vt non opus sit huic rei immorari.

293. Disquisitiones praecedentes etiam suppeditant demonstrationem theorematis famosi, *omnem numerum integrum positiuum in tres numeros trigonales discerpi posse*, quod a Fermatio olim inuentum est, sed cuius demonstratio rigorosa hactenus desiderabatur. Manifestum est, quamuis discerptionem numeri M in trigonales $\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$ producere discerptionum numeri $8M + 3$ in terna quadrata imparia $(2x+1)^2 + (2y+1)^2 + (2z+1)^2$, et vice versa. Quiuis autem numerus integer positiuus $8M + 3$ per theoriam praecedentem in tria quadrata resolubis est, quae necessaria erunt imparia (V. annot. art. 291); resolutionumque multitudo pendet tum a multitudine factorum primorum ipsius $8M + 3$, tum a multitudine classium in quas formae binariae determinantis $-(8M + 3)$ distribuuntur. Totidem discerptiones numeri M in ternos trigonales dabuntur. Supponimus autem, $\frac{1}{2}x(x+1)$ pro valore quocunque integro ipsius x tamquam trigonalem spectari; quodsi magis placeret cifram

excludere, theorema ita immutare oporteret: Quiuis integer positiuus vel ipse trigonalis est, vel in duos vel in tres trigonales resolubilis. Similis mutatio in theoremate sequente facienda esset, si cifram a quadratis excludere placeret.

Ex iisdem principiis demonstratur aliud Fermatii theorema, *quemuis numerum integrum positiuum in quatuor quadrata decomponi posse.* Subtrahendo a numero formae $4n + 2$ quadratum arbitrarium (illo numero minus), a numero formae $4n + 1$ quadratum par, a numero formae $4n + 3$ quadratum impar, residuum in omnibus his casibus in tria quadrata resolubilis erit, adeoque numerus propositus in quatuor. Denique numerus formae $4n$ exhiberi potest per $4^{\mu}N$ ita vt N ad aliquam trium formarum praecedentium pertineat: resoluto autem ipso N in quatuor quadrata, etiam $4^{\mu}N$ resolutus erit. A numero formae $8n + 3$ etiam subduci potest quadratum radicis pariter paris, a numero formae $8n + 7$ quadratum radicis impariter paris, a numero formae $8n + 4$ quadratum impar, residuumque in tria quadrata resolubile erit. Ceterum hocce theorema iam ab ill. La Grange demonstratum erat, *Nouv. Mem. de l'Ac. de Berlin* 1770 *p.* 123, quam demonstrationem (a nostra prorsus diuersam) fusius explicauit ill. Euler in *Actis Ac. Petr. Vol. II. p.* 48. — Alia Fermatii thepraecedentium quasi continuationem constituunt, quinuis numerum integrum in quinque numeros pentagonales, sex hexagonales, septem heptagonales etc. resolubilem esse, demonstratione hactenus carent, aliaqua principia requirere videntur.

294. Theorema. *Designantibus a, b, c, numeros inter se primos quorum nullus neque* $= 0$ *neque per quadratum diuisibilis, aequatio* $axx + byy + czz = 0$ ... (Ω) *resolutionem in integris non admittet (praeter hanc* $x = y = z = 0$ *ad quam non respicimus) nisi* $-bc, -ac, -ab$ *resp. sint residua quadratica ipsorum a, b, c, atque hi numeri signis inaequalibus affecti; his vero quatuor conditionibus locum habentibus,* (Ω) *in integris resolubilis erit.*

Dem. Si (Ω) per integros omnino est resolubilis, etiam per tales valores ipsorum x, y, z resolui poterit qui diuisorem communem non habent; nam valores quicunque, aequ. Ω satisfacientes, etiamnum satisfacient, si per diuisorem communem maximum diuiduntur. Iam supponendo $app + bqq + crr = 0$, atque p, q, r a diuisore communi liberos, etiam inter se primi erunt; si enim q, r diuisorem communem μ haberent, hic ad p primus esset, $\mu\mu$ autem metiretur ipsum app adeoque etiam ipsum a, contra hyp.; et perinde p, r; p, q inter se primi erunt. Repraesentatur itaque $-app$ per formam binariam $byy + czz$, tribuendo ipsis y, z valores inter se primos q, r; vnde illius determinans $-bc$ residuum quadraticum ipsius app adeoque etiam ipsius a erit (art. 154); eodem modo erit $-acRb$, $-abRc$. Quod vero (Ω) resolutionem admittere non possit, si a, b, c idem signum habeant, tam obuium est vt explicatione non egeat.

Demonstrationem propositionis inuersae, quae theorematis partem secundam constituit, ita adornabimus, vt *primo* formam ternariam ipsi

$\begin{pmatrix} a, & b, & c \\ o, & o, & o \end{pmatrix} \ldots f$ aequiualentem inuenire doceamus, cuius coëfficientes 2, 3, 4 per abc diuisibiles sint, vnde *secundo* solutionem aequationis (Ω) deducemus.

I. Inuestigentur tres integri A, B, C a diuisore communi liberi, atque ita comparati, vt A primus sit ad b et c; B ad a et c; C ad a et b; $aAA + bBB + cCC$ autem per abc diuisibilis, quod efficietur sequenti modo. Sint $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ resp. valores expressionum $\sqrt{-bc}$ (mod. a), $\sqrt{-ac}$ (mod. b), $\sqrt{-ab}$ (mod. c), qui necessario ad a, b, c resp. primi erunt. Accipiantur tres integri $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ omnino ad lubitum, modo ita vt ad a, b, c resp. primi sint (e. g. omnes $= 1$), determinenturque A, B, C ita vt sit $A \equiv \mathfrak{b}c$ (mod. b) et $\equiv \mathfrak{c}\mathfrak{C}$ (mod. c); $B \equiv \mathfrak{c}a$ (mod. c) et $\equiv \mathfrak{a}\mathfrak{A}$ (mod. a), $C \equiv \mathfrak{a}b$ (mod. a) et $\equiv \mathfrak{b}\mathfrak{B}$ (mod. b). Tunc fiet $aAA + bBB + cCC \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} + c\mathfrak{b}\mathfrak{b}) \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A} - \mathfrak{A}\mathfrak{A}b) \equiv o$ (mod. a) siue per a diuisibilis, et perinde per b, c, adeoque etiam per abc diuisibilis erit. Praeterea patet, A necessario fieri primum ad b et c; B ad a et c; C ad a et b. Si vero hi valores ipsorum A, B, C diuisorem communem (maximum) μ implicant, hic manifesto ad a, b, c adeoque ad abc primus erit; quare illos valores per μ diuidendo nouos obtinebimus, qui diuisorem communem non habebunt, valorem ipsius $aAA + bBB + cCC$ etiamnum per abc diuisibilem producent, adeoque omnibus conditionibus satisfacient.

II. Numeris A, B, C, hoc modo determinatis, etiam Aa, Bb, Cc diuisorem communem

non habebunt. Si enim haberent diu. comm. μ, hic necessario primus esset ad a (quippe qui tum ad Bb tum ad Cc primus est) et similiter ad b et c; quare μ etiam ipsos A, B, C metiri deberet, contra hyp. Inueniri poterunt itaque integri α, β, γ tales vt sit $\alpha Aa + \beta Bb + \gamma Cc = 1$; quaerantur insuper sex integri α', β', γ', α'', β'', γ'' tales vt sit $\beta'\gamma'' - \gamma'\beta'' = Aa$, $\gamma'\alpha'' - \alpha'\gamma'' = Bb$, $\alpha'\beta'' - \beta'\alpha'' = Cc$. Iam transeat f per substitutionem

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

in $\begin{pmatrix} m, m', m'' \\ n, n', n'' \end{pmatrix} = g$ (quae ipsi f aequiualens erit), dicoque m', m'', n per abc diuisibiles fore. Ponatur enim $\beta''\gamma - \gamma''\beta = A'$, $\gamma''\alpha - \alpha''\gamma = B'$, $\alpha''\beta - \beta''\alpha = C'$, $\beta\gamma' - \gamma\beta' = A''$, $\gamma\alpha' - \alpha\gamma' = B''$, $\alpha\beta' - \beta\alpha' = C''$, eritque $\alpha' = B''Cc - C''Bb$, $\beta' = C'Aa - A''Cc$, $\gamma' = A''Bb - B''Aa$, $\alpha'' = C'Bb - B'Cc$, $\beta'' = A'Cc - C'Aa$, $\gamma'' = B'Aa - A'Bb$. Quibus valoribus in aequationibus $m' = a\alpha'\alpha' + b\beta'\beta' + c\gamma'\gamma'$, $m'' = a\alpha''\alpha'' + b\beta''\beta'' + c\gamma''\gamma''$, $n = a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma''$ substitutis, fit, secundum modulum a, $m' \equiv bcA'A''(BBb + CCc) \equiv 0$, $m'' \equiv bcA'A'(BBb + CCc) \equiv 0$, $n' \equiv bcA'A''(BBb + CCc) \equiv 0$, i. e. m', m'', n per a diuisibiles erunt; similique modo iidem numeri per b, c adeoque etiam per abc diuisibiles inueniuntur. *Q. E. P.*

III. Ponamus, concinnitatis caussa, determinantem formarum f, g, i. e. numerum $= abc$

$= d$, $md = M$, $m' = M'd$, $m'' = M''d$, $n = Nd$, $n' = N'$, $n'' = N''$, patetque f transire per substitutionem (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

in formam ternariam $\begin{pmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{pmatrix} = g'$, determinantis d^3, quae itaque sub f contenta erit. Iam dico, huic formae g' necessario aequiualere hanc $\begin{pmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{pmatrix} = g''$. Patet enim, $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix} = g'''$ fore formam ternariam determinantis 1; porro quum per hyp. a, b, c eadem signa non habeant, f erit forma indefinita, vnde facile concluditur etiam g' et g''' indefinitas esse debere; quare g''' aequiualebit formae $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$, (art. 277) poteritque transformatio (S') illius in hanc inueniri; manifesto autem per (S') forma g' transibit in g''. Hinc etiam g'' sub f contenta erit, et ex combinatione substitutionem (S), (S') deducetur transformatio formae f in g''. Quae si fuerit

$$\begin{matrix} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{matrix}$$

manifestum est, duplicem solutionem aequationis ( ) haberi, puta $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$, et $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; simul patet, neutros

valores simul = 0 euadere posse, quum necessario fiat $\delta'\varepsilon''\zeta''' + \delta''\varepsilon'''\zeta' + \delta'''\varepsilon'\zeta'' - \delta'''\varepsilon'\zeta' - \delta''\varepsilon''\zeta''' - \delta'\varepsilon'''\zeta'' = d$. *Q. E. S.*

Exemplum. Sit aequatio proposita $7xx - 15yy + 23zz = 0$, quae resolubilis est quia $345 R 7$, $-161 R 15$, $105 R 23$. Habentur hic valores ipsorum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ hi 3, 7, 6; faciendoque $a = b = c = 1$ inuenitur $A = 98$, $B = -39$, $C = -8$. Hinc eruitur substitutio

$$\begin{matrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{matrix}$$

per quam f transit in $\begin{pmatrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{pmatrix} = g$. Hinc fit

$$(S) = \begin{Bmatrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{Bmatrix}$$

$$g''' = \begin{pmatrix} 3670800, & 6, & -3 \\ -1, & -1246, & 4735 \end{pmatrix}$$

Forma g''' transire inuenitur in $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ per substitutionem

$$\left.\begin{matrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{matrix}\right\} \ldots (S')$$

qua cum (S) combinata prodit haec:

$$\begin{matrix} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3 \end{matrix}$$

per quam f transit in g''. Habemus itaque duplicem aequationis propositae solutionem $x = 11$, $y = 9$, $z = 4$, et $x = 12$, $y = -9$, $z = 3$; posterior simplicior redditur diuidendo valores per diuisorem communem 3, vnde $x = 4$, $y = -3$, $z = 1$.

295. Pars posterior theorematis art. praec. etiam sequenti modo absolui potest. Quaeratur integer h talis vt sit $ah \equiv \mathfrak{C} \pmod{c}$, (characteres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ eadem significatione accipimus vt in art. praec.), fiatque $ahh + b = ci$. Tunc facile perspicitur, i fieri integrum, numerumque $-ab$ esse determinantem formae binariae (ac, ah, i) ...Φ. Haec forma certo non erit positiua (quum enim per hyp. a, b, c eadem signa non habeant, ab et ac simul positiui esse nequeunt); porro habebit nnmerum characteristicum -1, quod synthetice ita demonstramus: Determinentur integri e, e' ita vt sit $e \equiv 0 \pmod{a}$ et $\equiv \mathfrak{B} \pmod{b}$; $ce' \equiv \mathfrak{A} \pmod{a}$ et $\equiv h\mathfrak{B} \pmod{b}$, eritque (e, e') valor expr. $\sqrt{-(ac, ah, i)}$. Nam secundum modulum a erit $ee \equiv 0 \equiv -ac$, $ee' \equiv 0 \equiv -ah$, $cce'e' \equiv \mathfrak{A}\mathfrak{A} \equiv -bc \equiv -cci$ adeoque $e'e' \equiv -i$; secundum modulum b autem erit $ee \equiv \mathfrak{B}\mathfrak{B} \equiv -ac$, $cee' \equiv h\mathfrak{B}\mathfrak{B} \equiv -ach$ adeoque $ee' \equiv -ah$, $cce'e' \equiv hh\mathfrak{B}\mathfrak{B} \equiv -achh \equiv -cci$ adeoque $e'e' \equiv -i$; eaedem vero tres congruentiae quae secundum vtrumque

modulum a, b locum habent, etiam secundum modulum ab valebunt. Hinc per theoriam formarum ternariarum facile concluditur, ϕ repraesentabilem esse per formam $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$; sit itaque $actt + 2ahtu + iuu = -(\alpha t + \mathfrak{G}u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$, eritque, multiplicando per c, $a(ct + hu)^2 + buu = -c(\alpha t + \mathfrak{G}u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u)$. Hinc patet, si ipsis t, u tales valores determinati tribuantur, vt vel $\gamma t + \delta u$, vel $\varepsilon t + \zeta u$ fiat $= 0$, haberi solutionem aequationis Ω, cui igitur satisfiet tum per $x = \delta c - \gamma h$, $y = \gamma$, $z = \alpha\delta - \mathfrak{G}\gamma$, tum per $x = \zeta c - \varepsilon h$, $y = \varepsilon$, $z = \alpha\zeta - \mathfrak{G}\varepsilon$; simul manifestum est, neque illos valores neque hos simul $= 0$ fieri posse; si enim $\delta c - \gamma h = 0$, $\gamma = 0$, fieret etiam $\delta = 0$ atque $\phi = -(\alpha t + \mathfrak{G}u)^2$ vnde $ab = 0$ contra hyp., et perinde de alteris. — In exemplo nostro inuenimus formam ϕ hanc $(161, -63, 24)$, valorem expr. $\sqrt{-\phi}$ (mod. 105) $= (7, -51)$, atque repraesentationem formae ϕ per $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ hanc, $\phi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$; hinc prodeunt solutiones $x = 7$, $y = 11$, $z = -8$; $x = 20$, $y = 15$, $z = -5$, siue diuidendo per 5 et negligendo signum ipsius z, $x = 4$, $y = 3$, $z = 1$.

Ex his duabus methodis aequationem Ω soluendi posterior eo praestat, quod plerumque per numeros minores absoluitur; prior vero, quae etiam per varia artificia hic silentio praetereunda contrahi potest, elegantior videtur ea imprimis ratione, quod numeri a, b, c prorsus eodem

modo tractantur, calculusque per horum permutationem quamcunque nihil mutatur. Hoc secus se habet in methodo secunda, vbi calculus maxime commodus plerumque prouenit, si pro a accipitur minimus, pro c maximus trium numerorum datorum, vti in exemplo nostro fecimus.

296. Elegans theorema in artt. praecc. explicatum primo inuentum est ab ill. Le Gendre, *Hist. de l'Ac. de Paris* 1785 *p.* 507, atque demonstratione pulcra (a duabus nostris omnino diuersa) munitum. Simul vero hic egregius geometra hoc loco operam dedit, demonstrationem propositionum quae cum theoremate fundamentali sect. praec. conueniunt inde deriuare, quam ad hunc scopum non idoneam nobis videri iam supra declarauimus, art. 151. Hic itaque locus erit, hanc demonstrationem (per se valde elegantem) breuiter exponendi iudiciique nostri rationes adiungendi. Praemittitur sequens obseruatio: *Si numeri* a, b, c *omnes sunt* $\equiv 1 \pmod 4$, *aequatio* $axx + byy + czz = 0$ ... (Ω) *solubilis esse nequit.* Facillime enim perspicitur, valorem ipsius $axx + byy + czz$ necessario in hoc casu fieri vel $\equiv 1$, vel $\equiv 2$, vel $\equiv 3 \pmod 4$, nisi omnes x, y, z simul pares accipiantur; si itaque Ω solubilis esset, hoc aliter fieri non posset quam per valores pares ipsorum x, y, z, *Q. E. A.*, quoniam valores quicunque aequationi Ω satisfacientes etiamnum satisfaciunt, si per diuisorem communem maximum diuiduntur, vnde necessario ad minimum vnus impar prodire debet. Iam casus diuersi theorematis demonstrandi ad sequentia momenta referuntur:

I. Designantibus p, q numeros primos formae $4n + 3$ (positiuos inaequales), nequit simul esse pRq, qRp. Si enim possibile esset, manifestum est statuendo $1 = a$, $-p = b$, $-q = c$, omnes conditiones ad resolubilitatem aequationis $axx + byy + czz = 0$ adimpletas esse (art. 294); eadem vero per obseruationem praec. resolutionem non admittit; quare suppositio consistere nequit. Hinc protinus sequitur propositio 7 art. 131.

II. Si p est numerus primus formae $4n + 3$, nequit simul esse qRp, pNq. Alioquin enim foret $-pRq$, atque aequatio $xx + pyy - qzz = 0$ resolubilis, quae per obs. praec. resolutionem respuit. Hinc deriuantur casus 4 et 5 art. 131.

III. Si p, q sunt numeri primi formae $4n + 1$, nequit simul esse pRq, qNp. Accipiatur alius numerus primus r formae $4n + 3$, qui sit residuum ipsius q et cuius non-residuum sit p. Tunc erit per casus modo (II) demonstratos qRr, rNp. Si itaque esset pRq, qNq, foret $qrRp$, pRq, $pqNr$ et proin $-pqRr$. Hinc aequatio $pxx + qyy - rzz = 0$ resolubilis esset contra obs. praec.; quare suppositio consistere nequit. Hinc sequuntur casus 1 et 2 art. 131.

Concinnius hic casusse quenti modo tractatur. Designet r numerum primum formae $4n + 3$ cuius non residuum sit p. Tunc erit etiam rNp, adeoque (supponendo pRq, qNp) $qrRp$, porro $-pRq$, $-pRr$ et proin etiam $-pRqr$; quare

aequatio $xx + pyy - qrzz = 0$ resolubilis esset contra obs. praec. Hinc etc.

IV. Si p est numerus primus formae $4n + 1$, q primus formae $4n + 3$, nequit simul esse pRq, qNp. Accipiatur numerus primus auxiliaris r formae $4n + 1$ qui sit non residuum vtriusque p, q. Tunc erit (per II) qNr et (per III) pNr; hinc $pqRr$; si itaque esset pRq, qNp, haberetur etiam $prNq$, $-prRq$, $qrRp$; quare aequatio $pxx - qyy + rzz = 0$ resolubilis esset, *Q. E. A.* — Hinc deriuantur casus 3 et 6 art. 131.

V. Designantibus p, q numeros primos formae $4n + 3$, nequit simul esse pNq, qNp. Supponendo enim fieri posse, et accipiendo numerum primum auxiliarem r formae $4n + 1$ qui sit non residuum vtriusque p, q erit $qrRp$, $prRq$; porro (per II) pNr, qNr, vnde $pqRr$ et $-pqRr$; hinc aequatio $-pxx - qyy + rzz = 0$ possibilis, contra obs. praec. Hinc deducitur casus 8 art. 131.

297. Demonstrationem praec. proprius contemplando quisque facile intelliget, casus I et II ita absolutos esse vt nihil obiici possit. At demonstrationes casuum reliquorum innituntur existentiae numerorum auxiliariorum, qua nondum demonstrata methodus manifesto omnem vim perdit. Quae suppositiones, etsi tam speciosae sint, vt minus attendenti demonstratione ne opus quidem habere videri possint, atque certe theorema demonstrandum ad maximum *probabilitatis* gradum euehant, tamen si rigor geometricus

desideretur, neutiquam gratuito sunt admittendae. Quod quidem attinet ad suppositionem in IV et V, exstare numerum primum r formae $4n + 1$, qui duorum aliorum primorum datorum p, q non residuum sit, e Sect. IV facile concluditur, omnes numeros ipso $4pq$ minores ad ipsumque primos (quorum multitudo est $2(p-1)(q-1)$) in quatuor classes aequaliter distribui, quarum vna contineat non residua vtriusque p, q, tres reliquae residua ipsius p non residua ipsius q, non residua ipsius p residua ipsius q, residua vtriusque p, q; et in singulis classibus semissem fore numeros formae $4n + 1$, semissem formae $4n + 3$. Habebuntur itaque inter illos $\frac{1}{4}(p-1)(q-1)$ non residua vtriusque p, q formae $4n + 1$, qui sint g, g', g'' etc.; numeri $\frac{3}{4}(p-1)(q-1)$ reliqui sint h, h', h'' etc. Manifesto omnes numeri in formis $4pqt + g$, $4pqt + g'$, $4pqt + g''$ etc. (G) contenti quoque erunt non residua ipsorum p, q formae $4n + 1$. Iam patet, ad suppositionem stabiliendam demonstrari tantummodo debere, sub formis (G) certo contineri *numeros primos*, quod sane iam per se valde plausibile videtur, quum hae formae vna cum his $4pqt + h$, $4pqt + h'$ etc. (H) omnes numeros ad $4pq$ primos adeoque etiam omnes numeros absolute primos (praeter 2, p, q) comprehendant, nullaque ratio adsit, quin numerorum primorum series inter illas formas aequaliter distributi sint, ita vt pars octaua referantur ad (G), reliqui ad (H). Attamen perspicuum est, tale ratiocinium a rigore geometrico longe abesse. Ill. Le Gendre ipse fatetur, demonstrationem theorematis, sub tali forma $kt + l$, designantibus

k, l numeros inter se primos datos, t indefinitum, certo contineri numeros primos, satis difficilem videri, methodumque obiter addigitat, quae forsan illuc conducere possit; multae vero disquisitiones praeliminares necessariae nobis videntur, antequam hacce quidem via ad demonstrationem rigorosam peruenire liceat. — — Circa aliam vero suppositionem (III, meth. secunda) dari numerum primum r formae $4n + 3$ cuius non residuum sit alius numerus primus datus p formae $4n + 1$, ill. Le Gendre nihil omnino adiecit. Supra demonstrauimus (art. 129), numeros primos quorum $N.R.$ sit p certo dari, sed methodus nostra haud idonea videtur ad existentiam talium numerorum primorum *qui simul sint formae* $4n + 3$ ostendendam (vt hic requiritur neque vero in dem. nostra prima). Ceterum veritatem quidem huius suppositionis ita facile probare possumus. Per art. 287 dabitur genus positiuum formarum binariarum det. $= p$, cuius character 3, 4; Np; sit (a, b, c) talis forma atque a impar (quod supponere licet). Tum a erit formae $4n + 3$ atque vel ipse primus vel saltem factorem primum r formae $4n + 3$ implicabit. Erit autem $= pRa$, adeoque etiam $= pRr$, vnde pNr. At probe notandum est, propp. artt. 263, 287 theoremati fundamentali inniti, adeoque circulum vitiosum fore, si qua huius pars illis superstruatur. — — Denique suppositio in methodo prima II adhuc multo magis gratuita est, ita vt non opus sit plura de illa hic adiicere.

Liceat obseruationem addere circa casum V, qui per methodum praec. quidem non satis pro-

batur, attamen per sequentem commode absolutur. Si illic simul esset pNq, qNp, foret $-pRq$, $-qRp$, vnde facile deriuatur, — 1 esse numerum characteristicum formae $(p, 0, q)$, quae proin, (secundum theoriam formarum ternariarum) per formam $xx + yy + zz$ repraesentari poterit. Sit $ptt + quu = (\alpha t + \mathfrak{E}u)^2 + (\alpha' t + \mathfrak{E}' u)^2 + (\alpha'' t + \mathfrak{E}'' u)$, siue $\alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' = p$, $\mathfrak{E}\mathfrak{E} + \mathfrak{E}'\mathfrak{E}' + \mathfrak{E}''\mathfrak{E}'' = q$, $\alpha\mathfrak{E} + \alpha'\mathfrak{E}' + \alpha''\mathfrak{E}'' = 0$, eruntque ex aequatt. 1 et 2, omnes α, α', α'', $\mathfrak{E}$, $\mathfrak{E}'$, $\mathfrak{E}''$ impares; tum vero manifesto aequatio tertia consistere nequit. — Haud absimili modo etiam casus II absolui potest.

298. Problema. *Designantibus a, b, c numeros quoscunque, quorum tamen nullus* $= 0$: *inuenire conditiones resolubilitatis aequationis* $axx + byy + czz = 0 \ldots (\omega)$.

Sol. Sint $\alpha\alpha$, $\mathfrak{E}\mathfrak{E}$, $\gamma\gamma$ quadrata maxima ipsos bc, ac, ab resp. metientia, fiatque $\alpha a = \mathfrak{E}\gamma A$, $\mathfrak{E}b = \alpha\gamma B$, $\gamma c = \alpha\mathfrak{E}C$. Tum A, B, C erunt integri, inter se primi; aequatio (ω) autem resolubilis erit vel non erit, prout haec $AXX + BYY + CZZ = 0 \ldots (\Omega)$ resolutionem admittit vel non admittit, quod per art. 294 diiudicari poterit.

Dem. Ponatur $bc = \mathfrak{A}\alpha\alpha$, $ac = \mathfrak{B}\mathfrak{E}\mathfrak{E}$, $ab = \mathfrak{C}\gamma\gamma$, eruntque $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ integri a factoribus quadratis liberi atque $\mathfrak{A} = BC$, $\mathfrak{B} = AC$, $\mathfrak{C} = AB$; hinc $\mathfrak{A}\mathfrak{B}\mathfrak{C} = (ABC)^2$, adeoque $ABC = A\mathfrak{A} = B\mathfrak{B} = \mathfrak{C}C$ necessario integer. Sit numerorum $\mathfrak{A}$, $A\mathfrak{A}$ diuisor comm. max. m, atque $\mathfrak{A}$

$= gm$, $A\mathfrak{A} = hm$, eritque g primus ad h, nec non (quia $\mathfrak{A}$ liber a fact. qu.) ad m. Iam fit $hhm = gAA\mathfrak{A} = g\mathfrak{BC}$, vnde g metietur ipsum hhm, quod manifesto impossibile est, nisi $g = \pm 1$. Hinc $\mathfrak{A} = \pm m$, $A = \pm h$, et proin integer, et perinde B, C integri erunt. *Q. E. P.* — Quam $\mathfrak{A} = BC$ factores quadratos non implicet, necessario B, C inter se primi esse debebunt; et similiter A ad C et ad B primus erit. *Q. E. S.* — Denique patet, si aequationi (Ω) satisfaciat $X = P$, $Y = Q$, $Z = R$, aequationem ( ) resolui per $x = \alpha P$, $y = \mathfrak{C}Q$, $z = \gamma R$; et vice versa si huic satisfiat per $x = p$, $y = q$, $z = r$, illi satisfieri per $X = \mathfrak{C}\gamma p$, $Y = \alpha\gamma q$, $Z = \alpha\mathfrak{C}r$, vnde vel vtraque resolubilis vel neutra. *Q. E. T.*

299. Problema. *Proposita forma ternaria* $f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$, *inuenire, an cifra per eam repraesentari possit (per valores indeterminatarum qui non simul* $= 0$*).*

Sol. I. Quando $a = 0$, valores ipsorum x', x'' ad lubitum assumi possunt, patetque ex aequatione $a'x'x' + 2bx'x'' + a''x''x'' = -2x\,b'x'' + b''x')$, x inde valorem determinatum rationalem nancisci; quoties pro x hoc modo fractio prouenit, oportet tantummodo, valores ipsorum x, x', x'' per fractionis denominatorem multiplicare, habebunturque integri. Vnice excludendi sunt tales valores ipsorum x', x'', qui reddunt $b'x'' + b''x' = 0$, nisi simul faciant $a'x'x' + 2bx'x'' + a''x''x'' = 0$, in quo casu x ad libitum accipi poterit. Simul patet, hoc modo omnes

solutiones possibiles obtineri posse. Ceterum is casus vbi b' et $b'' = 0$ huc non pertinet; tunc enim x in f non ingreditur, siue f est forma binaria, cifraeque repraesentabilitas per f e theoria talium formarum diiudicari debet.

II. Quando vero non est $a = 0$, aequationi $f = 0$ aequiualebit haec $(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = 0$, ponendo $b''b'' - aa' = A''$, $ab - b'b'' = B$, $b'b' - aa'' = A'$. Iam quando hic $A'' = 0$, neque vero $B = 0$, manifestum est, si $ax + b''x' + b'x''$ atque x'' ad lubitum assumantur, x et x' inde rationaliter determinari, et quando integri non fiant, saltem multiplicatorem idoneum integros producturum. Pro vnico valore ipsius x'' valor ipsius $ax + b''x' + b'x''$ non est arbitrarius sed quoque $= 0$ poni debet; tunc vero x' ad lubitum assumi poterit valoremque rationalem ipsius x producet. — Quando vero simul A'' et $B = 0$, patet, si A'' sit quadratum $= kk$, aequationem $f = 0$ reduci ad has duas lineares (e quibus *vel* vna *vel* altera locum habere debet) $ax + b''x' + (b' + k)x'' = 0$, $ax + b''x' + (b' - k)x'' = 0$; si vero (in eadem hyp.) A'' est nonquadratus, manifesto solutio aequ. propositae pendet ab his (quae *simul* locum habere debent) $x'' = 0$ et $ax + b''x' = 0$.

Ceterum vix necessarium erit obseruare, methodum in I etiam applicari posse, quando a' vel $a'' = 0$, methodumque in II quando $A' = 0$.

III. Quando vero nec a nec $A'' = 0$, aequationi $f = 0$ aequiualet haec $A'(ax + b''x' + b'x'')$

$-(A''x' - Bx'')^2 + Dax''x'' = 0$, designando per D determinantem formae f siue per Da numerum $BB - A'A''$. Quando $D = 0$, solutio simili modo se habebit vt in fine casus praec.; scilicet si A' est quadratum $= kk$, aequ. prop. reducitur ad has $kax + (kb'' - A'')x' + kb' + B)x'' = 0$, $kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$; si vero A' est non quadratus, fieri debet $ax + b''x' + b'x'' = 0$, $A''x' - Bx'' = 0$. Quando autem D non $= 0$, reducti sumus ad aequationem $A'tt - uu + Davv = 0$, cuius possibilitas per art. praec. diiudicari potest. Quodsi haec aliter resolui nequit, quam per $t = 0$, $u = 0$, $v = 0$, manifesto etiam proposita aliam solutionem non admittet, quam hanc $x = 0$, $x' = 0$, $x'' = 0$; si vero illa aliter solubilis est, e valoribus integris quibusuis ipsorum t, u, v deriuabuntur, per aequationes $ax + b''x' + b'x'' = t$, $A''x' - Bx'' = u$, $x'' = v$, saltem valores rationales ipsorum x, x', x'', e quibus si fractiones inuoluunt per idoneum multiplicatorem integri elici poterunt.

Quamprimum autem *vna* solutio aequationis $f = 0$ in integris inuenta est, problema ad casum I reduci, et perinde ac illic solutiones omnes exhiberi poterunt sequenti modo Satisfaciant aequationi $f = 0$ valores ipsorum x, x', x'' hi α, α', α'', quos a factoribus communibus liberos supponimus, accipiantur (per artt. 40, 279) integri ξ, ξ', ξ'', γ, γ', γ'' tales vt sit $\alpha(\xi'\gamma'' - \xi''\gamma') + \alpha'(\xi''\gamma - \xi\gamma'') + \alpha''(\xi\gamma' - \xi'\gamma) = 1$, transeatque f per substitutionem (S) ... $x = \alpha y + \xi y' + \gamma y''$, $x' = \alpha' y + \xi' y' + \gamma' y''$, $x'' = \alpha'' y + \xi'' y' + \gamma'' y''$

in $g = cyy + c'y'y' + c''y''y'' + 2dy'y'' + 2d'yy'' + 2d''yy'$. Tunc manifesto erit $c = 0$, atque g ipsi f aequiualens, vnde facile concluditur, ex omnibus solutionibus aequationis $g = 0$ deriuari (per S) omnes solutiones aequationis $f = 0$ in integris. Iam ex I sequitur, omnes solutiones aequ. $g = 0$ contineri sub formulis $y = -z(c'pp + 2dpq + c''qq)$, $y' = 2z(d''pp + d'pq)$, $y'' = 2z(d''dq + d'qq)$, designantibus p, q integros indefinitos, z numerum indefinitum pro quo etiam fractiones accipi possunt, modo ita vt y, y', y'' integri maneant. His valoribus ipsorum y, y', y'' in (S) substitutis, omnes solutiones aequ. $f = 0$ in integris habebuntur. — Ita *e. g.* si $f = xx + x'x' + x''x'' - 4x'x'' + 2xx'' + 8xx'$, atque vna solutio aequationis $f = 0$ habetur $x = 1$, $x' = -2$, $x'' = 1$: faciendo ξ, ξ', ξ'', η, η', η'' $= 0, 1, 0, 0, 0, 1$ prodit $g = y'y' + y''y'' - 4y'y'' + 12yy''$. Hinc omnes solutiones aequ. $g = 0$ in integris contenti erunt sub formula $y = -z(pp - 4pq + qq)$, $y' = 12zpq$, $y'' = 12zqq$, et proin omnes solutiones aequ. $f = 0$ sub hac $x = -z(pp - 4pq + qq)$, $x' = 2z(pp + 2pq + qq)$, $x'' = -z(pp - 4pq - 11qq)$.

300. E problemate art. praec. sponte defluit solutio aequationis indeterminatae $axx + 2bxy + cyy + 2dx + 2ey + f = 0$, si valores tantummodo rationales desiderantur, quam, si integri postulantur, supra (art. 216 sqq.) iam absoluimus. Nam omnes valores rationales ipsorum x, y exhiberi possunt per $\frac{t}{v}$, $\frac{u}{v}$, ita vt t, u,

v sint integri, vnde patet, solutionem illius aequationis per numeros rationales identicam esse cum solutione aequationis $att + 2btu + cuu + 2dtv + 2euv + fvv = 0$ per numeros integros; haec vero conuenit cum aequ. in art. praec. tractata. Excludi debent eae solae solutiones vbi $v = 0$; tales autem prouenire nequeunt, quando $bb - ac$ est numerus non-quadratus. Ita e. g. omnes solutiones aequationis (in art. 221 per integros generaliter solutae) $xx + 8xy + yy + 2x - 4y + 1 = 0$ per numeros rationales contentae erunt sub formula

$$x = \frac{pp - 4pq + qq}{pp - 4pq + 11qq}, \quad y = -\frac{2pp + 4pq + 2qq}{pp - 4pq + 11qq}$$

designantibus p, q integros quoscunque. — Ceterum de his duobus problematibus arctissimo nexu coniunctis breuiter tantummodo hic egimus, multasque obseruationes huc pertinentes suppressimus, tum ne nimis prolixi fieremus, tum quod solutionem aliam probl. art. praec. habemus, principiis generalioribus innixam, cuius expositionem, quia penitiorum formarum ternariarum disquisitionem postulat, ad aliam occasionem nobis reseruare debemus.

301. Reuertimus ad formas binarias, de quibus adhuc plures proprietates singulares recensere oportet. Et primo quasdam obseruationes circa multitudinem generum et classium in ordine proprie primitiuo (positiuo pro det. neg.) adiicemus, ad quem breuitatis caussa disquisitionem restringimus.

Multitudo generum, in quae omnes formae (pr. prim. pos.) determinantis dati positiui vel negatiui $\pm D$ distribuuntur, semper est 1, 2, 4 vel altior potestas numeri 2, cuius exponens pendet a factoribus ipsius D, et per disquisitiones praec. omnino a priori inueniri potest. Iam quum in serie numerorum naturali numeri primi cum magis minusque compositis permixti sint, euenit, vt pro pluribus determinantibus successiuis $\pm D$, $\pm(D+1)$, $\pm(D+2)$ etc. multitudo generum nunc crescat nunc decrescat, nullusque in hac serie perturbata ordo adesse videatur. Nihilominus si multitudines generum multis dett. successiuis $\pm D$, $\pm(D+1)\ldots\pm(D+m)$ respondentes adduntur, summaque per determinantium multitudinem diuiditur, *multitudo generum mediocris* prouenit, quae circa medium determinantium $\pm(D+\frac{1}{2}m)$ locum habere censeri poterit, progressionemque valde regularem constituit. Supponimus autem, non modo m esse satis magnum, sed etiam D multo maiorem, vt ratio determinantium extremorum D, $D+m$ non nimis a ratione aequalitatis discrepet. Regularitas illius progressionis ita intelligenda est: si D' est numerus multo maior quam D, multitudo generum mediocris circa determinantem $\pm D'$ sensibiliter maior erit quam circa D; si vero D, D' non nimis differunt, etiam generum multitudines mediocres circa D et D' fere aequales erunt. Ceterum multitudo mediocris generum circa determinantem positiuum $+D$ semper fere aequalis inuenitur multitudini mediocri circa negatiuum, eoque exactius quo maior est D, quum pro valore paruo prior paullulum maior euadat

quam posterior. Hae obseruationes magis illustrabuntur per exempla sequentia, e tabula classificationis formarum binariarum plures quam 4000 determinantes complectente excerpta. Inter centum determinantes a 801 vsque ad 900 reperiuntur 7 quibus vnicum genus respondet; 32, 52, 8, 1 quibus resp. 2, 4, 8, 16 genera respondent; hinc omnino emergunt genera 359, vnde multitudo mediocris = 3,59. Centum determinantes negatiui a —801 vsque ad —900 producunt genera 360. Exempla sequentia omnia desumuntur a determinantibus negatiuis. In centade 16 (a —1501 vsque ad —1600) mult. med. generum inuenitur 3,89; in centade 25 est 4,01; in centade 51 prodit 4,24; e sexcentis dett. —9401 ... —10000 computatur 4,59. Ex his exemplis patet, multitudinem generum mediocrem multo lentius crescere, quam determinantes ipsos; sed quaeritur, quaenam sit lex huius progressionis? — Per disquisitionem theoreticam satis difficilem, quam hic explicare nimis prolixum foret, inuentum est, multitudinem generum mediocrem circa determinantem $+D$ vel $-D$ quam proxime exhiberi per formulam $\alpha \log D + \mathfrak{C}$, vbi α, $\mathfrak{C}$ sunt quantitates constantes, et quidem $\alpha = \frac{4}{\pi\pi} =$ 0,4052847346 (designante π semiperipheriam circuli cuius radius 1), $\mathfrak{C} = 2g + 3\alpha\alpha h - \frac{1}{6}\alpha \log 2 =$ 0,8830460462, vbi g est summa seriei $1 - \log(1+1) + \frac{1}{2} - \log(1+\frac{1}{2}) + \frac{1}{3} - \log(1+\frac{1}{3}) +$ etc. = 0,5772156649 (V. Euler Inst. Calc. Diff. p. 444); h vero summa seriei $\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 +$ etc., quae per approximationem inuenta est = 0,9375482543. Ex

hac formula patet, multitudinem mediocrem generum crescere in progressione arithmetica, si determinantes augeantur in geometrica. Valores huius formulae pro $D = 850\frac{1}{2}$, $1550\frac{1}{2}$, $2450\frac{1}{2}$, $5050\frac{1}{2}$, $9700\frac{1}{2}$ inueniuntur 3,627; 3,86; 4,046; 4,339; 4,601, qui a multitudinibus mediocribus supra datis parum discrepant. Quo maior fuerit determinans medius, et e quo pluribus multitudo mediocris computetur, eo minus a valore formulae differet. Adiumento huius formulae etiam aggregatum multitudinum generum determinantibus successiuis $\pm D$, $\pm(D+1)$... $\pm(D+m)$ respondentium quam proxime erui potest, si multitudines mediocres singulis respondentes computantur et in summam colliguntur, quantumuis diuersi sint extremi D, $D+m$. Haec summa erit $= \alpha(\log D + \log(D+1 + \text{etc.} + \log(D+m)) + \mathfrak{G}(m+1)$ siue satis exacte $= \alpha((D+m)\log(D+m) - (D-1)\log(D-1)) + (\mathfrak{G} - \alpha)(m+1)$. Hoc modo summa mult. gen. pro dett. -1 vsque ad -100 inuenitur $= 234{,}4$ quum reuera sit 233; similiter, a -1 vsque ad -2000, $= 7116{,}6$, quum sit 7108; a -9001 vsque ad -10000 vbi est 4595 formula praebet 4594,9 qualis consensus vix exspectari potuisset.

302. Respectu *multitudinis classium* (pr. primit. posit., quod semper subintelligendum) determinantes positiui prorsus aliter se habent quam negatiui; quamobrem vtrosque seorsim considerabimus. In eo hi cum illis conueniunt, quod pro determinante dato in singulis generibus classes aeque multae continentur, adeoque multitudo omnium classium aequalis est producto e multi-

tudine generum in multitudinem classium in singulis generibus contentarum.

Quod primo attinet ad determinantes negatiuos, multitudo classium pluribus dett. successiuis $-D$, $-(D+1)$, $-(D+2)$ etc. respondentium progressionem aeque perturbatam constituit, ac multitudo generum. Multitudo classium mediocris autem (quae definitione opus non habebit) valde regulariter crescit, vt ex exemplis sequentibus apparebit. Centum determinantes a -500 vsque ad -600 suppeditant classes 1729, vnde multitudo mediocris $= 17{,}29$. Similiter in centade 15 multitudo classium mediocris inuenitur 28,26; e centadibus duabus 24 et 25 computatur 36,28; e tribus 61, 62 et 63 prodit 58,50 e quinque $91 = 95$, fit 71,56; denique e quinque $96 = 100$ fit 73,54. Haec exempla ostendunt, classium multitudinem mediocrem lentius quidem crescere, quam determinantes, multo tamen citius, quam multitudinem mediocrem generum; leui autem attentione cognoscetur, illam satis exacte crescere in ratione radicum quadratarum e determinantibus mediis. Reuera per disquisitionem theoreticam inuenimus, classium multitudinem mediocrem circa determinantem $-D$ proxime exprimi per $\gamma\sqrt{D} - \delta$, vbi $\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$, denotante e summam seriei $1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125}$ etc.; $\delta = 0{,}2026423673 = \frac{2}{\pi\pi}$: valores mediocres secundum hanc formulam computati ab iis quos supra e tabula classificationum excripsimus pa-

rum differunt. Adiumento huius formulae etiam aggregatum multitudinum omnium classium (pr. pr. pos.) determinantibus successiuis $-D$, $-(D+1)$, $-(D+2)\ldots-(D+m-1)$ respondentium quam proxime assignari potest, quantumuis extremi sint diuersi, summando multitudines mediocres illis determinantibus secundum formulam respondentes, vnde erit $= \gamma(\sqrt{D}+\sqrt{(D+1)}+$ etc. $+\sqrt{(D+m-1)}) + \delta m$ siue quam proxime $= \frac{2}{3}((D+m-\frac{1}{2})^{\frac{3}{2}} - (D-\frac{1}{2})^{\frac{3}{2}}) + \delta m$. Ita e. g. illud aggregatum pro centum dett. $-1\ldots-100$ ex formula computatur $= 481{,}1$, quum reuera sit 477; mille determinantes $-1\ldots-1000$ secundum tabulam suppeditant 15533 classes, formula dat 15551,4; millias secunda sistit classes 28603 secundam tabulam, formula praebet 28585,7; similiter millias tertia reuera suggerit 37112 classes, formula dat 57074,3; millias decima dat 72549 per tabulam, formula 72572.

303. Tabula determinantium negatiuorum secundum diuersitatem classificationum ipsis respondentium digesta multas alias obseruationes singulares offert. Pro determinantibus formae $-(8n+3)$ multitudo classium (tum earum quae in omnibus, tum earum quae in singulis generibus pr. primitiuis contentae sunt) semper diuisibilis est per 3, vnico determinante -3 excepto, cuius rei ratio ex art. 256, VI sponte sequitur. Pro iis determinantibus, quorum formae vnicum genus conficiunt, multitudo classium semper impar est; quum enim pro tali determinante vnica tantum classis anceps detur, puta principalis, multitudo classium reliquarum,

e quibus binae semper oppositae erunt, necessario erit par, adeoque multitudo omnium impar; ceterum haec posterior proprietas etiam pro determinantibus positiuis valet. — Porro series determinantium, quibus eadem classificatio data (i. e. multitudo data tum generum tum classium) respondet, semper abrumpi videtur, quam obseruationem satis miram per aliquot exempla illustramus. (Numerus primus, romanus, indicat multitudinem generum pr. prim. pos.; sequens multitudinem classium in singulis generibus contentarum; tunc sequitur series determinantium, quibus illa classificatio respondet, et quorum signum negatiuum breuitatis caussa omittitur).

I. 1 ... 1, 2, 3, 4, 7
I. 3 ... 11, 19, 23, 27, 31, 43, 67, 163
I. 5 ... 47, 79, 103, 127
I. 7 ... 71, 151, 223, 343, 463, 487
II. 1 ... 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
II. 2 ... 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193
IV. 1 ... 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
VIII. 1. 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
XVI. 1. 840, 1320, 1365, 1848

Similiter 20 determinantes reperiuntur (maximus = — 1423), quibus classificatio I. 9 respondet; 4 (maximus = — 1303), quibus respondet classificatio I. 11 etc.; classificationes II. 3; II. 4;

II. 5; IV. 2 respondent determinantibus non pluribus quam 48, 32, 42, 68 resp., e quibus maximi — 652, — 862, — 1318, — 1012. Quum tabula, ex qua haec exempla sumsimus, longe vltra maximos determinantes hic occurrentes producta sit *), nec vlli amplius prodierint ad illas classificationes pertinentes: nullum dubium esse videtur, quin series adscriptae reuera abruptae sint, et per analogiam conclusionem eandem ad quasuis alias classificationes extendere licebit. E. g. quum in tota milliade decima determinantium nullus se obtulerit, cui multitudo classium infra 24 responderet: maxime est verisimile, classificationes I. 23; I. 21 etc.; II. 11; II. 10 etc.; IV. 5; IV. 4; IV. 3; VIII. 2 iam ante — 9000 desiisse, aut saltem perpaucis determinantibus vltra — 10000 competere. Demonstrationes autem *rigorosae* harum obseruationum perdifficiles esse videntur. — Non minus admiratione dignum est, quod omnes determinantes, quorum formae in 32 aut plura genera distribuantur, ad minimum binas classes in singulis generibus habeant, adeoque classificationes XXXII. 1, LXIV. 1 etc. omnino excidant (minimo ex huiusmodi dett., — 9240, respondet XXXII. 2); satisque probabile videtur, multitudine generum crescente continuo plures classificationes excidere. Hoc respectu 65 determinantes supra traditi, quibus classificationes I. 1; II. 1; IV. 1; VIII. 1; XVI. 1 respondent, val-

*) Dum haec imprimuntur, vsque ad — 3000 *vno tractu*, nec non per totam milliadem decimam, pluresque alias centades dispersas, quibus accedunt permulti determinantes singulares sedulo electi.

de sunt memorabiles, perspiciturque facile, illos omnes ac solos his duabus proprietatibus insignibus gaudere, vt omnes classes formarum ad ipsos pertinentes ancipites sint, et formae quaecunque in eodem genere contentae necessario tum proprie tum improprie aequiualeant. Ceterum iidem 65 numeri (sub aspectu paullulum diuerso cuius mentio infra fiet et cum criterio demonstratu facili) iam ab ill. Eulero traditi sunt *Nouv. Mem. de l'Ac. de Berlin* 1776 *p.* 338.

304. Multitudo classium pr. primitiuarum, quas formae binariae det. positiui *quadrati kk* constituunt, omnino a priori assignari potest, multitudinique numerorum ad $2k$ primorum ipsoque minorum aequalis est; vnde per ratiocinia non difficilia sed hic supprimenda deducitur, multitudinem mediocrem classium ad tales determinantes circa *kk* pertinentium proxime exprimi per $\frac{8k}{\pi\pi}$. — Determinantes positiui nonquadrati autem hoc respectu phaenomena prorsus singularia offerunt. Scilicet quum classium multitudo parua, e. g. classificatio I. 1 aut I. 3 aut II. 1 etc. pro determinantibus negatiuis et quadratis paruis tantum et mox omnino cessantibus locum habeat: contra e determinantibus positiuis nonquadratis, saltem non permagnis, pars longe maxima tales classificationes praebent, vbi vnica classis in quouis genere continetur, ita vt hae I. 3; I. 5; II. 2; II. 3; IV. 2 etc. sint rarissimae. Ita e. g. inter 90 dett. non qu. infra 100 reperiuntur 31, 48, 27, quibus respondent classificationes I. 1, II. 1, IV. 1 resp; vnicus tantum (37) habet

I. 3; duo (34 et 82) habent II, 2; vnus (79) II. 3. Attamen, determinantibus crescentibus, classium multitudines maiores sensim frequentiores fiunt; ita inter 96 dett. non qu. a 101 vsque ad 200 duo (101, 197) habent I. 3; quatuor (145, 146, 178, 194) II. 2; tres (141, 148, 189) II. 3. Ex 197 dett. a 801 vsque ad 1000 tres habent I. 3; quatuor II. 2; quatuordecim II. 3; duo II. 5; duo II. 6; quindecim IV. 2; sex IV. 3; duo IV. 4; quatuor VIII. 2; reliqui 145 vnam classem in quouis genere. — Quaestio curiosa foret, nec geometrarum sagacitate indigna, secundum quam legem determinantes vnam classem in quouis genere habentes continuo rariores fiant inuestigare; hactenus nec per theoriam decidere possumus, nec per obseruationem satis certo coniectare, vtrum tandem omnino abrumpantur (quod tamen parum probabile videtur), aut saltem *infinite rari* euadant, an ipsorum frequentia ad limitem fixum continuo magis accedat. Multitudo classium mediocris in ratione parum maiori increscit, quam multitudo generum, longeque lentius quam radices quadratae e determinantibus; inter 800 et 1000 illa inuenitur = 5,01. Liceat his obseruationibus aliam adiicere, quae analogiam inter determinantes positiuos et negatiuos quodammodo restituit. Scilicet inuenimus, pro determinante positiuo D non tam multitudinem classium ipsam, quam potius hanc multitudinem per logarithmum quantitatis $t + u\sqrt{D}$ multiplicatam (designantibus t, u numeros minimos, praeter 1, 0, aequationi $tt - Duu = 1$ satisfacientes) multitudini classium pro determinante negatiuo pluri-

bus rationibus hic fusius non explicandis analogam esse, atque valorem mediocrem illius producti aeque exacte exprimi per formulam talem $m\sqrt{D} - n$; sed valores quantitatum constantium m, n hactenus per theoriam determinare non licuit; si quid ex aliquot centadibus determinantium inter se comparatis concludere permissum est, m parum a $2\frac{1}{3}$ differe videtur. — Ceterum de principiis disquisitionum praecedentium circa valores mediocres quantitatum lege analytica non progredientium, sed ad talem legem asymptotice continuo magis approximantium alia occasione fusius agere nobis reseruamus. Transimus iam ad aliam disquisitionem, qua classes diuersae pr. prim. eiusdem det. inter se comparabuntur, finisque huic longae sectioni imponetur.

305. Theorema. *Designante K classem principalem formarum determinantis dati D, C classem quamcunque aliam e genere principali formarum eiusdem det.; $2C$, $3C$, $4C$ etc. classes resp. e duplicatione, triplicatione, quadruplicatione etc. classis C ortas (vt in art. 249): in progressione C, $2C$, $3C$ etc. satis continuata tandem ad classem cum K identicam peruenitur; supponendoque, mC esse primam cum K identicam, atque multitudinem omnium classium in genere principali $= n$, erit vel $m = n$, vel m pars aliquota ipsius n.*

Dem. I. Quum omnes classes K, C, $2C$, $3C$ etc. necessario ad genus principale pertineant (art. 247), classes $n + 1$ priores huius seriei K, C, $2C \ldots nC$ manifesto omnes diuersae esse nequeunt. Erit itaque vel K cum aliqua classium C, $2C$, $3C \ldots nC$ identica, vel saltem duae ex his classibus inter se identicae. Sit $rC = sC$

atque $r > s$, eritque etiam $(r - 1)\,C = (s - 1)\,C$, $(r - 2)\,C = (s - 2)\,C$ etc. et $(r + 1 - s)\,C = C$, vnde $(r - s)\,C = K$. *Q. E. P.*

II. Hinc etiam protinus sequitur, esse vel $m = n$ vel $m < n$, superestque tantummodo, vt ostendamus, in casu posteriori m esse partem aliquotam ipsius n. Quum classes K, C, $2C \ldots (m - 1)\,C$, quarum complexum per $\mathfrak{C}$ designabimus, totum genus principale in hoc casu nondum exhauriant, sit C' aliqua classis huius generis in $\mathfrak{C}$ non contenta, designeturque complexus classium, quae ex compositione ipsius C' cum singulis classibus in $\mathfrak{C}$ oriuntur, puta C', $C' + C$, $C' + 2C \ldots C' + (m - 1)\,C'$, per $\mathfrak{C}'$. Iam facile perspicitur, omnes classes in $\mathfrak{C}'$ tum inter se tum ab omnibus in $\mathfrak{C}$ diuersas esse et ad genus principale pertinere; quodsi itaque $\mathfrak{C}$ et $\mathfrak{C}'$ hoc genus omnino exhauriunt, habebimus $n = 2m$; sin minus, erit $2m < n$. Sit in casu posteriori C'' aliqua classis generis principalis nec in $\mathfrak{C}$ nec in $\mathfrak{C}'$ contenta, designeturque complexus classium ex compositione ipsius C'' cum singulis classibus in $\mathfrak{C}$ prodeuntium i. e. harum C'', $C'' + C$, $C'' + 2C \ldots C'' + (m - 1)\,C$ per $\mathfrak{C}''$, patetque facile, has omnes inter se et ab omnibus in $\mathfrak{C}$ et $\mathfrak{C}'$ diversas esse, et ad genus principale pertinere. Quare si $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$ hoc genus exhauriunt, erit $n = 3m$; sin minus, $n > 3m$, in quo casu classis alia C''', in genere principali contenta, neque vero in $\mathfrak{C}$, $\mathfrak{C}'$ vel $\mathfrak{C}''$, simili modo tractata docebit esse vel $n = 4m$ vel $n > 4m$, et sic porro. Iam quum n et m sint numeri finiti, genus principa-

le necessario tandem exhaurietur, eritque n multiplum ipsius m, siue m pars aliquota ipsius n. *Q. E. S.*

Ex. Sit $D = -356$, $C = (5, 2, 72)$ *), inuenieturque $2C = (20, 8, 21)$, $3C = (4, 0, 89)$ $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Hic itaque est $m = 6$, n vero pro hoc determinante est 12. Accipiendo pro C' classem $(8, 2, 45)$, classes quinque reliquae in $\mathfrak{C}'$ erunt $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

306. Demonstratio theor. praec. omnino analoga inuenietur demonstrationibus in artt. 45, 49, reueraque theoria multiplicationis classium cum argumento in Sect. III. tractato permagnam vndique affinitatem habet. At limites huius operis non permittunt, illam theoriam ea qua digna est vbertate hic persequi; quocirca paucas tantummodo obseruationes hic adiiciemus, eas quoque demonstrationes quae apparatum prolixiorem requirerent supprimemus, disquisitionemque ampliorem ad aliam occasionem nobis reseruabimus.

I. Si series K, C, $2C$, $3C$ etc. vltra $(m-1)C$ producitur, eaedem classes iterum comparent, $mC = K$, $(m+1)C = C$, $(m+2)C = 2C$ etc.; generaliterque (spectando concinnitatis caussa K tamquam $0C$) classes gC, $g'C$ identicae erunt vel diuersae, prout g et g' secundum modulum m congrui sunt vel incongrui. Classis itaque nC semper identica est cum principali K.

*) Classes hic semper per *formas* (simplissimas) in ipsis contentas exprimuntur.

II. Complexum classium K, C, $2C \ldots (m - 1)C$, quem supra per $\mathfrak{C}$ designauimus, vocabimus *periodum* classis C, quae expressio non est confundenda cum *periodis formarum* reductarum det. positiui non-quadrati in art. 186 sqq. tractatis. Patet itaque, e compositione classium quotcunque in eadem periodo contentarum oriri classem in ea periodo quoque contentam $gC + g'C + g''C$ etc. $= (g + g' + g'' + \text{etc.})\, C$.

III. Quum $C + (m - 1)\, C = K$, classes C et $(m - 1)\, C$ oppositae erunt, et perinde $2C$ et $(m - 2)\, C$, $3C$ et $(m - 3)\, C$ etc. Si itaque m est par, classis $\frac{1}{2}mC$ sibi ipsa opposita erit adeoque *anceps*; vice versa, si in $\mathfrak{C}$ praeter K adhuc alia classis anceps occurrit puta gC, erit $gC = (m - g)\, C$ adeoque $g = (m - g) = \frac{1}{2}m$. Hinc sequitur, si m sit par, praeter duas K et $\frac{1}{2}mC$; si vero m sit impar, praeter vnam K, aliam classem ancipitem in $\mathfrak{C}$ contentam esse non posse.

IV. Si periodus alicuius classis hC in $\mathfrak{C}$ contentae supponitur esse K, hC, $2hC$, $3hC \ldots (m' - 1)\, hC$, manifestum est, $m'h$ esse multiplum minimum ipsius h per m diuisibile. Si itaque m et h inter se primi sunt, erit $m' = m$, duaeque periodi easdem classes sed ordine diuerso dispositas continebunt; generaliter autem designante μ diuisorem comm. max. ipsorum m, h, erit $m' = \frac{m}{\mu}$. — Hinc patet, multitudinem classium in periodo cuiusuis classis ex $\mathfrak{C}$ contentarum esse vel m vel partem aliquotam ipsius m;

et quidem tot classes in $\mathfrak{C}$ habebunt periodos m terminorum, quot numeri ex his 0, 1, 2... $m-1$ ad m primi sunt, siue ϕm, vtendo signo art. 39; generaliter vero tot classes in $\mathfrak{C}$ habebunt periodos $\frac{m}{\mu}$ terminorum, quot numeri ex his 0, 1, 2 .... $m-1$ diuisorem maximum μ cum m communem habent, quorum multitudinem esse $\phi\frac{m}{\mu}$ facile perspicitur. Si itaque $m=n$, siue *totum* genus principale sub $\mathfrak{C}$ contentum, dabuntur in hoc genere omnino ϕn classes, quarum periodi idem genus totum includunt, et ϕe classes, quarum periodi ex e terminis constant, denotante e diuisorem quemcunque ipsius n. Haec conclusio generaliter valet, quando in genere principali vlla classis datur, cuius periodus ex n terminis constat.

V. Sub eadem suppositione, systema classium generis principalis aptius disponi nequit, quam aliquam classem, periodum n terminorum habentem, quasi pro *basi* adoptando, generisque principalis classes eodem ordine collocando, quo in illius periodo progrediuntur. Quodsi tunc classi principali *index* 0 adscribitur, classi quae pro basi accepta est index 1 et sic porro: per solam indicum additionem inueniri poterit, quaenam classis e compositione classium quarumcunque generis principalis oriatur. Ecce exemplum pro determinante — 356, vbi classem (9, 2, 40) pro basi accepimus:

0 (1, 0, 356)	4 (20, 8, 21)	8 (20, — 8, 21)
1 (9, 2, 40)	5 (17, 1, 21)	9 (8, 2, 45)
2 (5, 2, 72)	6 (4, 0, 89)	10 (5, — 2, 72)
3 (8, —2, 45)	7 (17, —1, 21)	11 (9, — 2, 40)

VI. Quamquam vero tum analogia cum Sect. III, tum inductio circa plures quam 200 determinantes negatiuos, longeque adhuc plures positiuos non quadratos instituta maximam probabilitatem afferre videantur, illam suppositionem pro *omnibus* determinantibus locum habere: talis conclusio nihilominus falsa foret, et per tabulae classificationum continuationem refelleretur. Liceat, breuitatis caussa, eos determinantes, pro quibus totum genus principale vnicae periodo includi potest, *regulares* vocare, reliquos vero pro quibus hoc fieri nequit *irregulares*. Hoc argumentum, quod ad arithmeticae sublimioris mysteria maxime recondita pertinere, disquisitionibusque difficillimis locum relinquere videtur, paucis tantum obseruationibus hic illustrare possumus, quibus sequentem generalem praemittimus.

VII. Si in genere principali classes C, C' occurrunt, quarum periodi ex m, m' classibus constant, atque M est numerus minimus per m et m' diuisibilis: in eodem genere etiam classes dabuntur, quarum periodi M terminos contineant. Resoluatur M in duos factores r, r' inter se primos, quorum alter (r) metiatur ipsum m, alter (r') ipsum m' (v. art. 73), habebitque classis $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ proprietatem praescri-

ptam. Supponamus enim, periodum classis C'' constare ex g terminis, eritque $K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C'$, vnde $\frac{grm'}{r'}$ per m' diuisibilis esse debebit siue gr per r', adeoque etiam g per r'. Prorsus simili modo g per r diuisibilis inuenitur, vnde etiam per $rr' = M$ diuisibilis erit. Sed quum manifesto sit $MC'' = K$, erit etiam M per g diuisibilis; quare necessario $M = g$. Hinc nullo negotio sequitur, multitudinem *maximam* classium, in vlla periodo contentarum (pro det. dato), diuisibilem esse per multitudinem classium in quauis alia periodo (classis ex eodem genere principali). Simul ibinde methodus deriuari potest, talem classem cuius periodus sit quam maxima (adeoque pro det. regulari totum genus principale complectatur) eruendi, methodo artt. 73, 74 prorsus analoga, etsi in praxi laborem per plura artificia contrahere liceat. Quotiens e diuisione numeri n per multitudinem classium in periodo maxima, qui pro determinantibus regularibus est 1, pro irregularibus semper fit integer maior quam 1, et pro his imprimis commodus est ad diuersas irregularitatis species exprimendas; quamobrem *exponens irregularitatis* dici poterit.

VIII. Hactenus regula generalis non habetur, per quam determinantes regulares ab irregularibus a priori distingui possent, praesertim quum inter posteriores numeri tum primi tum compositi reperiantur; sufficiat itaque quasdam

obseruationes particulares hic adiunxisse. Quando in genere principali plures quam duae classes ancipites continentur, determinans certo est irregularis atque exponens irregularitatis par; quando vero vna tantum aut duae in illo genere adsunt, det. aut regularis erit aut saltem exp. irr. impar. Omnes determinantes negatiui formae $-(216k + 27)$, vnico -27 excepto, irregulares sunt, et exp. irr. per 3 diuisibilis; idem valet de dett. negg. formae $-(1000k + 75)$ et $-(1000k + 675)$, vnico -75 excepto, infinitisque aliis. Si exp. irr. est numerus primus p, aut saltem per p diuisibilis, n per pp diuisibilis erit, vnde sequitur, si n nullum diuisorem quadratum implicet, determinantem certo esse regularem. Pro solis determinantibus *quadratis* positiuis *ee* a priori semper dignosci potest, vtrum regulares sint an irregulares; scilicet illud euenit, quando e est 1 aut 2 aut numerus primus impar aut potestas numeri primi imparis; hoc in omnibus reliquis casibus. Pro dett. negg., irregulares continuo frequentiores euadunt, quo maiores fiunt determinantes; e. g. in tota milliade prima tredecim irregulares reperiuntur, (signo negatiuo omisso) 576, 580, 820, 884, 900, quorum exp. irr. est 2, atque 243, 307, 339, 459, 675, 755, 891, 974, quorum exp. irr. 3; in milliade secunda reperti sunt 13 quorum exp. irr. 2, atque 15 quorum exp. irr. 3; in milliade decima 31 cum exp. irr. 2 atque 32 cum exp. irr. 3. Num determinantes cum exp. irr. maiori quam 3 infra $= 10000$ occurrant, decidere nondum licet; vltra hunc limitem exponentes quicunque dati prouenire possunt. Frequentiam determinantium

negatiuorum irregularium ad frequentiam regularium continuo magis, dett. crescentibus, ad rationem constantem appropinquare valde probabile est, cuius determinatio geometrarum sagacitate magnopere digna foret. — Pro determinantibus positiuis non-quadratis irregulares multo rariores sunt; tales, quorum exp. irr. par sit, infinite multi certo dantur (e. g. 3026 pro quo est 2); nullum quoque dubium videtur, quin tales exstent, quorum exp. irr. sit impar, etsi fateri oporteat, nullum se hactenus nobis obtulisse.

IX. De adornatione maxime commoda systematis classium, in genere principali pro determinante irregulari contentarum, hic agere propter breuitatem non licet; obseruamus tantummodo, quum vnica basis hic non sufficiat, duas vel adeo plures adhuc classes hic esse accipiendas, e quarum multiplicatione et compositione omnes producantur. Hinc *indices duplices aut multiplices* emergent, qui eundem fere vsum praestabunt ac simplices pro regularibus. Sed hanc rem alio tempore fusius tractabimus.

X. Denique obseruamus, quum omnes proprietates in hoc art. et praec. consideratae imprimis a numero n pendeant, qui simile quid est ac $p - 1$ in Sect. III; hunc numerum summa attentione dignum esse; quamobrem quam maxime optandum esset, vt inter ipsum atque determinantem, ad quem pertinet, nexus generalis petegatur. De qua re grauissima eo minus desperandum censemus, quoniam iam successit, va-

lorem mediocrem producti ex n in multitudinem generum (quae a priori assignari potest) saltem pro determinantibus negatiuis formulae analyticae subiicere (art. 302).

307. Disquisitiones artt. praecc. solas classes generis principales complectuntur, adeoque sufficiunt tum pro dett. poss. vbi vnicum omnino genus datur, tum pro negatiuis vbi vnicum genus positiuum adest, si ad genus negatiuum respicere nolumus. Superest, vt de reliquis quoque generibus (pr. primitiuis) quaedam adiiciamus.

I. Quando in genere G' a principali G (eiusdem det.) diuerso vlla classis anceps datur, totidem in ipso aderunt ac in G. Sint in G classes ancipites L, M, N etc. (inter quas etiam erit classis principalis K), in G' vero hae L', M', N' etc., designeturque illarum complexus per A, complexus harum per A'. Quum manifesto omnes classes $L + L'$, $M + L'$, $N + L'$ etc. ancipites diuersaeque sint, et ad G' pertineant, adeoque sub A' contentae esse debeant: multitudo classium in A' certo nequit esse minor quam in A; similiter quum classes $L' + L'$, $M' + L'$, $N' + L'$ etc. diuersae ancipitesque sint et ad G pertineant, adeoque sub A contineantur, multitudo classium in A nequit esse minor quam in A'; quare multitudines classium in A et A' necessario aequales erunt.

II. Quum multitudo omnium classium ancipitum multitudini generum aequalis sit (artt.

261, 287 III): manifestum est, si in G vna tantum classis anceps detur, in *quouis* genere vnam classem ancipitem contentam esse debere; si in G duae ancipites exstent, in semissi omnium generum binas dari, in reliquis nullas; denique si in G plures ancipites contineantur puta a *), partem a^{tam} omnium generum a classes ancipites continere, reliqua nullas.

III. Sint, pro eo casu vbi G duas classes ancipites continet, G, G', G'' etc. ea genera, quae binas, atque H, H', H'' etc. ea quae nullas continent, designeturque complexus illorum per $\mathfrak{G}$, complexus horum per $\mathfrak{H}$. Quum e compositione duarum classium ancipitum semper proueniat classis anceps (art. 249), nullo negotio perspicietur, e compositione duorum generum ex $\mathfrak{G}$ semper prodire genus ex $\mathfrak{G}$. Hinc porro sequitur, e compositione generis ex $\mathfrak{G}$ cum genere ex $\mathfrak{H}$ prodire genus ex $\mathfrak{H}$; si enim e. g. $G' + H$ non ad $\mathfrak{H}$ sed ad $\mathfrak{G}$ pertineret, etiam $G' + H + G'$ ad $\mathfrak{G}$ referendum esset, *Q. E. A.*, quoniam $G' + G' = G$ adeoque $G' + H + G' = H$. Denique facillime intelligitur genera $G + H$, $G' + H$, $G'' + H$ etc., vna cum his $H + H$, $H' + H$, $H'' + H$ etc. omnia diuersa fore adeoque cum $\mathfrak{G}$ et $\mathfrak{H}$ simul sumtis identica; sed, per ea quae modo demonstrata sunt, genera $G + H$, $G' + H$, $G'' + H$ etc. omnia pertinent ad $\mathfrak{H}$ adeoque hunc complexum exhauriunt; quare necessario reliqua $H + H$, $H' + H$, $H'' + H$ etc. omnia ad $\mathfrak{G}$ pertinebunt,

*) Hoc pro solis determinantibus irregularibus euenire potest, eritque a semper potestas binarii.

i. e. e compositione duorum generum ex $\mathfrak{H}$ semper oritur genus ex $\mathfrak{G}$.

IV. Si E est classis generis V, a principali G diuersi, patet, $2E$, $4E$, $6E$ etc. omnes pertinere ad G; has vero $3E$, $5E$, $7E$ etc. ad V. Si itaque periodus classis $2E$ ex m terminis constat: manifesto in serie E, $2E$, $3E$ etc. classis $2mE$, nec vlla prior, cum K identica erit, siue periodus classis E ex $2m$ terminis constabit. Hinc multitudo terminorum in periodo classis cuiuscunque, ex alio genere quam principali, erit vel $2n$ vel pars aliquota ipsius $2n$, designante n multitudinem classium in singulis generibus.

V. Sit C classis data generis principalis G; E classis generis V e cuius duplicatione C oriatur (qualis semper dabitur, art. 286), atque omnes classes ancipites (pr. prim. eiusdem det.) K, K', K'' etc., eruntque *omnes* classes, e quarum duplicatione C oritur, hae: E $(= E + K)$, $E + K'$, $E + K''$ etc., quarum complexus exprimatur per Ω; multitudo harum classium aequalis erit multitudini classium ancipitum siue multitudini generum. Manifestum est, e classibus in Ω tot ad genus V pertinere, quot ancipites dentur in G; designando itaque harum multitudinem per a, patet, in quouis genere vel a classes ex Ω dari vel nullas. Hinc facile colligitur, quando sit $a = 1$, in quouis genere contineri vnam classem ex Ω, quando $a = 2$, semissem omnium generum binas classes ex Ω continere, reliqua nullas, et quidem semissem priorem vel totam cum $\mathfrak{G}$ coincidere (in eadem significatione vt supra III), posteri-

orem cum $\mathfrak{H}$, vel hanc cum $\mathfrak{G}$, illam cum $\mathfrak{H}$. — Quando a adhuc maior est, semper pars a^{ta} omnium generum classes Ω includent (singula a classes).

VI. Supponamus iam, C esse talem classem, cuius periodus ex n terminis constet, perspicieturque facile, in eo casu vbi $a = 2$ adeoque n par, nullam ex Ω ad G pertinere posse (tunc enim talis classis in periodo classis C contenta foret; si itaque esset $= rC$, siue $2rC = C$, foret $2r \equiv 1 \pmod{n}$ *Q. E. A.*); quamobrem quum G ad $\mathfrak{G}$ pertineat, necessario omnes classes Ω inter genera $\mathfrak{H}$ distributa erunt. Hinc colligitur, quoniam (pro det. reg.) in G omnino dantur ϕn classes periodos n terminorum habentes, pro eo casu vbi $a = 2$ inueniri in quouis genere $\mathfrak{H}$ omnino $2\phi n$ classes, quarum periodi $2n$ terminos, adeoque tum genus suum tum principale, complectantur; quando vero $a = 1$, in quouis genere a principali diuerso ϕn huiusmodi classes dabuntur.

VII. His obseruationibus methodum sequentem superstruimus, systema *omnium* classium pr. prim. pro quolibet determinante regulari dato (irregulares enim omnino seponimus) quam aptissime construendi. Eligatur ad lubitum classis E, cuius periodus $2n$ terminos, adeoque tum genus suum quod sit V tum principale G complectatur; classes horum duorum generum ita disponantur, vt in illa periodo progrediuntur. Hoc modo res iam absoluta erit, quando plura genera quam haec duo omnino non adsunt, siue reliqua adiicere non necesse videtur (e. g. pro tali det. neg., vbi duo

tantum genera positiua dantur). Quando vero quatuor aut plura genera construenda sunt, reliqua hoc modo tractentur. Sit V' aliquod e reliquis atque $V + V' = V''$, dabunturque in V' et V'' duae classes ancipites (puta vel in vtroque vna, vel in altero duae in altero nulla); ex his eligatur vna A ad lubitum, patetque facile, si A cum singulis classibus in G et V componatur, prodire $2n$ classes diuersas ad V' et V'' pertinentes, adeoque haec genera omnino exhaurientes; ita haec quoque genera ordinari poterunt. — Si praeter haec quatuor genera alia adhuc supersunt, sit V''' vnum e reliquis, atque V^{IV}, V^{V}, V^{VI} genera ea quae prodeunt e compositione generis V''' cum V, V' et V''. Haec quatuor genera $V''' = V^{VI}$ quatuor classes ancipites continebunt, patetque, si ex his vna A''' eligatur atque cum singulis classibus in G, V, V', V'' componatur, omnes classes in $V''' = V^{VI}$ prodire. — Si adhuc plura genera supersunt, simili modo continuetur, donec omnia exhaustae sint. Patet, si multitudo omnium generum construendorum sit 2^{μ}, omnino opus fore $\mu - 1$ classibus ancipitibus, et quamuis classem horum generum produci posse vel e multiplicatione classis E, vel e compositione classis, e tali compositione ortae, cum vna pluribusue ancipitibus. Ecce duo exempla, per quae haec praecepta illustrabuntur; plura de vsu talis constructionis, vel de artificiis per quae labor subleuari potest, hic adiicere non licet.

I. Determinans — 161.

Quatuor genera positiua; in singulis quaternae classes.

G	V
1, 4; $R7$; $R23$	3, 4; $N7$; $R23$
$(1, 0, 161) = K$	$(3, 1, 54) = E$
$(9, 1, 18) = 2E$	$(6, -1, 27) = 3E$
$(2, 1, 54) = 4E$	$(6, 1, 27) = 5E$
$(9, -1, 18) = 6E$	$(3, -1, 54) = 7E$

V'	V''
3, 4; $R7$; $N23$	1, 4; $N7$; $N23$
$(7, 0, 23) = A$	$(10, 3, 17) = A+E$
$(11, -2, 15) = A+2E$	$(5, 2, 33) = A+3E$
$(14, 7, 15) = A+4E$	$(5, -2, 33) = A+5E$
$(11, 2, 15) = A+6E$	$(10, -3, 17) = A+7E$

II. Determinans — 546.

Octo genera positiua; in singulis ternae classes.

G	V
1 *et* 3, 8; $R3$; $R7$; $R13$	5 *et* 7, 8; $N3$; $N7$; $N13$
$(1, 0, 546) = K$	$(5, 2, 110) = E$
$(22, -2, 25) = 2E$	$(21, 0, 26) = 3E$
$(22, 2, 25) = 4E$	$(5, -2, 110) = 5E$

V'	V''
1 *et* 3, 8; $N3$; $R7$; $N13$	5 *et* 7, 8; $R3$; $N7$; $R13$
$(2, 0, 273) = A$	$(10, 2, 55) = A+E$
$(11, -2, 50) = A+2E$	$(13, 0, 42) = A+3E$
$(11, 2, 50) = A+4E$	$(10, -2, 55) = A+5E$

V^{III}

1 et 3 8; N3; N7; R13

$(3,\ 0,\ 182) = A'$

$(17,\ 7,\ 35) = A' + 2E$

$(17, -7, 35) = A' + 4E$

V^{IV}

5 et 7 8; R3; R7; N13

$(15, -3, 37) = A' + E$

$(7,\ 0,\ 78) = A' + 3E$

$(15,\ 3,\ 37) = A' + 5E$

V^{V}

1 et 3 8; R3; N7; N13

$(6,\ 0,\ 91) = A + A'$

$(19, 9, 33) = A + A' + 2E$

$(19, -9, 53) = A + A' + 4E$

V^{VI}

5 et 7 8; N3; R7; R13

$(23, 11, 29) = A + A' + E$

$(14, 0, 26) = A + A' + 3E$

$(23, -11, 29) = A + A' + 5E$

Sectio Sexta

VARIAE DISQVISITIONVM PRAECEDENTIVM APPLICATIONES.

308. Quam fertilis sit arithmetica sublimior veritatibus, quae in aliis quoque matheseos partibus vsum praestent, pluribus iam passim locis addigitauimus; quasdam vero applicationes, quae expositionem ampliorem merentur, seorsim tractare non inutile duximus, non tam vt hoc argumentum, quo plura volumina facile impleri possent, exhauriatur, quam potius vt per aliqua specimina illustretur. In hacce quidem sectione primo de resolutione fractionum in simpliciores agemus; dein de conuersione fractionum communium in decimales; tum methodum nouam exclusionis explicabimus, solutioni aequationum indeterminatarum secundi gradus inseruientem; tandem methodos nouas expeditas trademus, numeros primos a compositis dignoscendi, horumque factores explorandi. In sectione sequente autem theoriam generalem generis peculiaris functionum, per totam analysin latissime patentis, quatenus cum arithmetica sublimiori arctissime connexa est, stabiliemus, imprimisque theoriam sectionis circuli, cuius prima tantum elementa

hactemus innotuerunt, nouis incrementis amplificare studebimus.

309. Problema: *Fractionem* $\frac{m}{n}$, *cuius denominator* n *est productum e duobus numeris inter se primis* a, b, *in duas alias discerpere, quarum denominatores sint* a, b.

Sol. Sint fractiones quaesitae $\frac{x}{a}$, $\frac{y}{b}$, fierique debebit $bx + ay = m$; hinc x erit radix congruentiae $bx \equiv m \pmod{a}$, quae per sect. II erui poterit, y vero fiet $= \frac{m - bx}{a}$.

Ceterum constat, congruentiam $bx \equiv m$ radices infinite multas, sed secundum a congruas, habere, vnica vero tantum positiua minorque quam a dabitur; fieri autem potest etiam, vt y euadat negatiuus. Vix necesse erit monere, y etiam per congruentiam $ay \equiv m \pmod{b}$, atque x per aequationem $x = \frac{m - ay}{b}$ inueniri posse. — E. g. proposita fractione $\frac{58}{77}$, erit 4 valor expr. $\frac{58}{11} \pmod{7}$, vnde $\frac{58}{77}$ resoluitur in $\frac{4}{7} + \frac{2}{11}$.

310. Si fractio $\frac{m}{n}$ proponitur, cuius denominator n est productum e factoribus quotcunque inter se primis a, b, c, d etc.: per art. praec. primo in duas resolui potest, quarum denominatores sint a et bcd etc.; secunda iterum in duas denominatorum b et cd etc.; posterior rursus in duas et sic porro, vnde tandem fractio proposita

sub hanc formam redigetur $\frac{m}{n} = \frac{\alpha}{a} + \frac{\mathfrak{b}}{b} + \frac{\gamma}{c} + \frac{\delta}{d}$ etc. Numeratores α, $\mathfrak{b}$, γ, δ etc. manifesto positiuos ac denominatoribus suis minores accipere licebit, praeter vltimum, qui reliquis determinatis non amplius est arbitrarius, atque etiam negatiuus aut denominatore maior fieri potest (siquidem non supponimus $m < n$). Tum plerumque e re erit, ipsum sub formam $\frac{\varepsilon}{e} \mp k$ redigere, ita vt ε sit positiuus ac minor quam e, k vero integer. Denique patet, a, b, c etc. ita accipi posse, vt sint vel numeri primi vel numerorum primorum potestates.

Ex. Fractio $\frac{391}{924}$, cuius denominator $= 4.3.7.11$ hoc modo resoluitur in $\frac{1}{4} + \frac{100}{231}$; $\frac{100}{231}$ in $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ in $\frac{1}{7} - \frac{7}{11}$; vnde, scribendo $\frac{4}{11} - 1$ pro $-\frac{7}{11}$ fit $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311. Fractio $\frac{m}{n}$ *vnico tantum modo* sub formam $\frac{\alpha}{a} + \frac{\mathfrak{b}}{b} + \text{etc.} \mp k$ reduci potest, ita vt α, $\mathfrak{b}$ etc. sint positiui ac minores quam a, b etc. scilicet supponendo $\frac{m}{n} = \frac{\alpha}{a} + \frac{\mathfrak{b}}{b} + \frac{\gamma}{c} + \text{etc.} \mp k = \frac{\alpha'}{a} + \frac{\mathfrak{b}'}{b} + \frac{\gamma'}{c} + \text{etc.} \mp k'$, atque etiam α', $\mathfrak{b}'$ etc. positiuos ac minores quam a, b etc., necessario erit $\alpha = \alpha'$, $\mathfrak{b} = \mathfrak{b}'$, $\gamma = \gamma'$ etc., $k = k'$. Multiplicando enim per $m = abc$ etc., patet fieri $m \equiv \alpha bcd$ etc. $\equiv \alpha' bcd$ etc. (mod. a), vnde quoniam bcd etc. ad a primus

est, necessario $\alpha \equiv \alpha'$ adeoque $\alpha = \alpha'$, et perinde $\mathfrak{C} = \mathfrak{C}'$ etc., vnde etiam sponte $k = k'$. Iam quum prorsus arbitrarium sit, cuiusnam denominatoris numerator primus supputetur, manifestum est, *omnes* numeratores ita inuestigari posse, vt α in art. praec. puta $\mathfrak{C}$ per congruentiam $\mathfrak{C}acd$ etc. $\equiv m \pmod{b}$, γ per hanc γabd etc. $\equiv m \pmod{c}$ etc.; summa omnium fractionum sic inuentarum vel propositae $\frac{m}{n}$ aequalis erit, vel differentia numerus integer $= k$, qua via simul confirmationem calculi nanciscimur. Ita in ex. art. praec. valores expr. $\frac{391}{211} \pmod{4}$, $\frac{391}{308} \pmod{3}$, $\frac{391}{132} \pmod{7}$, $\frac{391}{84} \pmod{11}$ statim suppeditant numeratores 1, 2, 1, 4 denominatoribus 4, 3, 7, 11 respondentes, summaque harum fractionum propositam vnitate superare inuenitur.

312. Definitio. Si fractio communis in decimalem conuertitur, seriem figurarum decimalium *) (excluso si quis adest numero integro), siue finita sit, siue in infinitum excurrat, fractionis *mantissam* vocamus, expressionem, alias tantummodo apud logarithmos vsitatam, in significatione latiori accipientes. Ita e. g. fractionis $\frac{1}{8}$ mantissa est 125, mantissa fractionis $\frac{35}{16}$ 1875, fractionis $\frac{2}{37}$ mantissa 054054... in inf.

Ex hac definitione statim patet, fractiones eiusdem denominatoris $\frac{l}{n}$, $\frac{m}{n}$ easdem vel diuersas

*) Breuitatis caussa disquisitionem sequentem ad systema vulgare decadicum restringimus, quum facile ad quoduis aliud extendi possit.

mantissas habere, prout numeratores l, m secundum m congrui sint vel incongrui. Mantissa finita non mutatur, si ad dextram cifrae quotcunque apponantur. Mantissa fractionis $\frac{10m}{n}$ obtinetur, rescindendo a mantissa fractionis $\frac{m}{n}$ figuram primam et generaliter mantissa fractionis $\frac{10^\nu m}{n}$ inuenitur rescindendo ν figuras primas mantissae ipsius $\frac{m}{n}$. Mantissa fractionis $\frac{1}{n}$ statim figura significatiua (i. e. a cifra diuersa) incipit, si $n < 10$; si vero $n = 10$ vel < 10, multitudoque figurarum e quibus constat est k, primae $k - 1$ figurae mantissae ipsius $\frac{1}{n}$ erunt cifrae atque demum sequens k^{ta} erit significatiua. Hinc facile deducitur, si $\frac{l}{n}$, $\frac{m}{n}$ mantissas diuersas habeant (i. e. si l, m sec. n incongrui), has certo in primis k figuris conuenire non posse, sed saltem in k^{ta} discrepare debere.

313. Problema. *Dato denominatore fractionis $\frac{m}{n}$ atque primis k figuris ex ipsius mantissa, inuenire numeratorem m, quem ipso n minorem supponimus.*

Sol. Considerentur illae k figurae tamquam numerus integer, qui per n multiplicetur, productumque per 10^k diuidatur (siue k vltimae figurae resecentur). Si quotiens est integer (siue figurae resectae cifrae), ipse manifesto erit numerator quaesitus atque mantissa data completa;

sin minus, numerator quaesitus erit integer proxime maior, siue ille quotiens vnitate auctus, postquam figurae decimales sequentes reiectae sunt. Ratio huius regulae tam facile ex iis quae ad finem art. praec. obseruauimus cognoscitur, vt explicatione vberiori opus non habeat.

Ex. Si constat, duas figuras primas mantissae fractionis, cuius denominator 23, esse 59, habemus productum $23.59 = 1557$, a quo duas vltimas figuras abiiciendo, vnitatemque addendo, numerator quaesitus prodit $= 16$.

314. Inchoamus a consideratione talium fractionum, quarum denominatores sunt numeri primi vel numerorum primorum potestates, posteaque reliquas ad has reducere ostendemus. Et primo statim obseruamus, mantissam fractionis $\frac{a}{p^\mu}$ (cuius numeratorem a per numerum primum p non diuisibilem esse semper supponimus) finitam esse, atque ex μ figuris constare, si $p = 2$ aut $= 5$; in casu priori haec mantissa, tamquam numerus integer considerata, erit $= 5^\mu a$, in posteriori $= 2^\mu a$. Haec tam obuia sunt, vt expositione non egeant.

Si vero p est alius numerus primus, $10^r a$ per p^μ numquam diuisibilis erit, quantumuis magnus accipiatur r, vnde sponte sequitur, mantissam fractionis $F = \frac{a}{p^\mu}$ necessario in infinitum progredi. Supponamus, 10^e esse potestatem

infimam numeri 10, quae vnitati secundum modulum p^μ congrua fit (Conf. sectio III, vbi ostendimus, e vel numero $(p-1)p^{\mu-1}$ aequalem vel ipsius partem aliquotam esse), perspicieturque facile, etiam $10^e a$ fore numerum, in serie $10a$, $100a$, $1000a$ etc. primum, qui ipsi a secundum eundem modulum sit congruus. Iam quum per art. 312 mantissae fractionum $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$ ... $\frac{10^e a}{p^\mu}$ oriantur, demendo mantissae fractionis F figuram primam, duas ... e figuras primas resp., manifestum est, in hac mantissa post primas e figuras, neque prius, easdem iterum repeti. Has primus e figuras, e quibus infinities repetitis mantissa formata est, *periodum* huius mantissae siue fractionis F vocare possumus, patetque magnitudinem periodi, i. e. multitudinem figurarem e quibus constat, quae, est $= e$, a numeratore a omnino independentem esse, et per solum denominatorem determinari. Ita e. g. periodus fractionis $\frac{1}{11}$ est 09, fractionis $\frac{3}{7}$ periodus 428571 *).

315. Simulac igitur fractionis alicuius periodus habetur, mantissa ad figuras quotcunque produci poterit. Porro patet, si fuerit $b \equiv 10^\lambda a \pmod{p^\mu}$, periodum fractionis $\frac{b}{p^\mu}$ oriri, si primae λ figurae periodi fractionis F (supponendo

*) Cel. Robertson periodi initium et finem duobus punctis figurae primae et vltimae suprascriptis indicat (Theory of circulating fractions, Philos. Trans. 1764), quod hic non necessarium putamus.

$\lambda < e$ quod licet) reliquis $e - \lambda$ postscribantur, adeoque cum periodo fractionis F simul periodos omnium fractionum haberi, quarum numeratores ipsis $10a$, $100a$, $1000a$ etc. secundum denominatorem p^μ sint congrui. Ita *e. g.* quum $6 \equiv 3.10^2 \pmod 7$, periodus fractionis $\frac{6}{7}$ statim e periodo fractionis $\frac{3}{7}$ fit 857142.

Qnoties itaque pro modulo p^μ numerus 10 est radix primitiua (artt. 57, 89), e periodo fractionis $\frac{1}{p^\mu}$ protinus deduci poterit periodus cuiusuis alius fractionis $\frac{m}{p^\mu}$ (cuius numerator m per p non diuisibilis), tot figuras ab illa a laeua resecando et ad dextram restituendo, quot vnitates habet index ipsius m, numero 10 pro basi accepto. Hinc perspicuum est, quamobrem in hocce casu numerus 10 in tabula I semper pro basi acceptus sit (v. art. 72).

Quando vero 10 non est radix primitiua, e periodo fractionis $\frac{1}{p^\mu}$ earum tantummodo fractionum periodi exscindi possunt, quarum numeratores alicui potestati ipsius 10 secundum p^μ sunt congrui. Sit 10^e potestas infima ipsius 10 vnitati secundum p^μ congrua, $(p-1)\,p^{\mu-1} = ef$, atque talis radix primitiua r pro basi accepta, vt index numeri 10 fiat f (art. 71). In hoc itaque systemate numeratores fractionum, quarum periodi e periodo fractionis $\frac{1}{p^\mu}$ exscindo possunt, habebunt indices f, $2f$, $3f$ .... $ef - f$; simili modo

e periodo fractionis $\frac{r}{p^\mu}$ deduci possunt periodi fractionum, quarum numeratores $10r$, $100r$, $1000r$ etc. indicibus $f+1$, $2f+1$, $3f+1$ etc. respondentes; e periodo fractionis cum numeratore rr (cuius index 2) deducentur periodi fractionum cum numeratoribus quorum indices $f+2$, $2f+2$, $3f+2$ etc.; generaliterque e periodo fractionis cum numeratore r^i deriuari poterunt periodi fractionum cum numeratoribus, quorum indices $f+i$, $2f+i$, $3f+i$ etc. Hinc facile colligitur, si tantummodo periodi fractionum cum numeratoribus $1, r, rr, r^3 \ldots r^{f-1}$ habeantur, omnes reliquas inde per solam transpositionem deduci posse adiumento regulae sequentis: Sit index numeratoris m fractionis propositae $\frac{m}{p^\mu}$, in systemate vbi r pro basi acceptus est, $= i$ (quem supponimus minorem quam $(p-1)p^{\mu-1}$); fiat (diuidendo per f) $i = \alpha f + \epsilon$ ita vt α, ϵ sint integri positiui (siue etiam 0) atque $\epsilon < f$; quo facto orietur periodus fractionis $\frac{m}{p^\mu}$ e periodo fractionis cuius numerator r^ϵ (adeoque 1, quando $\epsilon = 0$), collocando huius α primas figuras post reliquas (adeoque hanc ipsam periodum retinendo, quando $\alpha = 0$). Haec sufficienter declarabunt, cur in condenda tabula I normam in art. 72 explicatam sequuti simus.

316. Secundam haec principia pro omnibus denominatoribus formae p^μ infra 1000 tabulam periodorum necessariarum construximus, quam integram siue etiam vlterius continuatam

occasione data publici iuris faciemus. Hoc loco tabula III vsque ad 100 tantum producta tamquam specimen sufficiat, quae explicatione vix opus habebit. Pro iis denominatoribus, vbi 10 est radix primitiua, periodos fractionum cum numeratore 1 exhibet (puta pro 7, 17, 19, 23, 29, 47, 59, 61, 97); pro reliquis, f periodos numeratoribus $1, r, rr \ldots r^{f-1}$ respondentes, quae per numeros adscriptos (0), (1), (2) etc. sunt distinctae; pro basi r semper eadem radix primitiua adoptata est vt in tabula I. Hinc igitur periodus fractionis cuiusuis cuius denominator in hac tabula continetur adiumento praeceptorum art. praec. erui poterit, postquam numeratoris index per tabulam I est computatus. Ceterum pro denominatoribus tam paruis negotium aeque facile absque tabula I absoluere poterimus, si per diuisionem vulgarem tot figuras initiales mantissae quaesitae computamus, quot per art. 313. necessariae sunt, vt ab omnibus aliis eiusdem denominatoris distingui possit (pro tabula III non plures quam 2), omnesque periodos denominatori dato respondentes perlustramus, vsquedum ad illas figuras initiales perueniamus, quae periodi initium haud dubie indicabunt; monere tamen oportet, illas figuras etiam separatas esse posse, ita vt prima (vel plures) finem alicuius periodi constituant, reliqua vel reliquae eiusdem initium.

Ex. Quaeritur periodus fractionis $\frac{12}{19}$. Hic pro modulo 19 per tab. I habetur ind. $12 = 2$ ind. $2 +$ ind. $3 = 39 \equiv 3$ (mod. 18, art. 57); quare quum pro hoc casu vnica tantum periodus numeratori 1 respondens habeatur,

huius tres primas figuras ad finem translocare oportet, vnde fit periodus quaesita 6315789473 68421052. — Aeque facile periodi initium e duabus primus figuris 63 inuentum fuisset.

Si periodus fractionis $\frac{45}{53}$ desideratur, fit pro modulo 53, ind. $45 = 2$ ind. $3 +$ ind. $5 = 49$; multitudo periodorum hic est $4 = f$, atque $49 = 12f + 1$, quare a periodo cum (1) signata 12 primae figurae postponendae erunt vltimae, periodusque quaesita fit 849056603773 5. Figurae initiales 84 in hoc casu separatae sunt in tabula.

Obseruabimus adhuc, adiumento tabulae III etiam numerum inueniri posse, qui pro modulo dato (in ipsa sub denominatoris titulo contento) indici dato respondeat, vt in art. 59 polliciti sumus. Patet enim per praecc., inueniri posse periodum fractionis cuius numeratori (licet incognitus sit) index datus respondeat; sufficit autem, tot figuras initiales huius periodi excerpere, quot figuras habet denominator; ex illis per art. 313. eruetur numerator siue numerus quaesitus indici dato respondens.

317. Per praecedentia mantissa fractionis cuiuscunque, cuius denominator est numerus primus aut numeri primi potestas intra limites tabulae, ad figuras quotcunque sine computo erui potest; sed adiumento disquisitionum in initio huius sectionis tabulae ambitus multo latius patet, omnesque fractiones, quarum denominatores sunt producta e numeris primis aut primorum pote-

states intra ipsius limitem, complectitur. Quum enim talis fractio in alias decomponi possit, quarum denominatores sint hi factores, atque has in fractiones decimales ad figuras quotcunque conuertere liceat, restat tantummodo, vt hae in summam vniantur. Ceterum vix opus erit monere, summae sic prodeuntis figuram vltimam iusto minorem euadere posse; manifesto autem defectus ad tot vnitates adscendere nequit, quot fractionis particulares adduntur, vnde hae ad aliquot figuras vlterius computare conueniet, quam fractio proposita iusta desideratur. Exempli caussa considerabimus fractionem $\frac{6099380351}{1271808720} = F$ *), cuius denominator est productum e numeris 16, 9, 5, 49, 13, 47, 59. Per praecepta supra data inuenitur $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$, quae fractiones particulares ita vt sequitur in decimales conuertuntur:

$$
\begin{array}{rcl}
1 & = & 1 \\
\frac{11}{16} & = & 0,625 \\
\frac{4}{5} & = & 0,8 \\
\frac{4}{9} & = & 0,4444444444\ 4444444444\ 44 \\
\frac{22}{49} & = & 0,4489795918\ 3673469387\ 75 \\
\frac{5}{13} & = & 0,3846153846\ 1538461538\ 46 \\
\frac{7}{47} & = & 0,1489361702\ 1276595744\ 68 \\
\frac{52}{59} & = & 0,8813559322\ 0338983050\ 84 \\
\hline
F & = & 4,7958315233\ 1271954166\ 17
\end{array}
$$

*) Haec fractio est vna ex iis, quae ad radicem quadratam ex 23 quam proxime appropinquant, et quidem excessus est minor quam septem vnitates in loco figurae decimalis vigesimae.

Defectus huius summae a iusto certo minor est quinque vnitatibus in figura vltima vigesima secunda, quare viginti primae inde mutari nequeunt. Calculum ad plures figuras producendo, pro duabus figuris vltimis 17 prodit 1893936 ... — Ceterum vel nobis non monentibus quisque videbit, hanc methodum, fractiones communes in decimales conuertendi, ei potissimum casui accommodatam esse, vbi multae figurae decimales desiderentur; quando enim paucae sufficiunt, diuisio vulgaris siue logarithmi aeque expedite plerumque adhiberi poterunt.

318. Quum itaque resolutio talium fractionum, quarum denominatores e pluribus numeris primis diuersis compositi sunt, ad eum casum iam reducta sit, vbi denominator est primus aut primi potestas: de illarum mantissis pauca tantum adiiciemus. Si denominator factorem 2 et 5 non continet, mantissa etiam hic e periodis constabit, quoniam pro hoc quoque casu in serie 10, 100, 1000 ad terminum, vnitati secundum denominatorem congruum, tandem peruenitur, simulque huius termini exponens, qui per art. 92 facile determinari poterit, periodi magnitudinem, a numeratore independentem, indicabit, siquidem hic ad denominatorem primus fuerit. — Si vero denominator est formae $2^{\alpha}5^{\mathfrak{C}}N$, designante N numerum ad 10 primum, α et $\mathfrak{C}$ numeros quorum vnus saltem non est 0, fractionis mantissa post primas α vel $\mathfrak{C}$ figuras (prout α vel $\mathfrak{C}$ maior) e periodis constare incipiet, cum periodis fractionum cum denominatore N respectu longitudinis conuenientibus; hoc

facillime inde deriuatur, quod illa fractio in duas alias cum denominatoribus $2^{\alpha}5^{\beta}$ et N resolubilis est, quarum prior post primas α vel β figuras abrumpetur. — Ceterum de hoc argumento multas alias obseruationes adiicere possemus, praesertim circa artificia, talem tabulam vt III quam citissime construendi, quas breuitatis caussa eo lubentius hoc loco supprimimus, quum plura huc pertinentia tum a cel. Robertson l. c., tum a cel. Bernoulli (*Nouv. Mem. de l'Ac. de Berlin* 1771) iam sint tradita.

319. Congruentiae $xx \equiv A \pmod{m}$, quae conuenit cum aequatione indeterminata $xx = A + my$, *possibilitatem* in sect. IV (art. 146) ita tractauimus, vt nihil amplius desiderari posse videatur; respectu inuestigationis incognitae ipsius autem, iam supra (art. 152) obseruauimus, methodos indirectas directis longe esse praeferendas. Si m est numerus primus (ad quem casum reliqui facile reducuntur), tabulam indicum I (cum III secundum obs. art. 316 combinatam) ad hunc finem adhibere possemus, vt in art. 60 generalius ostendimus: haec vero methodus intra tabulae limites restricta foret. Propter has rationes methodum sequentem generalem ac expeditam arithmeticae amatoribus haud ingratam fore speramus.

Ante omnio obseruamus sufficere, si ii tantummodo valore ipsius x habeantur, qui sint positiui atque non maiores quam $\frac{1}{2}m$, quum quiuis alius horum alicui vel ipsi vel negatiue sumto secundum modulum m congruus sit; pro tali

vero valore ipsius x valor ipsius y necessario inter limites $-\frac{A}{m}$ et $\frac{1}{4}m - \frac{A}{m}$ contentus erit. Methodus itaque, quae statim se offert, in eo consisteret, vt pro singulis valoribus ipsius y intra hos limites contentis, quorum complexum exprimemus per Ω, valor ipsius $A + my$ quem per V denotabimus computetur, iique soli retineantur, pro quibus V fit quadratum. Quando m est numerus paruus (e. g. infra 40), hoc tentamen tam breue est, vt contractione vix opus habeat; quando autem m est magnus, labor per *methodum exclusionis* sequentem, quantum lubet, abbreuiari poterit.

320. Sit E numerus arbitrarius integer ad m primus ac maior quam 2; omnia eius non residua quadratica diuersa (i. e. secundum E incongrua) haec a, b, c etc.; denique radices congruentiarum $A + my \equiv a$, $A + my \equiv b$, $A + my \equiv c$ etc. sec. mod. E hae α, β, γ etc., quas omnes positiuas ac minores quam E accipere licebit. Si itaque ipsi y valor alicui ex his numeris α, β, γ etc. secundum E congruus tribuitur, valor ipsius $V = A + my$ inde oriundus alicui ex his a, b, c etc. congruus et proin non residuum ipsius E erit, neque adeo quadratum esse poterit. Hinc patet, ex Ω omnes statim numeros tamquam inutiles excludi posse, qui sub formis $Et + \alpha$, $Et + \beta$, $Et + \gamma$ etc. contenti sint, sufficietque, tentamen de reliquis, quorum complexus sit Ω', instituisse. In illa operatione numero E nomen *excludentis* tribui potest.

Accipiendo autem pro excludente numerum idoneum alium E', prorsus simili modo inuenientur tot numeri α', $\mathfrak{G}'$, γ' etc., quot non residua diuersa quadratica habet, quibus y secundum modulum E' congruus esse nequit. Quare denuo ex Ω' eiicere licebit omnes numeros sub formis $E't + \alpha'$, $E't + \mathfrak{G}'$, $E't + \gamma'$ etc. contentos. Hoc modo continuari poterit, alios aliosque semper excludentes adhibendo, donec multitudo numerorum ex Ω tantum deminuta fuerit, vt non difficilius videatur, omnes superstites tentamini reuera subiicere, quam exclusiones nouas instituere.

Ex. Proposita aequatione $xx = 22 + 97y$, limites valorum ipsius y erunt $-\frac{22}{97}$ et $24\frac{1}{4} - \frac{22}{97}$, vnde (quoniam inutilitas valoris 0 per se est obuia) Ω comprehendet numeros $1, 2, 3 \ldots 24$. Pro $E = 3$ habetur vnicum non residuum $a = 2$; vnde fit $\alpha = 1$; excludendi sunt itaque ex Ω omnes numeri formae $3t + 1$; multitudo remanentium Ω' erit 16. Simili modo pro $E = 4$ habetur $a = 2$, $b = 3$, vnde $\alpha = 0$, $\mathfrak{G} = 1$; quare reiici debent numeri formae $4t$ et $4t + 1$ restantque hi octo 2, 3, 6, 11, 14, 15, 18, 23. Perinde pro $E = 5$ reiiciendi inueniuntur numeri formarum $5t$ et $5t + 3$; remanentque hi 2, 6, 11, 14. Excludens 6 remoueret numeros formarum $6t + 1$ et $6t + 4$, hi vero (qui cum numeris formae $3t + 1$ conueniunt) iam absunt. Excludens 7 eiicit numeros formarum $7t + 2$, $7t + 3$, $7t + 5$, ac relinquit hos 6, 11, 14. Hi pro y substituti producunt resp. $V = 604$, 1089, 1380, e quibus valor secundus solus est quadratus, vnde $x = \pm 33$.

321. Quum operatio cum excludente E instituta e valoribus ipsius V, valoribus ipsius y in Ω respondentibus, omnes eos releget, qui sunt non residua quadratica ipsius E, residua vero eiusdem numeri non attingat; facile intelligitur, vsum excludentium E et $2E$ nihil differre, si E sit impar, quum in hoc casu E et $2E$ eadem residua et non residua habeant. Hinc patet, si successiue numeri 3, 4, 5 etc. tamquam excludentes adhibeantur, numeros impariter pares 6, 10, 14 etc. tamquam superfluos praetereundos esse. Porro perspicuum est, operationem duplicem, cum excludentibus E, E' institutam, omnes eos valores ipsius V remouere, qui vel vtriusque E, E' vel vnius non residua sint, eosque qui sint, vtriusque residua remanere. Iam quum in eo casu, vbi E et E' diuisorem communem non habent, illi numeri eiecti omnes sint non residua, atque hi superstites residua producti EE', manifestum est, vsum excludentis EE' in hoc casu omnino tantundem efficere, ac vsum duorum E, E', adeoque illum, post hunc, superfluum fieri. Quare eos quoque excludentes omnes praeterire licebit, qui in duos factores inter se primos resolui possunt, sufficietque iis vti, qui sunt vel numeri primi (ipsum m non metientes) vel primorum potestates. Denique manifestum est, post vsum excludentis p^μ, qui sit potestas numeri primi p, excludentem p seu p^ν, quando $\nu < \mu$ superfluum fieri; quum enim p^μ inter valores ipsius V sola sui residua reliquerit, a potiori non-residua ipsius p aut potestatis cuiusuis inferioris p' non amplius aderunt. Si vero p aut p^ν iam ante p^μ adhibitus est, hic manifesto

tales tantum valores ipsius V eiicere potest, qui simul sunt residua ipsius p (aut p') atque non residua ipsius p''; quare huiusmodi tantum non-residua ipsius p'' pro a, b, c etc. accipere sufficiet.

322. Computus numerorum α, $\mathfrak{C}$, γ etc. cuiuis excludenti dato E respondentium multum contrahitur per obseruationes sequentes. Sint $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. radices congruentiarum $my \equiv a$, $my \equiv b$, $my \equiv c$ etc. (mod. E) atque k radix huius $my \equiv -A$, patetque fieri $\alpha \equiv \mathfrak{A} + k$, $\mathfrak{C} \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k$ etc. Iam si ipsos $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. reuera per solutionem illarum congruentiarum eruere oporteret, haec via ipsos α, $\mathfrak{C}$, γ etc. inueniendi nihil vtique breuior foret, quam ea quam supra ostendimus: sed illud neutiquam est necessarium. Si enim, primo, E est numerus primus, atque m residuum qu. ipsius E, patet per art. 98, ipsos $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc., qui sunt valeres expr. $\frac{a}{m}$, $\frac{b}{m}$, $\frac{c}{m}$ etc. (mod. E), fieri non residua diuersa ipsius E, adeoque cum ipsis α, $\mathfrak{C}$, γ etc. omnino conuenire, abstrahendo ab ipsorum ordine, cuius nihil hic refert; si vero in eadem suppositione m est non-residuum ipsius E, numeri $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. cum omnibus residuis quadraticis, abiecto o, conuenient. Si E est quadratum numeri primi (imparis), $= pp$, atque p iam tamquam excludens applicatus, sufficit per art. praec., pro a, b, c etc. ea non residua ipsius pp assumere qui sunt residua ipsius p, i. e. numeros p, $2p$, $3p \ldots pp - p$ (scilicet omnes numeros infra pp praeter o qui per p sunt diuisibi-

les); hinc vero facile perspicitur, pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. omnino eosdem numeros prouenire debere, aliter tantum dispositos. Similiter si post applicationem excludentium p et pp ponitur $E = p^3$, sufficiet pro a, b, c etc. accipere producta singulorum nonresiduorum ipsius p in pp, vnde pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. prouenient vel iidem numeri, vel producta ipsius pp in singula residua ipsius p praeter 0, prout m est residuum vel non residuum ipsius p. Generaliter accipiendo pro E potestatem quamcunque numeri primi puta p^μ, omnibus inferioribus iam applicatis, pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. prodibunt producta ipsius $p^{\mu-1}$ vel in omnes numeros ipso p minores, 0 semper excepto, quando μ par, vel in omnia non residua ipsius p minora quam p, quando μ impar atque mRp, vel in omnia residua, quando mNp. — Si $E = 4$, adeoque $a = 2$, $b = 3$, pro $\mathfrak{A}$, $\mathfrak{B}$ habemus vel 2 et 3 vel 2 et 1, prout $m \equiv 1$ aut $\equiv 3 \pmod 4$. Si post vsum excl. 4 statuitur $E = 8$, habemus $\alpha = 5$, vnde $\mathfrak{A}$ fit 5, 7, 1, 3, prout $m \equiv 1, 3, 5, 7 \pmod 8$. Generaliter autem, si E est potestas altior quaecunque binarii puta 2^μ, inferioribus iam applicatis, poni debet $a = 2^{\mu-1}$, $b = 3.2^{\mu-2}$, quando μ est par, vnde fit $\mathfrak{A} = 2^{\mu-1}$, $\mathfrak{C} = 3.2^{\mu-2}$ vel $= 2^{\mu-2}$, prout $m \equiv 1$ vel $\equiv 3$, quando vero μ est impar, ponendum est $a = 5.2^{\mu-3}$, vnde $\mathfrak{A}$ aequalis fit producto numeri $2^{\mu-3}$ in 5, 7, 1, vel 3, prout $m \equiv 1, 3, 5$ vel 7 (mod. 8).

Ceterum periti facile comminiscentur apparatum, per quem valores inutiles ipsius y *mechanice* ex Ω eiici possint, postquam pro tot exclu-

dentibus quot necessarii videntur numeri α, ε, γ etc. sunt computati; sed de hac re sicut de aliis artificiis laborem contrahendi hic agere non licet.

323. Omnes repraesentationes numeri dati A per formam binariam $mxx + nyy$, siue solutiones aequationis indeterminatae $mxx + nyy = A$, in sectione V methodo generali inuenire docuimus, cuius breuitas quoque nihil desiderandum relinquere videtur, si omnes valores expr. $\sqrt{-mn}$ secundum modulum A ipsum, et per suos factores quadratos diuisum, iam habentur; hic autem pro eo casu, vbi mn est positiuus, solutionem explicabimus, directa multo expeditiorem, si ad hanc illos valores antea computare oportet. Supponemus autem, numeros m, n et A esse positiuos atque inter se primos, quum casus reliqui ad hunc facile possint reduci. Manifesto quoque sufficit, valores positiuos ipsorum x, y eruere, quum reliqui inde per solam signorum mutationem deducantur.

Perspicuum est, x ita comparatum esse debere, vt $\frac{A - mxx}{n}$, pro quo scribemus V, positiuus, integer, et quadratus euadat. Conditio prima requirit, vt x non sit maior quam $\sqrt{\frac{A}{m}}$; secunda iam per se locum habet quando $n = 1$, alioquin requirit, vt valor expr. $\frac{A}{m}$ (mod. n) sit residuum quadraticum ipsius n, designandoque omnes valores diuersos expr. $\sqrt{\frac{A}{m}}$ (mod. n) per $\pm r$, $\pm r'$ etc., x sub aliqua formarum nt

$+ r$, $nt - r$, $nt + r'$ etc. contentus esse debebit. Simplicissimum itaque foret, omnes numeros harum formarum infra limitem $\sqrt{\frac{A}{m}}$, quorum complexum per Ω exprimemus, pro x substituere, eosque solos retinere, pro quibus V fit quadratum. Hoc tentamen, quantum lubeat, contrahere, in art. sq. docebimus.

324. Methodus exclusionum, per quam hoc efficiemus, perinde ac in disqu. praec. in eo consistit, vt plures numeros, etiam hic *excludentes* vocandos, ad lubitum accipiamus, pro quibusnam valoribus ipsius x valor ipsius V fiat non residuum qu. horum excludentium inuestigemus, talesque x ex Ω eiiciamus. Per ratiocinia iis quae in art. 321 exposuimus omnino analoga apparet, tales tantum excludentes adhibendos esse, qui sint numeri primi aut numerorum primorum potestates, et pro excludente posterioris generis ea tantum ipsius non residua a valoribus ipsius V arcenda, quae sint residua omnium potestatum inferiorum eiusdem numeri primi, siquidem exclusio cum his iam est instituta.

Sit itaque excludens $E = p^\mu$ (includendo etiam eum casum vbi $\mu = 1$), vbi p est numerus primus ipsum m non metiens, supponamusque *) p^ν esse summam potestatem eiusdem numeri primi per quam n sit diuisibilis. Sint a, b,

*) Breuitatis caussa duos casus, in quibus n per p est diuisibilis ac non diuisibilis, simul complectimur; in posteriori $\nu = 0$ ponere oportet.

c etc. non residua quadratica ipsius E (omnia, quando $\mu = 1$; necessaria siue ea quae sunt residua potestatum inferiorum, quando $\mu > 1$). Computentur radices congruentiarum $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$ etc. (mod. $Ep^\nu = p^{\mu+\nu}$), quae sint α, $\mathfrak{G}$, γ etc., patetque facile, si pro quo valore ipsius x fiat $xx \equiv \alpha$ (mod. Ep^ν), valorem respondentem ipsius V fieri $\equiv a$ (mod. E) siue non residuum ipsius E, similiterque de numeris reliquis $\mathfrak{G}$, γ etc.; aeque facile vice versa perspicitur, si quis valor ipsius x producat $V \equiv a$ (mod. E), pro eodem fieri $xx \equiv \alpha$ (mod. Ep^ν), adeoque omnes valores ipsius x, pro quibus xx nulli numerorum α, $\mathfrak{G}$, γ etc. sec. mod. Ep^ν congruus sit, tales valores ipsius V producere, qui nulli numerorum a, b, c etc. sec. mod. E sint congrui. Eligantur iam e numeris α, $\mathfrak{G}$, γ etc. omnia residua quadratica ipsius Ep^ν, quae sint g, g', g'' etc., computentur valores expressionum $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$ etc. (mod. Ep^ν), ponamusque hinc prodire $\pm h$, $\pm h'$, $\pm h''$ etc. His ita factis manifestum est, omnes numeros formarum $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$ etc. ex Ω tuto eiici posse, nullique valori ipsius x in Ω post hanc exclusionem remanenti valorem ipsius V sub formis $Eu + a$, $Eu + b$, $Eu + c$ etc. contentum respondere posse. Ceterum manifestum est, tales valores ipsius V iam per se e nullo valore ipsius x prodire posse, quando inter numeros α, $\mathfrak{G}$, γ etc. nulla residua qu. ipsius Ep^ν inueniantur, adeoque in hoc casu numerum E tamquam excludentem applicari non posse. — Huiusmodi excludentes, quot placet, adhiberi,

atque sic numeri in Ω ad lubitum diminui possunt.

Videamus iam, annon etiam numeros primos ipsum m metientes, taliumue numerorum potestates tamquam excludentes adhibere liceat. Sit B valor expr. $\frac{A}{n}$ (mod. m), patetque, V semper ipsi B secundum mod. m congruum fieri, quicunque valor pro x accipiatur, adeoque ad possibilitatem aequ. prop. necessario requiri, vt B sit residuum quadraticum ipsius m. Designante itaque p diuisorem quemcunque primum imparem ipsius m, qui per hyp. ipsos n et A, adeoque etiam ipsum B non metietur, pro valore quocunque ipsius x erit V residuum ipsius p adeoque etiam cuiuscunque potestatis ipsius p; quamobrem p ipsiusque potestates nequeunt excludentium loco haberi. — Prorsus simili ratione quando m per 8 est diuisibilis ad, aequ. prop. possibilitatem necessario requiritur vt sit $B \equiv 1$ (mod. 8), vnde etiam V pro valore quocunque ipsius x fiet $\equiv 1$ (mod. 8), et proin binarii potestates ad exclusionem non idoneae. — Quando autem m per 4 neque vero per 8 est diuisibilis, ex simili ratione esse debebit $B \equiv 1$ (mod. 4), adeoque valor expr. $\frac{A}{n}$ (mod. 8) vel 1 vel 5; designetur per C. Nullo negotio perspicietur, pro valore pari ipsius x hic fieri $V \equiv C$; pro impari, $V \equiv C + 4$ (mod. 8); vnde patet, valores pares reiiciendos esse, quando $C = 5$; impares, quando $C = 1$. — Denique quando m per 2, neque vero per 4 est diuisibilis, sit vt an-

te C valor expr. $\frac{A}{n}$ (mod. 8), qui erit 1, 3, 5, vel 7; atque D valor huius $\frac{\frac{1}{2}m}{n}$ (mod. 4), qui erit 1 vel 3. Iam quum valor ipsius V manifesto semper fiat $\equiv C - 2Dxx$ (mod. 8), adeoque pro x pari $\equiv C$, pro impari $\equiv C - 2D$, facile hinc colligitur, reiiciendos esse omnes valores impares ipsius x, quando $C = 1$; omnes pares, quando $C = 3$ et $D = 1$, aut $C = 7$ et $D = 3$, atque valores remanentes omnes producere $V \equiv 1$ (mod. 8) siue residuum cuiusuis potestatis binarii; in casibus reliquis autem, puta quando $C = 5$, aut $C = 3$ et $D = 3$, aut $C = 7$ et $D = 1$, fiet $V \equiv 3$, 5 vel 7 (mod. 8), siue x accipiatur par siue impar, vnde liquet, in his casibus aequationem prop. solutionem omnino non admittere.

Ceterum quum prorsus simili modo, vt hic valorem ipsius x per exclusiones inuenire docuimus, etiam, mutatis mutandis, valorem ipsius y elicere possimus, methodum exclusionis ad problematis propositi solutionem duobus semper modis applicare licebit (nisi $m = n = 1$, vbi coincidunt), e quibus si plerumque est praeferendus, pro quo Ω terminorum multitudinem minorem continet, quod facile a priori aestimari poterit. — Denique vix necesse erit obseruare, si post aliquot exclusiones *omnes* numeri ex Ω abierint, hoc vt certum indicium impossibilitatis aequationis propositae esse considerandum.

325. *Ex.* Proposita sit aequatio $3xx + 455yy = 10857362$, quam duplici modo solue-

mus, primo inuestigando valores ipsius x, dein valores ipsius y. Limes illorum in hoc casu est $\sqrt{3619120\frac{2}{3}}$, qui cadit inter 1902 et 1903; valor expr. $\frac{A}{3}$ (mod. 455) est 354 atque valores expr. $\sqrt{354}$ (mod. 455) hi $\pm$ 82, $\pm$ 152, $\pm$ 173, $\pm$ 212. Hinc Ω constat e 33 numeris sequentibus: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. Numerus 3 in hoc casu ad exclusionem adhiberi nequit, quia ipsum m metitur. Pro excludente 4 habemus $a = 2$, $b = 3$, vnde $\alpha = 0$, $\beta = 3$; $g = 0$, atque valores expr. $\sqrt{g}$ (mod. 4) hos 0 et 2; hinc sequitur, omnes numeros formarum $4t$ et $4t + 2$, i. e. omnes pares ex Ω eiiciendos esse; designentur (sedecim) reliqui per Ω'. Pro $E = 5$, qui etiam ipsum n metitur, habemus radices congruentiarum $mz \equiv A - 2n$ et $mz \equiv A - 3n$ (mod. 25) has 9 et 24, quae ambae sunt residua ipsius 25, valoresque expressionum $\sqrt{9}$ et $\sqrt{24}$ (mod. 25) fiunt $\pm$ 3, $\pm$ 7; eiectis ex Ω' omnibus numeris formarum $25t \pm 3$, $25t \pm 7$ restant hi decem (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Pro $E = 7$, habemus congruentiarum $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) radices 32, 39, 18, quae omnes sunt residua ipsius 49, atque valores expr. $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) hos $\pm$ 9, $\pm$ 23, $\pm$ 19; eiectis ex Ω'' numeris formarum $49t \pm 9$, $49t \pm 19$, $49t \pm 23$ remanent hi quinque (Ω'''): 537, 737, 1083, 1213,

1517. Pro $E = 8$ habemus $a = 5$, vnde $\alpha = 5$, qui est non residuum ipsius 8; quare excludens 8 non potest adhiberi. Numerus 9 ex eadem ratione praetereundus est vt 3. Pro $E = 11$ numeri a, b etc. fiunt 2, 6, 7, 8, 10; $\nu = 0$; vnde numeri α, $\mathfrak{C}$ etc. $= 8, 10, 5, 0, 1$, e quibus tres sunt residua ipsius 11 puta 0, 1, 5; hinc deducitur, ex Ω''' reiiciendos esse numeros formarum $11t$, $11t \pm 1$, $11t + 4$, quo facto remanent 537, 1083, 1213. Quos tentando prodeunt pro V resp. valores 21961, 16129, 14161, e quibus secundus ac tertius soli sunt quadrata. Quare aequ. prop. duas solutiones per valores positiuos ipsorum x, y admittit, $x = 1083$, $y = 127$, et $x = 1213$, $y = 119$.

II. Si alteram eiusdem aequationis incognitam per exclusiones indagare placet, ponatur haec sub formam $455xx + 3yy = 10857362$, commutando x cum y, vt omnia signa artt. 323, 324 retinere liceat. Limes valorum ipsius x hic cadit inter 154 et 155; valor expr. $\frac{A}{m}$ (mod. n) est 1; valores huius $\sqrt{1}$ (mod. 3) sunt $+1$ et -1. Quare Ω continet omnes numeros formarum $3t + 1$ et $3t - 1$, i. e. omnes per 3 non diuisibiles vsque ad 154 incl., quorum multitudo est 103; applicando autem praecepta supra data inuenitur

pro excl.	reiiciendos esse numeros formarum
3	$9t \pm 4$
4	$4t$, $4t + 2$ siue omnes pares
9	$27t \pm 1$, $27t \pm 10$
11	$11t$, $11t \pm 1$, $11t \pm 3$
17	$17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$
19	$19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$
23	$23t$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$

His deletis superstites inueniuntur 119, 127, 137, e quibus duo priores soli ipsi V valorem quadratum conciliant, easdemque solutiones suggerunt, ad quas supra peruenimus.

326. Methodus praecedens iam per se tam expedita est, vt vix quidquam optandum relinquat; attamen per multifaria artificia magnopere adhuc contrahi potest, e quibus hic pauca tantum attingere licet. Restringemus itaque disquisitionem ad eum casum, vbi excludens est numerus primus impar ipsum A non metiens, siue talis primi potestas, praesertim quoniam casus reliqui vel ad hunc reduci vel methodo analoga tractari possunt. Supponendo *primo*, excludentem $E = p$ esse numerum primum ipsos m, n non metientem, atque valores expr. $\frac{A}{m}$, $-\frac{na}{m}$, $-\frac{nb}{m}$, $-\frac{nc}{m}$ etc. (mod. p) resp. k, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc.: numeri α, $\mathfrak{C}$, γ etc. inueniuntur per congruentias $\alpha \equiv k + \mathfrak{A}$, $\mathfrak{C} \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$ etc. (mod. p). Numeri $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. autem per artificium ei prorsus simile quo in art. 322 vsi sumus sine congruentiarum computatio-

ne erui possunt, et vel cum omnibus non-residuis, vel cum omnibus residuis ipsius p (praeter 0) conuenient, prout valor expr. $-\frac{m}{n}$ (mod. p), siue (quod hic eodem redit) numerus $-mn$ est residuum vel non residuum ipsius p. Ita in *ex.* II art. praec. pro $E = 17$ fit $k = 7$; $-mn = -1365 \equiv 12$ est non residuum ipsius 17; hinc numeri $\mathfrak{A}$, $\mathfrak{B}$ etc. erunt 1, 2, 4, 8, 9, 13, 15, 16 adeoque numeri α, $\mathfrak{C}$ etc. 8, 9, 11, 15, 16, 3, 5, 6; ex his residua sunt 8, 9, 15, 16, vnde $\pm h$, h' etc. fiunt $\pm 5, 3, 7, 4$. — Quibus saepius occasio est huiusmodi problemata soluendi, commoditati suae eximie consulent, si pro pluribus numeris primis p, valores ipsorum h, h' etc. singulis valoribus ipsorum k, (1, 2, 3...$p - 1$) respondentes, in duplici suppositione (puta vbi $-mn$ est residuum et vbi non-residuum ipsius p) computent. Ceterum obseruamus adhuc, multitudinem numerorum h, $-h$, h' etc. semper esse $\frac{1}{2}(p-1)$, quando vterque numerus k et $-mn$ sit residuum vel vterque non residuum ipsius p; $\frac{1}{2}(p-3)$, quando prior *R.*, posterior *N.R.*; $\frac{1}{2}(p+1)$, quando prior *NR.*, posterior *R.*; sed demonstrationem huius theorematis ne nimis prolixi fiamus supprimere debemus.

Quod autem, *secundo*, eos casus attinet, vbi E est numerus primus ipsum n metiens, aut potestas numeri primi (imparis) ipsum n metientis seu non metientis, hi adhuc expeditius tractari possunt. Omnes hos casus simul complectemur, omnibusqus art. 324 signis retentis ponemus $n = n'p'$, ita vt n' per p non sit di-

uisibilis. Numeri a, b, c etc. erunt producta numeri $p^{\mu-1}$ vel in omnes numeros ipso p minores (praeter o), vel in omnia non residua ipsius p infra p, prout μ est par vel impar; exprimantur indefinite per $up^{\mu-1}$. Sit k valor expr. $\frac{A}{m}$ (mod. $p^{\mu+\nu}$), eritque per p non diuisibilis, quia eadem proprietas in A supponitur; porro patet, omnes α, β, γ etc. ipsi k sec. mod. p congruos fieri, adeoque p^{μ} nihil ex Ω excludere, si kNp; si vero kRp adeoque etiam $kRp^{\mu+\nu}$, sit r valor expr. $\sqrt{k}$ (mod. $p^{\mu+\nu}$), qui per p non erit diuisibilis, atque e valor huius $-\frac{n'}{2mr}$ (mod. p), eritque $\alpha \equiv rr + 2erap$ (mod. $p^{\mu+\nu}$), vnde facile colligitur, α esse residuum ipsius $p^{\mu+\nu}$, atque valores expr. $\sqrt{\alpha}$ (mod. $p^{\mu+\nu}$) fieri $\pm (r + eap^{\mu})$; hinc omnes h, h', h'' etc. exprimentur per $r + ep^{\mu+\nu-1}$. Denique nullo negotio hinc concluditur, numeros h, h', h'' etc. oriri ex additione numeri r cum productis numeri $p^{\mu+\nu-1}$ *vel* in omnes numeros infra p (praeter o), puta quando μ par; *vel* in omnia non residua ipsius p infra hunc limitem, quando μ impar atque eRp siue quod hic eodem redit quando $-2mrn'Rp$; *vel* in omnia residua (praeter o), quando μ impar atque $-2mrn'Np$.

Ceterum simulac pro singulis excludentibus, quos applicare placet, numeri h, h' etc. sunt eruti, exclusionem ipsam etiam per operationes mechanicas perficere licebit, quales quisque harum rerum peritus facile proprio marte excogitare poterit, si operae pretium esse videbitur.

Tandem obseruare debemus, quamuis aequationem $axx + 2bxy + cyy = M$, in qua $bb - ac$ negatiuus $= -D$, facile ad eam formam quam in praecc. considerauimus reduci posse. Designando enim diuisorem communem maximum numerorum a, b per m, et ponendo $a = ma'$, $b = mb'$, $\frac{D}{m} = a'c - mb'b' = n$, $a'x + b'y = x'$, aequ. illa manifesto aequiualet huic $mx'x' + nyy = a'M$, quae per praecepta supra tradita solui poterit. Ex huius autem solutionibus eae tantum erunt retinendae, in quibus $x' - b'y$ per a' fit diuisibilis, siue vnde x valores integros nanciscitur.

327. Quemadmodum solutio directa aequationis $axx + 2bxy + cyy = M$ in sect. V contenta valores expr. $\sqrt{(bb - ac)}$ (mod. M) notos supponit: ita vice versa pro eo casu, vbi $bb - ac$ est negatiuus, solutio indirecta in praecc. exposita methodum expeditissimam subministrat, illos valores eruendi, quae, praesertim pro valore permagno ipsius M, methodo art. 322 sqq. longe est praeferenda. Supponemus autem, M esse numerum primum, aut saltem ipsius factores, si compositus esset, adhuc incognitos; si enim constaret, numerum primum p ipsum M metiri, atque esse $M = p^{\mu}M'$, ita vt M' factorem p non amplius implicet, longe commodius foret, valores expr. $\sqrt{(bb - ac)}$ pro modulis p^{μ} et M' sigillatim explorare (priores ex valoribus secundum modulum p, art. 101), valoresque sec. mod. M ex horum combinatione deducere (art. 105).

Quaerendi sint itaque omnes valores expr. $\sqrt{} - D$ (mod. M), vbi D et M positiui supponuntur, atque M sub forma diuisorum ipsius $xx + D$ contentus (art. 147 sqq.), alioquin enim a priori constaret, nullos numeros expressioni propositae satisfacere posse. Sint valores quaesiti, e quibus bini semper oppositi erunt, $\pm r$, $\pm r'$, $\pm r''$ etc., atque $D + rr = Mh$, $D + r'r' = Mh'$, $D + r''r'' = Mh''$ etc.; porro designentur classes ad quas formae (M, r, h), $(M, -r, h)$, (M, r', h), $(M, -r', h)$, (M, r'', h), $(M, -r'', h)$ etc. pertinent, resp. per $\mathfrak{C}$, $-\mathfrak{C}$, $\mathfrak{C}'$, $-\mathfrak{C}'$, $\mathfrak{C}''$, $-\mathfrak{C}''$ etc., ipsarumque complexus per $\mathfrak{G}$. Hae classes quidem, generaliter loquendo, tamquam incognitae sunt spectandae; attamen perspicuum est, *primo*, omnes esse positiuas atque proprie primitiuas, *secundo* omnes ad idem genus pertinere, cuius *character* ex indole numeri M, i. e. ex ipsius relationibus ad singulos diuisores primos ipsius D (insuperque ad 4 aut 8 quando hae sunt necessariae) facile cognosci possit (art. 230). Quum suppositum sit, M contineri sub forma diuisorum ipsius $xx + D$, a priori certi esse possumus, huic characteri necessario genus pos. pr. pr. formarum determ. — D respondere, etiamsi forsan expressioni $\sqrt{} - D$ (mod. M) satisfieri nequeat; quum itaque hoc genus sit notum, omnes classes in ipso contentae erui poterunt, quae sint C, C', C'' etc., atque ipsarum complexus G. Patet igitur, singulas classes $\mathfrak{C}$, $-\mathfrak{C}$ etc. cum aliqua classe in G identicas esse debere; fieri potest quoque, vt plures classes in $\mathfrak{G}$ inter se, adeoque cum eadem in G identicae sint, et quando G vnicam

classem continet, certo omnes in $\mathfrak{G}$ cum hac conuenient. Quare si e classibus C, C', C'' etc. formae (simplissimae) f, f', f'' etc. eliguntur, (vna e singulis): e singulis classibus in $\mathfrak{G}$ vna forma inter has reperietur. Iam si $axx + 2bxy + cyy$ est forma in classe $\mathfrak{C}$ contenta, dabuntur duae repraesentationes numeri M per ipsam ad valorem r pertinentes, et si vna est $x = m$, $y = n$, altera erit $x = -m$, $y = -n$; vnicus casus excipi debet, vbi $D = 1$, in quo quatuor repraesentationes dabuntur (v. art. 180).

Ex his colligitur, si omnes repraesentationes numeri M per singulas formas f, f', f'' etc. inuestigentur (per methodum indirectam in praecc. traditam), atque hinc valores expr. $\sqrt{-D}$ (mod. M) ad quos singulae pertinent deducantur (art. 154 sqq), *omnes* valores huius expressionis inde obtineri, et quidem singulos bis, aut, si $D = 1$, quater. *Q. E. F.* Si quae formae inter f, f' etc. reperiuntur, per quas M repraesentari nequit, hoc est indicium, ipsas, ad nullam classem in $\mathfrak{G}$ pertinere, adeoque negligendas esse: si vero M per nullam illarum formarum repraesentari potest, necessario $-D$ debebit esse non residuum quadraticum ipsius M. — Circa has operationes teneantur adhuc obseruationes sequentes.

I. Repraesentationes numeri M per formas f, f' etc., quas hic adhibemus, subintelliguntur esse tales, in quibus indeterminatarum valores inter se primi sunt; si quae aliae se offerunt, in quibus hi valores diuisorem communem μ ha-

bent (quod tunc tantummodo accidere potest, vbi $\mu\mu$ metitur ipsum M, certoque accidet, quando $-DR\frac{M}{\mu\mu}$) hae: ad institutum praesens omnino negligi debent, etsi alio respectu vtiles esse possint.

II. Ceteris paribus labor manifesto eo facilior erit, quo minor est multitudo classium f, f', f'' etc., adeoque breuissimus, quando D est vnus e 65 numeris in art. 303. traditis, pro quibus in singulis generibus vnica tantum classis datur.

III. Quum binae semper huiusmodi repraesentationes $x = m$, $y = n$; $x = -m$, $y = -n$ ad eundem valorem pertineant, perspicuum est, sufficere, si eae tantummodo repraesentationes considerentur, in quibus y positiuus. *Tales* itaque repraesentationes diuersae semper valoribus diuersis expr. $\sqrt{-D}$ (mod. M) respondent, vnde multitudo omnium valorum diuersum multitudini omnium talium repraesentationum prodeuntium aequalis erit (semper excipiendo casum $D = 1$, vbi illa huius semissis erit).

IV. Quoniam, simulac alter duorum valorum oppositorum $+r$, $-r$, cognitus est, alter sponte innotescit, operationes adhuc aliquantum abbreuiari possunt. Si valor r obtinetur e repraesentatione numeri M per formam in classe C contentam, i. e. si $\mathfrak{C} = C$; valor oppositus $-r$ manifesto emerget e repraesentatione per formam, in classe ipsi C opposita contentam,

quae differens erit a classe C, nisi haec est anceps. Hinc sequitur, quando non omnes classes in G ancipites sint, e reliquis semissem tantum considerare oportere, puta e binis oppositis quibusque vnam, alteram negligendo, e qua valores iis, quos prior suppeditauit, oppositos resultare iam absque calculo praeuidere licet. Quando autem C est anceps, ambo valores r et $-r$ simul inde emergent; puta, si ex C classis anceps $axx + 2bxy + cyy$ electa est, atque valor r prodiit e repr. $x = m$, $y = n$, valor $-r$ prodibit ex hac $x = -m - \frac{2bn}{a}$, $y = n$.

V. Pro eo casu vbi $D = 1$, vna tantum classis omnino datur, e qua formam $xx + yy$ electam esse supponere licebit. Quodsi valor r ex repraesentatione $x = m$, $y = n$ prouenit, idem ex his prodibit $x = -m$, $y = -n$; $x = n$, $y = -m$; $x = -n$, $y = m$, oppositusque $-r$ ex his $x = m$, $y = -n$; $x = -m$, $y = n$; $x = n$, $y = m$; $x = -n$, $y = -m$; quare ex his octo reprr., quae vnicam discerptionem constituunt, vna sufficit, si modo valori inde resultanti oppositum associemus.

VI. Valor expr. $\sqrt{-D}$ (mod. M), ad quem repr. haec $M = amm + 2bmn + cnn$ pertinet, per art. 155 est $\mu(mb + nc) - \nu(ma + nb)$ siue numerus quicunque huic secundum M congruus, ipsis μ, ν ita acceptis vt fiat $\mu m + \nu n = 1$. Designando itaque talem valorem per v, erit $mv = \mu m(mb + nc) - \nu(M - mnb =$

$nnc) \equiv (\mu m + m)(mb + nc) \equiv mb + nc \pmod{M}$. Hinc patet, v esse valorem expr. $\frac{mb+nc}{m} \pmod{M}$; similique modo inuenitur, v esse valorem expr. $-\frac{ma+nb}{n} \pmod{M}$. Hae formulae saepenumero ei ex qua deductae fuerunt praeferendae sunt.

328. *Exempla.* I. Quaeruntur omnes valores expr. $\sqrt{\ } - 1365 \pmod{5428681 = M}$; numerus M hic est $\equiv 1, 1, 1, 6, 11 \pmod{4, 3, 5, 7, 13}$ adeoque sub forma diuisorum ipsorum $xx + 1$, $xx + 3$, $xx - 5$, et sub forma non diuisorum ipsorum $xx + 7$, $xx - 13$, et proin sub forma diuisorum ipsius $xx + 1365$ contentus; characterque generis in quo classes $\mathfrak{G}$ reperientur erit $1, 4; R3; R5; N7; N13$. In hoc genere vnica classis continetur, e qua eligimus formam $6xx + 6xy + 229yy$; vt omnes repraesentationes numeri M per hanc inueniantur, ponemus $2x + y = x'$, vnde fieri debebit $3x'x' + 455yy = 2M$. Haec aequatio quatuor solutiones admittit in quibus y est positiuus, puta $y = 127$, $x' = \pm 1083$, $y = 119$, $x' = \pm 1213$. Hinc prodeunt quatuor solutiones aequ. $6xx + 6xy + 229yy = M$, in quibus y positiuus,

x	478	— 605	547	— 666
y	127	127	119	119

Solutio prima dat pro v valorem expr. $\frac{30517}{478}$ si-

ue $-\frac{3249}{127}$ (mod. M), vnde inuenitur 2350978; secunda producit valorem oppositum — 2350978; tertia hunc 2600262, quarta oppositum — 2600262.

II. Si qnaerendi sunt valores expr. $\sqrt{\ } - 286$ (mod. 4272943 = M), character generis in quo classes $\mathfrak{G}$ contentae sunt, inuenitur 1 *et* 7, 8; $R11$; $R13$; quare erit genus principale, in quo tres classes continentur, per formas (1, 0, 286), (14, 6, 23), (14, — 6, 23) exhibitae; ex his tertiam, vtpote secundae oppositam negligere licet. Per formam $xx + 286yy$ duae repraesentationes numeri M inueniuntur, in quibus y positiuus, puta $y = 103$, $x = \pm 1113$, vnde prodeunt valores expr. propositae hi 1493445, — 1493445. Per formam (14, 6, 23) autem M non repraesentabilis inuenitur, vnde concluditur, praeter duos valores inuentos alios non dari.

III. Proposita expr. $\sqrt{\ } - 70$ (mod. 997331), classes $\mathfrak{G}$ contentae esse debebunt in genere cuius character 3 *et* 5, 8; $R5$; $N7$; in hoc vnica classis reperitur cuius forma repraesentans haec (5, 0, 14). At calculo instituto inuenitur, numerum 997331 per formam (5, 0, 14) non esse repraesentabilem, quamobrem — 70 necessario erit non residuum qu. illius numeri.

329. Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resoluendi, ad grauissima ac vtilissima toti-

us arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupauisse, tam notum est, vt de hac re copiose loqui superfluum foret. Nihilominus fateri oportet, omnes methodos hucusque prolatas vel ad casus valde speciales restrictas esse, vel tam operosas et prolixas, vt iam pro numeris talibus, qui tabularum a viris meritis constructarum limites non excedunt, i. e. pro quibus methodi artificiales superuacuae sunt, calculatoris etiam exercitati patientiam fatigent, ad maiores autem plerumque vix applicari possint. Etsi vero illae tabulae, quae in omnium manibus versantur, et quas subinde adhuc vlterius continuatum iri sperare licet, in plerisque casibus vulgo occurrentibus vtique sufficiant: tamen calculatori perito occasio haud raro se offert, e numerorum magnorum resolutione in factores magna emolumenta capiendi, quae temporis dispendium mediocre largiter compensent; praetereaque scientiae dignitas requirere videtur, vt omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur. Propter has rationes non dubitamus, quin duae methodi sequentes, quarum efficaciam ac breuitatem longa experientia confirmare possumus, arithmeticae amatoribus haud ingratae sint futurae. Ceterum in problematis natura fundatum est, vt methodi *quaecunque* continuo prolixiores euadant, quo maiores sunt numeri ad quos applicantur; attamen pro methodis sequentibus difficultates perlente increscunt, numerique e septem, octo vel adeo adhuc pluribus figuris constantes praesertim per secundam felici semper successu tra-

ctati fuerunt, omnique celeritate, quam pro tantis numeris exspectare aequum est, qui secundum omnes methodos hactenus notas laborem, etiam calculatori indefatigabili intolerabilem, requirerent.

Antequam methodi sequentes in vsum vocentur, semper vtilissimum est, diuisionem numeri cuiusque propositi per aliquot numeros primos minimos tentare, puta per 2, 3, 5, 7 etc. vsque ad 19 aut adhuc vlterius, non solum, ne poeniteat, talem numerum quando diuisor est per methodos subtiles ac artificiosas eruisse, qui multo facilius per solam diuisionem inueniri potuisset *), sed etiam, quod tunc, vbi nulla diuisio successit, applicatio methodi secundae *residuis* ex illis diuisionibus ortis magno cum fructu vtitur. Ita e. g. si numerus 314159265 in factores suos resoluendus est, diuisio per 3 bis succedit, posteaque etiam diuisiones per 5 et 7, vnde habetur $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$, sufficitque numerum 997331, qui per 11, 13, 17, 19 non diuisibilis inuenitur, examini subtiliori subiicere. Similiter proposito numero 43429448, factorem 8 auferemus, methodosque magis artificiales ad quotientem 5428681 applicabimus.

330. Fundamentum METHODI PRIMAE est theorema, *quemuis numerum positiuum seu negatiuum, qui alius numeri M residuum quadraticum sit, etiam residuum cuiusuis diuisoris*

*) Eo magis, quod inter sex numeros, generaliter loquendo, vix *vnus* per omnes 2, 3, 5 ... 19 non diuisibilis reperitur.

ipsius M esse. Vulgo notum est, si M per nullum numerum primum infra $\sqrt{M}$ diuisibilis sit, certo M esse primum; si vero omnes numeri primi infra hunc limitem, ipsum M metientes sint p, q etc., numerum M vel ex his *solis* (ipsorumue potestatibus) compositum esse, vel *vnum* tantum alium factorem primum maiorem quam $\sqrt{M}$ implicare posse, qui inuenitur, diuidendo ipsum M per p, q etc. quoties licet. Designando itaque complexum omnium numerorum primorum infra $\sqrt{M}$ (exclusis iis, per quos diuisio frustra iam tentata est) per Ω, manifesto sufficit, si omnes diuisores primi ipsius M, in Ω contenti, habeantur. Iam si alicunde constat, numerum aliquem r (non-quadratum) esse residuum quadraticum ipsius M, nullus certo numerus primus cuius NR est r diuisor ipsius M esse poterit; quare ex Ω omnes huiusmodi numeros primos (qui plerumque omnium semissem fere efficient) eiicere licebit. Si insuper de alio numero non quadrato, r', constat, ipsum esse residuum ipsus M, e numeris primis in Ω post primam exclusionem relictis iterum eos excludere poterimus, quorum $N.R$ est r', qui rursus illorum semissem fere conficient, siquidem residua r et r' sunt independentia, (*i. e.* nisi alterum necessario per se est residuum omnium numerorum, quorum residuum est alterum, quod eueniret quando rr' esset quadratum). Si adhuc alia residua ipsius M noti sunt, r'', r''' etc., quae omnia a reliquis sunt independentia *), cum singulis ex-

*) Si productum e numeris quotcunque r, r', r'' etc. quadratum est; quisque ipsorum e, g, r erit residuum cuiusuis

clusiones similes institui possunt, per quas multitudo numerorum in Ω rapidissime diminuetur, ita vt mox vel omnes deleti sint, in quo casu M certo erit numerus primus, vel tam pauci restent (inter quos, omnes diuisores primi ipsius M, si quos habet, manifesto reperientur), vt diuisio per ipsos nullo negotio tentari possit. Pro numero millionem non multum superante plerumque sex aut septem; pro numero ex octo aut nouem figuris constante, nouem aut decem exclusiones abunde sufficient. Duo iam sunt de quibus agere oportebit, *primo* quomódo residua ipsius M idonea et satis multa inueniri possint, *deinde* quo pacto exclusionem ipsam commodissime perficere liceat. Sed ordinem harum quaestionum inuertemus, praesertim quoniam secunda docebit, qualia potissimum residua ad hunc finem sint commoda.

331. Numeros primos quorum residuum est numerus datus r (quem per nullum quadratum diuisibilem supponere licet), ab iis quorum non residuum est, siue diuisores expr. $xx - r$ a non diuisoribus distinguere, in sect. IV copiose docuimus, omnes priores sub certis huiusmodi formulis $rz + a$, $rz + b$ etc., aut talibus $4rz + a$, $4rz + b$ etc. contentos esse, posterioresque sub aliis similibus. Quoties r est numerus valde paruus, exclusiones adiumento harum formularum percommode perfici possunt; e. g. excludendi erunt

numeri primi (nullum ex ipsis metientis), qui reliquorum r', r'' etc. residuum est. Vt igitur residua quotcunque tamquam independentia considerari possint, nullum productum nec e binis, nec e ternis etc. quadratum esse oportet.

omnes numeri formae $4z + 3$, quando $r = -1$; omnes numeri formarum $8z + 3$ et $8z + 5$, quando $z = 2$ etc. Sed quum non semper in potestate sit, huiusmodi residua numeri propositi M inuenire, neque formularum applicatio pro valore magno ipsius r satis commoda sit, ingens lucrum est, laboremque exclusionis mirifice subleuat, si pro multitudine satis magna numerorum (r) per quadratum non diuisibilium tum positiuorum tum negatiuorum *tabula* iam constructa habetur, in qua numeri primi quorum residua sunt illi singuli (r) ab iis quorum non residua sunt distinguuntur. Talis tabula perinde adornari poterit ac specimen ad calcem huius operis adiectum supraque iam descriptum; sed vt ad institutum praesens vtilitatem satis amplam praestet, numeri primi in margine positi (moduli) longe vlterius puta saltem vsque ad 1000 aut ad 10000 continuati esse debent, praetereaque commoditas multum augetur, si in facie etiam numeri compositi et negatiui recipiuntur, etsi hoc non sit absolute necessarium, vt e sect. IV perspicuum est. Ad summum autem commoditatis fastigium vsus talis tabulae euehetur, si singulae columellae verticales e quibus constat exsecantur lamellisque aut baculis (Neperianis similibus) agglutinantur, ita vt eae quae in quouis casu sunt necessariae i. e. quae numeris r, r', r'' etc., residuis numeri propositi in factores resoluendi, respondent, separate examinari possint. Quibus iuxta tabulae columnam primam (quae modulos exhibet) *rite* positis, i. e. ita, vt loca singulorum baculorum eidem numero primo columnae primae respondentium

cum hoc in directum iaceant, siue in eadem linea horizontali siti sint: manifesto ei numeri primi, qui post exclusiones cum residuis r, r', r'' ex Ω remanent, per solam inspectionem immediate cognosci poterunt; nimirum hi conuenient cum iis in columna prima, quibus in *omnibus* baculis adiacentibus lineolae respondent, reiiciique debent omnes, quibus in *vllo* bacillo spatium vacuum adiacet. Per exemplum haec sufficienter illustrabuntur. Si alicunde constat, numeros -6, $+13$, -14, $+17$, $+37$, -53 esse residua ipsius 997331, consociandae erunt columna prima (quae in hoc casu vsque ad 997 continuata esse debet, i. e. vsque ad numerum primum proxime minorem quam $\sqrt{997331}$) atque lamellae, in quarum facie numeri -6, $+13$ etc. sunt suprascripti. Ecce partem schematis hoc modo prodeuntis:

	−	+	−	+	+	−
	6	13	14	17	37	53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
e	t	c.		e	t	c.
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—			
e	t	c.		e	t	c.

Quemadmodum hic ex sola inspectione cognoscitur, ex iis numeris primis *qui in hac schematis parte continentur* solum 127 post exclusiones cum residuis — 6, 13 etc. in Ω relinqui, ita schema integrum vsque ad 997 extensum ostendit, *omnino* nullum alium ex Ω remanere; diuisione autem tentata, 997331 per 127 reuera diuisibilis inuenitur. Hoc itaque modo ille numerus in factores primos 127×7853 resolutus habetur *).

Ceterum ex hac expositone abunde colligitur, praesertim vtilia esse residua non nimis magna, aut saltem in factores primos non nimis magnos resolubilia, quum tabulae auxiliaris vsus immediatus non vltra numeros in facie positos pateat, vsusque mediatus tales tantum complectatur, qui in factores in tabula contentos resolui possunt.

332. Ad inuenienda residua numeri dati M tres methodos diuersas trademus, quarum expositioni duas obseruationes praemittimus, quarum adiumento e residuis minus idoneis simpliciora deriuari possunt. *Primo*, si numerus akk per quadratum kk diuisibilis (quod ad M primum esse supponitur) est residuum ipsius M, etiam a erit residuum; propter hanc rationem residua

*) Auctor apparatum satis amplum tabulae hic descriptae, quem ad vsum suum construendum curauit, publici iuris lubenter faceret, si paucitas eorum, quibus vsui esse potest, sumtibus talis incepti sustentandis sufficeret. Si quis interea arithmeticae amator, principiis probe penetratis, proprio marte talem tabulam sibi condere optat, auctor magnae voluptati sibi ducet, omnia cum eo emolumenta ac artificia per literas communicare.

per magna quadrata diuisibilia aeque vtilia sunt ac parua; omniaque residua per methodos sequentes suppeditata a factoribus suis quadratis statim liberata supponemus. *Secundo* si duo pluresue numeri sunt residua, etiam productum ex ipsis residuum erit. Combinando hanc obseruationem cum praec., persaepe e pluribus residuis quae non omnia sunt satis simplicia aliud admodum simplex deduci potest, si modo illa multos factores communes implicant. Hanc ob caussam talia quoque residua valde sunt opportuna, quae e multis factoribus non nimis magnis composita sunt, conuenietque omnia statim in factores suos resoluere. Vis harum obseruationum melius per exempla vsumque frequentem quam per praecepta percipietur.

I. Methodus simplicissima, iisque, qui per frequentem exercitationem iam aliquam dexteritatem sibi conciliauerunt, commodissima, consistit in eo, vt M aut generalius multiplum quodcunque ipsius M quomodocunque in duas partes decomponatur $kM = a + b$ (siue vtraque sit positiua siue altera positiua altera negatiua) quarum productum signo mutato erit residuum ipsius M; erit enim $-ab \equiv aa \equiv bb \pmod{M}$, adeoque $-abRM$. Numeri a, b ita accipiendi sunt, vt productum per quadratum magnum diuisibile quotiensque vel paruus vel saltem in factores non nimis magnos resolubilis euadat, quod semper non difficile effici poterit. Imprimis commendandum est, vt pro a accipiatur vel quadratum, vel quadratum duplex, vel triplex etc. a numero M numero vel paruo

vel in factores commodos resolubili discrepans. Ita e. g. inuenitur $997331 = 999^2 - 2.5.67 = 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2 = 3.575^2 + 11.31.4^2 = 3.577^2 - 7.13.4^2 = 3.578^2 - 7.19.37 = 11.299^2 + 2.3.5.29.4^2 = 11.301^2 + 5.11^2$ etc. Hinc habentur residua sequentia $2.5.67$, -5.11, $-2.3.17$, $-3.11.31$, $3.7.13$, $3.7.19.37$, $-2.3.5.11.29$; discerptio vltima suppeditat residuum -5.11 quod iam habemus. Pro residuis $-3.11.31$, $2.3.5.11.29$ haec adoptare possumus $3.5.31$, $2.3.29$, ex illorum combinatione cum -5.11 oriunda.

II. Methodus secunda et tertia inde petuntur, quod, si duae formae binariae (A, B, C), (A', B', C') eiusdem determinantis M, aut $-M$, aut generalius $\pm kM$, ad idem genus pertinent, numeri AA', AC', $A'C$ sunt residua ipsius kM; hoc nullo negotio inde perspicitur, quod numerus quiuis characteristicus vnius formae, puta m, etiam est numerus char. alterius, adeoque mA, mC, mA', mC' omnes residua ipsius hM. Si itaque (a, b, a') est forma reducta determinantis positiui M aut generalius kM, atque (a', b', a''), (a'', b'', a''') etc. formae ex ipsius periodo, adeoque ipsi aequiualentes et a potiori sub eodem genere contentae: numeri aa', aa'', aa''' etc. omnes erunt residua ipsius M. Computus multitudinis magnae formarum talis periodi facillime adiumento algorithmi art. 187. instituitur; residua simplicissima plerumque prodeunt statuendo $a = 1$; ea quae factores nimis magnos implicant, erunt reiicienda. Ecce initia periodorum formarum $(1, 998, -1327)$ et $(1, 1412,$

— 918), quarum determinantes sunt 997331, 1994662:

(1, 998, — 1327)	(1, 1412, — 918)
(— 1327, 329, 670)	(— 918, 1342, 211)
(670, 341, — 1315)	(211, 1401, — 151)
(— 1315, 974, 37)	(— 151, 1317, 1723)
(37, 987, — 626)	(1723, 406, — 1062)
(— 626, 891, 325)	(— 1062, 656, 1473)
(325, 734, — 1411)	(1473, 817, — 901)
(— 1411, 677, 382)	(— 901, 985, 1137)
(382, 851, — 715)	etc.

Sunt itaque residua numeri 997331 omnes numeri — 1327, 670 etc.; negligendo autem ea, quae factores nimis magnos implicant, haecce habemus: 2.5.67, 37, 13, — 17.83, — 5.11.13, — 2.3.17, — 2.59, — 17.53; residuum 2.5.67, nec non hoc — 5.11, quod e combinatione tertii cum quinto euoluitur, iam supra erueramus.

III. Si C est classis quaecunque formarum det. neg. — M siue generalius — kM, a principali diuersa, ipsiusque periodus haec $2C$, $3C$ etc. (art. 307.): classes $2C$, $4C$ etc. ad genus principale pertinebunt; hae vero $3C$, $5C$ etc. ad idem genus vt C. Si itaque (a, b, c) est forma (simplicissima) ex C atque (a', b', c') forma ex aliqua classe illius periodi puta ex nC, erit vel a', vel aa' residuum ipsius M, prout n par vel impar (in casu priori manifesto etiam c', in posteriori ac', ca' et cc'). Euolutio periodi, i. e. formarum simplicissimarum in ipsius classibus, mira facilitate perficitur, quando a est valde paruus,

praesertim quando est $= 3$, quod semper efficere licet, quando $kM \equiv 2 \pmod 3$. Ecce initium periodi classis, in qua est forma $(3, 1, 332^2444)$

C $(3, 1, 332^2444)$	$6C$ $(729, -209, 1428)$
$2C$ $(9, -2, 110815)$	$7C$ $(476, 209, 2187)$
$3C$ $(27, 7, 36940)$	$8C$ $(1027, 342, 1085)$
$4C$ $(81, 34, 12327)$	$9C$ $(932, -437, 1275)$
$5C$ $(243, 34, 4109)$	$10C$ $(425, 12, 2347)$

Hinc promanant residua (inutilibus reiectis) $3.476, 1027, 1085, 425$ siue (tollendo factores quadratos) $3.7.17, 13.79, 5.7.31, 17$, e quorum combinatione apta cum octo residuis in II inuentis facile eruuntur duodecim sequentia -2.3, 13, -2.7, 17, 37, -53, -5.11, 79, -83, -2.59, -2.531, $2.5.67$; sex priores sunt iidem quibus in art. 331 vsi sumus. Adiici potuissent residua 19 et -29, si ea quoque in vsum vocare voluissemus, quae in I reperta sunt; reliqua illic eruta ab iis quae hic euoluimus iam sunt dependentia.

333. Methodus secunda, numerum datum M in factores resoluendi, petitur e consideratione valorum talis expr. $\sqrt{-D} \pmod M$, obseruationibusque sequentibus innititur.

I. Quando M est numerus primus aut potestas numeri primi (imparis ipsumque D non metientis), erit $-D$ residuum vel non residuum ipsius M, prout M vel in forma diuisorum vel in forma non diuisorum ipsius $xx + D$ continetur, et in casu priori expressio $\sqrt{-D} \pmod$

M) duos tantummodo valores diuersos habebit, qui oppositi erunt.

II. Quando vero M est compositus, puta $= pp'p''$ etc., designantibus p, p', p'' etc. numeros primos (diuersos impares ipsumque D non metientes) aut talium numerorum potestates: — D tunc tantummodo residuum ipsius M erit, quando est residuum singulorum p, p', p'' etc., i. e. quando hi numeri omnes in formis diuisorum ipsius $xx + D$ continentur. Designando autem valores expr. $\sqrt{-D}$ sec. modulos p, p', p'' etc. resp. per $\pm r$, $\pm r'$, $\pm r''$ etc., omnes valores eiusdem expressionis sec. mod. M orientur, eruendo numeros qui secundum p sint $\equiv r$ aut $\equiv -r$, secundum p' aut $\equiv r'$ aut $\equiv -r'$ etc., quocirca ipsorum multitudo fiet $= 2^{\mu}$, designante μ multitudinem numerorum p, p', p'' etc. Quodsi itaque hi valores sunt R, $-R$, R', $-R'$, R'' etc., sponte erit $R \equiv R$ secundum omnes p, p', p'' etc., sed secundum nullos $R \equiv -R'$, vnde diuisor communis maximus numeri M cum $R - R$ erit M, et 1 diu. comm. max. ipsius M cum $R + R'$; sed valores duo nec identici nec oppositi vt R et R' necessario secundum vnum pluresue numerorum p, p', p'' etc., neque vero secundum omnes, congrui erunt, et secundum reliquos $R \equiv -R'$; hinc illorum productum erit diuisor communis maximus numerorum M et $R - R'$, productumque horum d. c. m. ipsorum M et $R + R'$. Hinc facile sequitur, si omnes diuisores communes maximi ipsius M cum differentiis inter singulos valores expr. $\sqrt{-D}$ (mod. M) atque aliquem valorem datum

computentur, horum complexum continere numeros 1, p, p', p'' etc. atque omnia producta e binis, ternis etc. horum numerorum. *Hoc itaque modo e valoribus illius expressionis numeros p, p', p'' etc. eruere licebit.*

Ceterum quum methodus art. 327 singulos hosce valores ad valores expressionum huius formae $\frac{m}{n}$ (mod. M) reducat, ita vt denominator n ad M primus sit: ad institutum praesens ne necessarium quidem est, has ipsas computare. Nam diu. comm. max. numeri M cum differentia inter R et R' qui cum $\frac{m}{n}$, $\frac{m'}{n'}$ conueniunt manifesto etiam erit diu. comm. max. ipsorum M et $nn'(R - R')$, siue ipsorum M et $mn' - m'n$, quippe cui $nn'(R - R')$ secundum modulum M est congruus.

334. Applicatio obseruationum praecc. ad problema de quo agimus duplici modo institui potest; prior non solum decidet, vtrum numerus propositus M primus sit an compositus, sed in hoc casu etiam factores ipsos suppeditat; posterior autem eatenus praestat, quod plerumque calculum expeditiorem permittit, sed factores ipsos numerorum compositorum, quos quoque a primis protinus distinguit, interdum non profert, nisi pluries repetatur.

I. Inuestigetur numerus negatiuus $-D$, qui sit residuum quadraticum ipsius M, ad quem finem methodi in art. 332 sub I et II traditae adhiberi poterunt. Per se quidem arbitrarium

est, quidnam residuum eligatur, neque hic vt in methodo praec. opus est, vt D sit numerus paruus; sed calculus eo breuior erit, quo minor est multitudo classium formarum binariarum in singulis generibus pr. pr. det. $-D$ contentarum; quamobrem imprimis talia residua qui inter 65 numeros art. 303 continentur, si qui se offerunt, opportuna erunt. Ita pro $M = 997331$ ex omnibus residuis negatiuis supra erutis hoc -102 maxime idoneum esset. Eruantur omnes valores diuersi expr. $\sqrt{-D}$ (mod. M); quodsi duo tantum proueniunt (oppositi), M certo erit vel numerus primus vel numeri primi potestas; si plures, puta 2^{μ}, M compositus erit ex μ numeris primis, aut primorum potestatibus, diuersis, qui factores per methodum art. praec. erui poterunt. Vtrum vero hi factores numeri primi sint an primorum potestates, tum per se facillimum erit dignoscere; tum etiam via ipsa per quam valores expr. $\sqrt{-D}$ inueniuntur, omnes numeros primos, quorum potestas aliqua ipsum M metitur, sponte indicat; scilicet si M diuisibilis est per quadratum numeri primi π, ille calculus certo etiam vnam pluresue repraesentationes tales numeri M, $M = amm + 2bmn + cnn$, produxerit, in quibus diuisor comm. max. numerorum m, n est π (et quidem ideo, quod in hoc casu $-D$ etiam est residuum ipsius $\frac{M}{\pi\pi}$). Quando vero nulla repraesentatio prodiit, in qua m, et n diuisorem communem habent, hoc certum indicium est, M per nullum quadratum diuisibilem esse adeoque omnes p, p', p'' etc. numeros primos.

Ex. Per methodum supra traditam inueniuntur quatuor valores expr. $\sqrt{} - 102$ (mod. 997331) cum valoribus harum $\pm \frac{1664}{113}$, $\pm \frac{2824}{3}$ conuenientes; diuisores communes maximi 997331 cum his $3.1664 - 113.2824$ et $3.1664 + 113.2824$ siue cum 314120 et 324104 eruuntur hi 7853 et 127, vnde $997331 = 127.7853$, vt supra.

II. Accipiatur aliquis numerus negatiuus $-D$ talis, vt M contentus sit in forma diuisorum ipsius $xx + D$; per se arbitrarium est, quis huiusmodi numerus eligatur, sed commoditatis caussa imprimis videndum est, vt multitudo classium in generibus det. $-D$ sit quam maxime parua. Ceterum inuentio talis numeri nulli difficultati obnoxia est, si tentando adeatur; nam plerumque inter multitudinem considerabilem numerorum tentatorum pro totidem fere M in forma diuisorum continetur, ac in forma non diuisorum. Quare maxime e re erit, tentamen a 65 numeris art. 303 inchoare (et quidem a maximis), et si eueniret, vt nullus idoneus esset (quod tamen generaliter loquendo inter 16384 casus semel tantum accidit), ad alios progredi, vbi classes binae in singulis generibus continentur. — Tunc inuestigentur valores expr. $\sqrt{} - D$ (mod. M), et si qui inueniuntur, factores ipsius M prorsus eodem modo inde deducantur vt supra; si vero nulli valores prodeunt, adeoque $-D$ est non residuum ipsius M, certo M neque numerus primus neque numeri primi potestas esse poterit. Quodsi in hoc casu factores ipsi desiderantur, vel eandem operationem repetere oportet, alios valores pro D accipiendo, vel ad methodum aliam confugere.

Ita e. g. tentamine facto 997331 contentus inuenitur in forma non diuisorum ipsorum $xx + 1848$, $xx + 1365$, $xx + 1320$, sed in forma diuisorum ipsius $xx + 840$; pro valoribus expr. $\sqrt{-840}$ (mod. 997331) prodeunt expr. $\pm \frac{1272}{163}$, $\pm \frac{3238}{125}$, vnde iidem factores deducuntur vt ante. — Si quis plura exempla desiderat, art. 328 consulat, vbi primum docet esse $542861 = 307 \cdot 17683$; secundum, 4272943 esse numerum primum; tertium, 997331 certe e pluribus primis compositum esse.

* * *

Ceterum limites huius operis praecipua tantum momenta vtriusque methodi factores inuestigandi hic exsequi permiserunt; disquisitionem vberiorem vna cum pluribus tabulis auxiliaribus aliisque subsidiis aliae occasioni reseruamus.

Sectio Septima

DE AEQVATIONIBVS CIRCVLI SECTIONES DEFINIENTIBVS.

335. Inter incrementa splendidissima, mathesi per recentiorum labores adiecta, theoria functionum a circulo pendentium procul dubio locum imprimis insignem tenet. Cui mirabili quantitatum generi, ad quod in disquisitionibus maxime heterogeneis saepissime deferimur, cuiusque subsidio nulla vniuersae matheseos pars carere potest, summi geometrae recentiores industriam sagacitatemque suam tam assidue impenderunt, disciplinamque tam vastam inde efformauerunt, vt parum exspectari potuisset, vllam huius theoriae partem, nedum elementarem atque in limine quasi positam, grauium adhuc incrementorum capacem esse. Loquor de theoria functionum trigonometricarum, arcubus cum peripheria commensurabilibus respondentium, siue de theoria polygonorum regularium, cuius quam parua pars hucusque enucleata sit, sectio praesens patefaciet. Mirari possent lectores, talem disquisitionem in hocce potissimum opere, disciplinae primo aspectu maxime heterogeneae imprimis dicato, institui; sed tractatio ipsa abun-

de declarabit, quam intimo nexu hoc argumentum cum arithmetica sublimiori coniunctum sit.

Ceterum principia theoriae, quam exponere aggredimur, multo latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transscendentes applicari possunt, e. g. ad eas quae ab integrali $\int \frac{dx}{\sqrt{(1-x^4)}}$ pendent, praetereaque etiam ad varia congruentiarum genera: sed quoniam de illis functionibus transscendentibus amplum opus peculiare paramus, de congruentiis autem in continuatione disquisitionum arithmeticarum copiose tractabitur, hoc loco solas functiones circulares considerare visum est. Imo has quoque, quas summa generalitate amplecti liceret, per subsidia in art. sq. exponenda ad casum simplicissimum reducemus, tum breuitati consulentes, tum vt principia plane noua huius theoriae eo facilius intelligantur.

336. Designando circuli peripheriam siue quatuor angulos rectos per P, supponendoque m, n esse integros, atque n productum e factoribus inter se primis a, b, c etc.: angulus $A = \frac{mP}{n}$ per art. 310 sub hanc formam reduci potest $A = \left(\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{etc.}\right) P$, functionesque trigonometricae ipsi respondentes e functionibus ad partes $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$ etc. pertinentibus per methodos notas deducentur. Quoniam itaque pro a, b, c etc. numeros primos aut numerorum primo-

rum potestates accipere licet: manifesto sufficit, sectionem circuli in partes, quarum multitudo est numerus primus aut primi potestas, considerare, polygonumque n laterum e polygonis a, b, c etc. laterum protinus habebitur. Attamen hoc loco disquisitionem ad eum casum restringemus, vbi circulus in partes diuidendus est, quarum multitudo est numerus primus (impar), sequenti praesertim ratione inducti. Constat, functiones circulares angulo $\frac{mP}{pp}$ respondentes e functionibus ad $\frac{mP}{p}$ pertinentibus per solutionem aequationis p^{ti} gradus deriuari, et perinde ex illis per aequationem aeque altam functiones ad $\frac{mP}{p^3}$ pertinentes etc., ita vt, si polygonum p laterum iam habeatur, ad determinationem polygoni p^λ laterum necessario solutio $\lambda - 1$ aequationum p^{ti} gradus requiratur. Etiamsi vero theoriam sequentem ad hunc quoque casum extendere liceret, tamen hac via non minus ad totidem aequationes p^{ti} gradus delaberemur, quae, siquidem p est numerus primus, ad inferiores deprimi nullo modo possunt. Ita e. g. infra ostendetur, polygonum 17 laterum geometrice construi posse: sed ad determinationem polygoni 289 laterum aequationem 17^{mi} gradus nullo modo euitare licet.

337. Satis constat, functiones trigonometricas omnium angulorum $\frac{kP}{n}$, denotando per k indefinite omnes numeros $0, 1, 2 \ldots n - 1$, per

radices aequationum n^{ti} gradus exprimi, puta *sinus* per radices huius (I)

$$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\tfrac{n.n-3}{1.2}x^{n-4} - \tfrac{1}{64}\tfrac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \mp \frac{1}{2^{n-1}}nx = 0$$

cosinus per radices huius (II)

$$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\tfrac{n.n-3}{1.2}x^{n-4} - \tfrac{1}{64}\tfrac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \mp \frac{1}{2^{n-1}}nx - 1 = 0$$

denique *tangentes* per radices huius (III)

$$x^n - \tfrac{n.n-1}{1.2}x^{n-2} + \tfrac{n.n-1.n-2.n-3}{1.2.3.4}x^{n-4} - \text{etc.} \mp nx = 0$$

Hae aequationes (quae generaliter pro quouis valore impari ipsius n valent, II vero pro pari quoque), ponendo $n = 2m + 1$, facile ad gradum m^{tum} deprimuntur; scilicet I et III, diuidendo partem a laeua per x et substituendo y pro xx. Aequatio II autem manifesto radicem $x = 1\,(= \cos 0)$ implicat, et e reliquis binae semper aequales sunt ($\cos \frac{P}{n} = \cos \frac{(n-1)P}{n}$, $\cos \frac{2P}{n} = \cos \frac{(n-2)P}{n}$ etc.); quare ipsius pars a laeua per $x - 1$ diuisibilis, quotiensque quadratum erit, cuius radicem quadratam extrahendo, aequatio II reducitur ad hanc

$$x^m + \tfrac{1}{2}x^{m-1} - \tfrac{1}{4}(m-1)x^{m-2} - \tfrac{1}{8}(m-2)x^{m-3} + \tfrac{1}{16}\tfrac{m-2.m-3}{1.2}x^{m-4} + \tfrac{1}{32}\tfrac{m-3.m-4}{1.2}x^{m-5} - \text{etc.} = 0$$

cuius radices erunt cosinus angulorum $\frac{P}{n}$, $\frac{2P}{n}$,

$\frac{3P}{n} \ldots \frac{mP}{n}$. Vlteriores reductiones harum aequationum, pro eo quidem casu vbi n est numerus primus, hactenus non habebantur.

Attamen nulla harum aequationum tam tractabilis et ad institutum nostrum tam idonea est, quam haec $x^n - 1 = 0$, cuius radices cum radicibus illarum arctissime connexas esse constat. Scilicet, scribendo breuitatis caussa i pro quantitate imaginaria $\sqrt{-1}$, radices aequationis $x^n - 1 = 0$ exhibentur per $\cos \frac{kP}{n} + i \sin \frac{kP}{n} = r$, vbi pro k accipiendi sunt omnes numeri $0, 1, 2 \ldots n - 1$. Quocirca quum sit $\frac{1}{r} = \cos \frac{kP}{n} - i \sin \frac{kP}{n}$, radices aequationis I exhibebuntur per $\frac{1}{2i}(r - \frac{1}{r})$ siue per $\frac{i(1-rr)}{2r}$; radices aequationis II per $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+rr}{2r}$; denique radices aequationis III per $\frac{i(1-rr)}{1+rr}$. Hanc ob caussam disquisitionem considerationi aequationis $x^n - 1 = 0$ superstruemus, ipsum n esse numerum primum imparem supponendo. Ne vero inuestigationum ordinem interrumpere oporteat, sequens lemma hic praemittimus.

338. Problema. *Data aequatione* $(W) \ldots z^m + Az^{m-1}$ *etc.* $= 0$, *inuenire aequationem* (W'), *cuius radices sint potestates* λ^{tae} *radicum aequationis* (W), *designante* λ *exponentem integrum positiuum datum.*

Sol. Designatis radicibus aequationis W per a, b, c etc., radices aequ. W' esse debebunt a^λ, b^λ, c^λ etc. Per theorema notum Newtonianum e coëfficientibus aequ. W inuenire licet aggregata quarumlibet potestatum radicum a, b, c etc. Quaerantur itaque summae $a^\lambda + b^\lambda + c^\lambda +$ etc., $a^{2\lambda} + b^{2\lambda} + c^{2\lambda}$ etc. etc. vsque ad $a^{m\lambda} + b^{m\lambda} + c^{m\lambda} +$ etc., vnde via inuersa per idem theorema coëfficientes aequ. W' deduci poterunt. *Q. E. F.* — Simul hinc liquet, si omnes coëfficientes in W sint rationales, omnes quoque in W' rationales euadere. Alia quidem via probari potest, si illi omnes integri sint, etiam hos omnes integros fieri; huic autem theoremati, ad institutum nostrum non adeo necessario, hic non immoramur.

339. Aequatio $x^n - 1 = 0$ (in suppositione semper abhinc subintelligenda, n esse numerum primum imparem) vnicam radicem realem implicat, $x = 1$; $n - 1$ reliquae, quas aequatio $x^{n-1} + x^{n-2} +$ etc. $+ x + 1 = 0$ complectitur, omnes sunt imaginariae; harum complexum per Ω, functionemque $x^{n-1} + x^{n-2} +$ etc. $+ x + 1$ per X denotabimus. Si itaque r est radix quaecunque ex Ω, erit $1 = r^n = r^{2n}$ etc., et generaliter $r^{en} = 1$ pro quouis valore integro ipsius e, positiuo seu negatiuo; hinc perspicuum est, si λ, μ sint integri secundum n congrui, fore $r^\lambda = r^\mu$. Si vero λ, μ sec. mod. n incongrui sunt, r^λ et r^μ inaequales erunt; in hoc enim casu integer ν ita accipi potest vt fiat $(\lambda - \mu)\nu \equiv 1 \pmod{n}$, vnde $r^{(\lambda-\mu)\nu} = r$, adeoque $r^{\lambda-\mu}$ certo non $= 1$. Porro patet, quamuis

potestatem ipsius r etiam radicem aequ. $x^n - 1 = 0$ esse; quocirca quum quantitates $1 (= r^0)$, $r, rr \ldots r^{n-1}$ omnes sint diuersae, hae exhibebunt omnes radices aequ. $x^n - 1 = 0$, et proin hae $r, rr, r^3 \ldots r^{n-1}$ cum Ω coincident. Facile hinc generalius colligitur, Ω conuenire cum r^e, r^{2e}, $r^{3e} \ldots r^{(n-1)e}$, si e sit integer quicunque per n non diuisibilis, positiuus seu negatiuus. Erit itaque $X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$, vnde $r^e + r^{2e} + r^{3e} \ldots + r^{(n-1)e} = -1$, et $1 + r^e + r^{2e} \ldots + r^{(n-1)e} = 0$. Duas radices tales vt r et $\frac{1}{r} (= r^{n-1})$, aut generaliter r^e et r^{-e} *reciprocas* vocabimus; manifestum est, productum ex duobus factoribus simplicibus $x - r$ et $x - \frac{1}{r}$ fieri reale $= xx - 2x \cos \omega + 1$, ita vt angulus ω vel angulo $\frac{P}{n}$ vel alicui multiplo eius sit aequalis.

340. Quoniam itaque, vna radice ex Ω per r expressa, omnes radices aequ. $x^n - 1 = 0$ per potestates ipsius r exprimuntur, productum, e pluribus radicibus huius aequ. quomodocunque conflatum, per r^λ exhiberi poterit, ita vt λ sit vel 0, vel positiuus et $< n$. Designando itaque per $\Phi(t, u, v \ldots)$ functionem algebraicam rationalem integram indeterminatarum t, u, v etc., qualem per summam talium partium $ht^\alpha u^\beta v^\gamma \ldots$ exprimere licet: manifestum est, si pro t, u, v etc. quaedam e radicibus aequ. $x^n - 1 = 0$ substituantur, puta $t = a$, $u = b$, $v = c$ etc., $\Phi(a, b, c \ldots)$ sub formam $A + A'r + A''rr + A'''r^3 \ldots + A^{(n-1)}r^{n-1}$ reduci posse, ita vt coëfficientes A, A' etc. (e quibus etiam aliqui deesse adeo-

que = o fieri possunt) sint quantitates determinatae, insuperque omnes hos coëfficientes integros fieri, si omnes coëfficientes determinati in $\Phi(t, u, v \ldots)$, i. e. omnes h sint integri. Quodsi vero postea pro $t, u, v \ldots$ substituuntur $aa, bb, cc \ldots$ resp., quaeuis pars vt $ht^{\alpha}u^{\beta}v^{\gamma} \ldots$, quae antea reducebatur ad r^{σ}, nunc fiet $r^{2\sigma}$, vnde facile concluditur, fieri $\Phi(aa, bb, cc \ldots) = A + A'rr + A''r^4 + A'''r^6 \ldots + A^{(n)}r^{2n-2}$. Perinde erit generaliter, pro valore quocunque integro ipsius λ, $\Phi(a^{\lambda}, b^{\lambda}, c^{\lambda} \ldots) = A + A'r^{\lambda} + A''r^{2\lambda} \ldots + A^{(n)}r^{(n-1)\lambda}$, quae propositio maximi est momenti, fundamentumque disquisitionum sequentium constituit. — Hinc sequitur etiam $\Phi(1, 1, 1 \ldots) = \Phi(a^n, b^n, c^n \ldots) = A + A' + A'' \ldots + A^{(n)}$; nec non $\Phi(a, b, c \ldots) + \Phi(aa, bb, cc \ldots) + \Phi(a^3, b^3, c^3 \ldots) \ldots + \Phi(a^n, b^n, c^n \ldots) = nA$, quae itaque summa semper fit integer per n diuisibilis, qnando omnes coëfficientes determinati in $\Phi(t, u, v \ldots)$ sunt integri.

341. Theorema. *Si functio X per functionem inferioris gradus $P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} \ldots + Kx + L$ est diuisibilis, coëfficientes $A, B \ldots L$ omnes integri esse nequeunt.*

Dem. Sit $X = PQ$, atque $\mathfrak{P}$ complexus radicum aequationis $\mathfrak{P} = 0$, $\mathfrak{Q}$ complexus radicum aequationis $\mathfrak{Q} = 0$, ita vt Ω constet ex $\mathfrak{P}$ et $\mathfrak{Q}$ simul sumtis. Porro sit $\mathfrak{R}$ complexus radicum ipsis $\mathfrak{P}$ reciprocarum, $\mathfrak{S}$ complexus radicum ipsis $\mathfrak{Q}$ reciprocarum, sintque radices quae continentur in $\mathfrak{R}$ radices aequationis $R = 0$

(quam fieri $x^\lambda + \frac{K}{L} x^{\lambda-1} + \text{etc.} + \frac{A}{L} x + 1 = 0$ facile perspicitur), eaeque quae continentur in $\mathfrak{S}$ radices aequationis $S = 0$. Manifesto etiam radices $\mathfrak{R}$ et $\mathfrak{S}$ iunctae complexum Ω efficient, ac erit $RS = X$. Iam quatuor casus distinguimus.

I. Quando $\mathfrak{P}$ conuenit cum $\mathfrak{R}$ adeoque $P = R$. In hoc casu manifesto binae semper radices in $\mathfrak{P}$ reciprocae erunt, adeoque P productum ex $\frac{1}{2}\lambda$ factoribus talibus duplicibus $xx - 2x \cos \omega + 1$; quum talis factor sit $= (x - \cos \omega)^2 + \sin \omega^2$, facile perspicietur, P pro valore quocunque reali ipsius x necessario valorem realem obtinere. Sint aequationes, quarum radices sunt quadrata, cubi, biquadrata ... potestates $n - 1^{\text{tae}}$ radicum in $\mathfrak{P}$ resp. hae $P' = 0$, $P'' = 0$, $P''' = 0$, ... $P^\nu = 0$, sintque valores functionum P, P', P'' ... P^ν, quos obtinent statuendo $x = 1$, resp. p, p', p'' ... p^ν, tunc per ante dicta p erit quantitas positiua et prorsus simili ratione etiam p', p'' etc. positiuae erunt. Quum itaque p sit valor functionis $(1 - t)(1 - u)(1 - v)$ etc., quem obtinet ponendo pro t, u, v etc. radices in $\mathfrak{P}$; p' valor eiusdem, statuendo pro t, u, v etc. quadrata illarum radicum etc., insuperque valor pro $t = 1$, $u = 1$, $v = 1$ etc. manifesto fiat $= 0$: summa $p + p' + p'' \ldots + p^\nu$ erit integer per n diuisibilis. Praeterea facile perspicietur, productum $PP'P''$ ... fieri $= X^\lambda$, adeoque $pp'p'' \ldots = n^\lambda$.

Iam si omnes coëfficientes in P rationales essent, omnes quoque in P', P'' etc. per art. 338

rationales euaderent; per art. 42 autem cuncti hi coëfficientes necessario forent integri. Hinc etiam p, p', p'' etc. omnes integri forent, quorum productum quum sit n^λ, multitudo vero $n - 1 > \lambda$, necessario quidam ex ipsis (saltem $n - 1 - \lambda$) esse debebunt $= 1$, reliqui vero ipsi n vel potestati ipsius n aequales. Quodsi itaque g ex ipsis sunt $= 1$, summa $p + p' +$ etc. manifesto erit $\equiv g \pmod{n}$ adeoque certo per n non diuisibilis. Quare suppositio consistere nequit.

II. Quando $\mathfrak{P}$ et $\mathfrak{R}$ non quidem coincidunt, attamen quasdem radices communes continent, sit $\mathfrak{T}$ harum complexus atque $T = 0$ aequatio cuius radices sunt. Tunc T erit diuisor communis maximus functionum P, R (vt e theoria aequationum constat). Manifesto autem binae semper radices in $\mathfrak{T}$ reciprocae erunt, vnde per ante demonstrata omnes coëfficientes in T rationales esse nequeunt. Hoc vero certo eueniret, si omnes in P adeoque etiam omnes in R rationales essent, vt e natura operationis, diuisorem comm. max. inuestigandi sponte sequitur. Quare suppositio est absurda.

III. Quando $\mathfrak{Q}$ et $\mathfrak{S}$ vel coincidunt, vel saltem radices communes implicant, prorsus eodem modo omnes coëfficientes in Q rationales esse nequeunt; fierent vero rationales, si omnes in P rationales essent; hoc itaque est impossibile.

IV. Si vero neque $\mathfrak{P}$ cum $\mathfrak{R}$, neque $\mathfrak{Q}$ cum $\mathfrak{S}$ vllam radicem communem habet, omnes

radices $\mathfrak{P}$ necessario reperientur in $\mathfrak{S}$, omnesque $\mathfrak{Q}$ in $\mathfrak{R}$, vnde erit $P = S$ et $Q = R$. Quamobrem $X = PQ$ erit productum ex P in R, i. e. ex $x^\lambda + Ax^{\lambda-1} \ldots + Kx + L$ in $x^\lambda + \frac{K}{L}x^{\lambda-1} \ldots + \frac{A}{L}x + \frac{1}{L}$, vnde statuendo $x = 1$, fit $nL = (1 + A \ldots + K + L)^2$. Iam si omnes coëfficientes in P rationales, adeoque per art. 42 etiam integri essent, L qui coëfficientem vltimum in X i. e vnitatem metiri deberet necessario foret $= \pm 1$, vnde $\pm n$ esset numerus quadratus. Quod quum hypothesi repugnet, suppositio consistere nequit.

Ex hoc itaque theoremate liquet, quomodocunque X in factores resoluatur, horum coëfficientes partim saltem irrationales fieri, adeoque aliter, quam per aequationem eleuatam, determinari non posse.

342. Propositum disquisitionum sequentium, quod paucis declarauisse haud inutile erit, eo tendit, vt X in factores continuo plures GRADATIM resoluatur, et quidem ita, vt horum coëfficientes per aequationes ordinis quam infimi determinentur, vsque dum hoc modo ad factores simplices siue ad radices Ω ipsas peruenia-tur. Scilicet ostendemus, si numerus $n - 1$ quomodocunque in factores integros α, β, γ etc. resoluatur (pro quibus singulis numeros primos accipere licet), X in α factores $\frac{n-1}{\alpha}$ dimensionum resolui posse, quorum coëfficientes per ae-

quationem α^{ti} gradus determinentur; singulos hos factores iterum in $\mathfrak{E}$ alios $\frac{n-1}{\alpha\mathfrak{E}}$ dimensionum adiumento aequationis $\mathfrak{E}^{ti}$ gradus etc., ita vt designante ν multitudinem factorum α, $\mathfrak{E}$, γ etc. inuentio radicum Ω ad resolutionem ν aequationum α^{ti}, $\mathfrak{E}^{ti}$, γ^{ti} etc. gradus reducatur. E. g. pro $n = 17$, vbi $n - 1 = 2.2.2.2$, quatuor aequationes quadraticas soluere oportebit; pro $n = 73$ tres quadraticas duasque cubicas.

Quum in sequentibus persaepe tales potestates radicis r considerandae sint, quarum exponentes rursus sunt dignitates, huiusmodi expressiones autem non sine molestia typis describantur: ad facilitandam impressionem sequenti in posterum abbreuiatione vtemur. Pro r, rr, r^3 etc. scribemus $[1]$, $[2]$, $[3]$ etc., generaliterque pro r^λ, denotante λ integrum quemcunque, $[\lambda]$. Tales itaque expressiones penitus determinatae nondum sunt, sed fiunt, simulac pro r siue $[1]$ radix determinata ex Ω accipitur. Erunt itaque generaliter $[\lambda]$, $[\mu]$ aequales vel inaequales, prout λ, μ secundum modulum n congrui sunt vel incongrui; porro $[0] = 1$; $[\lambda].[\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$; summa $[0] + [\lambda] + [2\lambda] \ldots + [(n-1)\lambda]$ vel 0 vel n, prout λ per n non diuisibilis est vel diuisibilis.

343. Si, pro modulo n, g est numerus talis, qualem in sect. III radicem primitiuam diximus, $n - 1$ numeri $1, g, gg \ldots g^{n-2}$ his $1, 2, 3 \ldots n - 1$ secundum mod. n congrui erunt, etsi alio ordine, puta quiuis numerus vnius seriei

congruum habebit in altera. Hinc sponte sequitur, radices $[1]$, $[g]$, $[gg] \ldots [g^{n-2}]$ cum Ω coincidere; et prorsus simili modo generalius $[\lambda]$, $[\lambda g]$, $[\lambda gg] \ldots [\lambda g^{n-2}]$ cum Ω coincident, designante λ integrum quemcunque per n non diuisibilem. Porro quum sit $g^{n-1} \equiv 1 \pmod{n}$, nullo negotio perspicietur, duas radices $[\lambda g^{\mu}]$, $[\lambda g^{\nu}]$ identicas vel diuersas esse, prout μ, ν secundum $n - 1$ congrui sint vel incongrui.

Si itaque G est alia radix primitiua, radices $[1]$, $[g] \ldots [g^{n-2}]$ etiam cum his $[1]$, $[G] \ldots [G^{n-2}]$ conuenient, si ad ordinem non respicitur. Sed praeterea facile probatur, si e sit diuisor ipsius $n - 1$, atque ponatur $n - 1 = ef$, $g^e = h$, $G^e = H$, etiam f numeros 1, h, hh $\ldots$ $hf-1$ his 1, H, $H^2 \ldots Hf-1$ secundum n congruos esse (sine respectu ordinis). Supponamus enim $G \equiv g^{\omega} \pmod{n}$ sitque μ numerus arbitrarius positiuus et $< f$ atque ν residuum minimum ipsius $\mu\omega \pmod{f}$. Tunc erit $\nu e \equiv \mu\omega e \pmod{n-1}$, hinc $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$, siue $H^{\mu} \equiv h^{\nu}$, i. e. quiuis numerus posterioris seriei 1, H, H^2 etc. congruum habebit in serie 1, h, $hh \ldots$, et perinde vice versa. — Hinc manifestum est, f radices $[1]$, $[h]$, $[hh] \ldots [hf-1]$ identicas esse cum his $[1]$, $[H]$, $[H^2] \ldots [Hf-1]$, generaliusque eodem modo facile perspicietur, $[\lambda]$, $[\lambda h]$, $[\lambda hh] \ldots [\lambda hf-1]$ cum $[\lambda]$, $[\lambda H]$, $[\lambda H^2] \ldots [\lambda Hf-1]$ conuenire. *Aggregatum* talium f radicum $[\lambda] + [\lambda h] +$ etc. $+ [\lambda hf-1]$, quod, quum non mutetur accipiendo pro g aliam radicem primitiuam, tamquam independens a g considerandum est, per (f, λ) designabimus; earun-

dem radicum *complexum* vocabimus *periodum* (f, λ), vbi ad radicum ordinem non respicitur *). — In exhibenda tali periodo e re erit, singulas radices e quibus constat ad expressionem simplicissimam reducere, puta pro numeris λ, λh, λhh etc. residua minima sec. mod. n substituere, secundum quorum magnitudinem, si placet, etiam periodi partes ordinari poterunt.

E. g. Pro $n = 19$, vbi 2 est radix primitiua, periodus (6, 1) constat e radicibus [1], [8], [64], [512], [4096], [32768], siue [1], [7], [8], [11], [12], [18]. Similiter periodus (6, 2) constat ex [2], [3], [5], [14], [16], [17]. Periodus (6, 3) cum praec. identica inuenitur. Periodus (6, 4) continet [4], [6], [9], [10], [13], [15].

344. Circa huiusmodi periodos statim sē offerunt obseruationes sequentes:

I. Quum sit $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$ etc. (mod. n), manifestum est, ex iisdem radicibus, e quibus constet (f, λ), etiam constare $(f, \lambda h)$, $(f, \lambda hh)$ etc.; generaliter itaque designante $[\lambda']$ radicem quamcunque ex (f, λ), haec periodus cum (f, λ') omnino identica erit. Si itaque duae periodi ex aeque multis radicibus constantes (quales *similes* dicemus) vllam radicem communem habent, manifesto identicae erunt. Quare fieri nequit, vt duae radices in aliqua periodo simul contineantur, in alia simili vero vna earum tantum reperiatur; porro patet, si duae radices

*) Aggregatum in sequentibus etiam periodi valorem numericum vocare liceat, aut simpliciter periodum, vbi ambiguitas non metuenda.

$[\lambda]$, $[\lambda']$ ad eandem periodum f terminorum pertineant, valorem expr. $\frac{\lambda'}{\lambda}$ (mod. n) alicui potestati ipsius h congruum esse, siue supponi posse $\lambda' \equiv \lambda g^{re}$ (mod. n).

II. Si $f = n - 1$, $e = 1$, periodus $(f, 1)$ manifesto cum Ω coincidit; in reliquis vero casibus Ω ex e periodis $(f, 1)$, (f, g), (f, gg) $\ldots (f, g^{e-1})$ compositus erit. Hae periodi itaque omnino inter se diuersae erunt, patetque quamuis aliam similem periodum (f, λ) cum harum aliqua coincidere, siquidem $[\lambda]$ ad Ω pertineat, i. e. si λ per n non diuisibilis sit. Periodus $(f, 0)$ autem aut (f, kn) manifesto ex f vnitatibus est composita. Aeque facile perspicitur, si λ sit numerus quicunque per n non diuisibilis, etiam complexum e periodorum (f, λ), $(f, \lambda g)$, $(f, \lambda gg)$ $\ldots (f, \lambda g^{e-1})$ cum Ω conuenire. — Ita e. g. pro $n = 19$, $f = 6$, Ω constat e tribus periodis $(6, 1)$, $(6, 2)$, $(6, 4)$, ad quarum aliquam quaeuis alia similis, praeter $(6, 0)$, reducitur.

III. Si $n - 1$ est productum e tribus numeris positiuis a, b, c, manifestum est, quamuis periodum bc terminorum ex b periodis c terminorum compositam esse, puta (bc, λ) ex (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a})$, $\ldots (c, \lambda g^{ab-a})$, vnde hae sub illa contentae dicentur. Ita pro $n = 19$ periodus $(6, 1)$ constat e tribus $(2, 1)$, $(2, 8)$, $(2, 7)$, quarum prima continet radices r, r^{18}; secunda r^8, r^{11}; tertia r^7, r^{12}.

345. Theorema. *Sint* (f, λ), (f, μ) *duae periodi similes, identicae aut diuersae, constetque* (f, λ) *e radicibus* $[\lambda]$, $[\lambda']$, $[\lambda'']$ *etc.*

Tunc productum ex (f, λ) *in* (f, μ) *erit aggregatum* f *periodorum similium puta* $= (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \text{etc.} = W$.

Dem. Sit vt supra $n - 1 = ef$; g radix primitiua pro modulo n, atque $h = g^e$, vnde per praecedentia erit $(f, \lambda) = (f, \lambda g) = (f, \lambda hh)$ etc. Hinc productum quaesitum erit $= [\mu].(f, \lambda) + [\mu h].(f, \lambda h) + [\mu hh].(f, \lambda hh) + \text{etc.}$ adeoque $=$

$$\begin{array}{l} [\lambda + \mu] \quad + [\lambda h + \mu] \ldots + [\lambda h^{f-1} + \mu] \\ + [\lambda h + \mu h] \; + [\lambda hh + \mu h] \ldots + [\lambda h^{f} + \mu h] \\ + [\lambda hh + \mu hh] + [\lambda h^3 + \mu hh] \ldots + [\lambda h^{f+1} + \mu hh] \\ \qquad \text{etc.} \end{array}$$

quae expressio omnino ff radices continet. Quodsi hic singulae columnae verticales seorsim in summam colliguntur, manifesto prodit $(f, \lambda + \mu) + (f, \lambda h + \mu) \ldots + (f, \lambda h^{f-1} + \mu)$, quam expressionem cum W conuenire nullo negotio perspicitur, quum numeri λ, λ', λ'' etc. per hyp. ipsis $\lambda, \lambda h, \lambda hh \ldots \lambda h^{f-1}$ secundum modulum n congrui esse debeant (quonam ordine hic nihil interest) adeoque etiam $\lambda + \mu$, $\lambda' + \mu$, $\lambda'' + \mu$ etc. ipsis $\lambda + \mu, \lambda h + \mu, \lambda hh + \mu \ldots \lambda h^{f-1} + \mu$. *Q. E. D.*

Huic theoremati adiungimus corollaria sequentia:

I. Designante k integrum quemcunque, productum ex $(f, k\lambda)$ in $(f, k\mu)$ erit $= (f, k(\lambda + \mu)) + (f, k(\lambda' + \mu)) + (f, k(\lambda'' + \mu) + \text{etc.}$

II. Quum singulae partes, e quibus W constat, vel cum aggregato $(f, 0)$, quod est $=$

f, vel cum aliquo ex his $(f, 1)$, (f, g), (f, gg) $\ldots (f, g^{e-1})$ conueniant, W ad formam sequentem reduci poterit $W = af + b(f, 1) + b'(f, g) + b''(f, gg) \ldots + b^{\varepsilon}(f, g^{e-1})$, vbi coëfficientes a, b, b' etc. erunt integri positiui (siue etiam quidam $= 0$): porro patet, productum ex $(f, k\lambda)$ in $(f, k\mu)$ tunc fieri $= af + b(f, k) + b(f, k) + b'(f, kg) \ldots + b^{\varepsilon}(f, kg^{e-1})$. — Ita e. g. pro $n = 19$ productum ex aggregato $(6, 1)$ in se ipsum, siue quadratum huius aggregati fit $= (6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = 6 + 2(6, 1) + (6, 2) + 2(6, 4)$.

III. Quum productum ex singulis partibus ipsius W in periodum similem (f, ν) ad formam analogam reduci possit, manifestum est, etiam productum e tribus periodis $(f, \lambda).(f, \mu).(f, \nu)$ per $cf + d(f, g) \ldots + d^{\varepsilon}(f, g^{e-1})$ exhiberi posse, et coëfficientes c, d etc. integros ac positiuos (siue $= 0$) euadere, insuperque pro valore quocunque integro ipsius k fieri $(f, k\lambda) . (f, k\mu) . (f, k\nu) = cf + d(f, k) + d'(f, kg) +$ etc. Perinde hoc theorema ad producta e periodis similibus quotcunque extenditur, nihilque interest, siue hae periodi omnes diuersae sint, siue partim aut cunctae identicae.

IV. Hinc colligitur, si in functione quacunque algebraica rationali integra $F = \Phi(t, u, v \ldots)$ pro indeterminatis t, u, v etc. resp. substituantur periodi similes (f, λ), (f, μ), (f, ν) etc., eius valorem ad formam $A + B(f, 1) + B'(f, g) + B''(f, gg) \ldots + B^{\varepsilon}(f, g^{e-1})$ reducibilem esse, coëfficientesque A, B, B' etc. omnes

integros fieri, si omnes coëfficientes determinati in F sint integri; si vero postea pro t, u, v etc. resp. substituantur $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$ etc., valorem ipsius F reduci ad $A + B(f, k) + B'(f, kg) +$ etc.

346. Theorema. *Supponendo, λ esse numerum per n non diuisibilem, et scribendo breuitatis ergo p pro (f, ν), quaeuis alia similis periodus (f, μ), vbi etiam μ per n non diuisibilis supponitur, reduci poterit sub formam talem $\alpha + \beta p + \gamma pp \ldots + \theta p^{e-1}$, ita vt coëfficientes α, β etc. sint quantitates determinatae rationales.*

Dem. Designentur ad abbreuiandum periodi $(f, \lambda g)$, $(f, \lambda gg)$, $(f, \lambda g^3)$ etc. vsque ad $(f, \lambda g^{e-1})$, quarum multitudo est $e - 1$, et cum quarum aliqua (f, μ) necessario conueniet, per p', p'', p''' etc. Habetur itaque statim aequatio $0 = 1 + p + p' + p'' + p'''$ etc. ... I); euoluendo autem secundum praecepta art. praec. valores potestatum ipsius p vsque ad $e - 1^{\text{tam}}$, $e - 2$ aliae tales promanabunt:

$$0 = pp + A + ap + a'p' + a''p'' + a'''p''' + \text{etc.} \quad \text{(II)}$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc.} \quad \text{(III)}$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{etc.} \quad \text{(IV)}$$
$$\text{etc.}$$

vbi omnes coëfficientes A, a, a' etc. B, b, b' etc. etc. erunt integri, atque, quod probe notandum est et ex art. praec. sponte sequitur, a λ omnino independentes; i. e. eaedem aequationes etiamnum valebunt, quicunque alius valor ipsi λ tribuatur; haec annotatio manifesto etiam ad aequ. I extenditur, si modo λ per n non diuisibilis accipiatur. — Supponamus $(f, \mu) = p'$; facillime

enim perspicietur, si (f, μ) cum alia periodo ex p'', p''' etc. conueniat, ratiocinia sequentibus prorsus analoga adhiberi posse. Quum multitudo aequationum I, II, III etc. sit $e - 1$, quantitates p'', p''' etc., quarum multitudo $= e - 2$, per methodos notas inde eliminari possunt, ita vt prodeat aequatio talis (Z) ab ipsis libera $0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}pp$ etc. $+ \mathfrak{M}p^{e-1} + \mathfrak{N}p'$, quod ita fieri poterit, vt omnes coëfficientes $\mathfrak{A}$, $\mathfrak{B} \ldots \mathfrak{N}$ sint integri atque certe non omnes $= 0$. Iam si hic non est $\mathfrak{N} = 0$, protinus liquet, p' inde ita vt in theoremate enunciatum est determinari. Superest itaque, vt demonstremus, $\mathfrak{N} = 0$ fieri non posse.

Supponendo esse $\mathfrak{N} = 0$, aequatio Z fit $\mathfrak{M}p^{e-1} + \text{etc.} + \mathfrak{B}p + \mathfrak{A} = 0$, cui, quum vltra gradum $e - 1^{\text{tum}}$ certo non ascendat, plures quam $e - 1$ valores diuersi ipsius p satisfacere nequeunt. At quum aequationes, e quibus Z deducta fuit, a λ sint independentes, liquet, etiam Z a λ non pendere, siue locum habere, quicunque integer per n non diuisibilis pro λ accipiatur. Quare aequ. Z satisfiet, cuicunque ex e aggregatis $(f, 1)$, (f, g), $(f, gg) \ldots (f, g^{e-1})$ aequalis statuatur p, vnde sponte sequitur, haec aggregata omnia inaequalia esse non posse, sed ad minimum duo inter se aequalia esse debere. Contineat vnum e duobus talibus aggregatis aequalibus radices $[\varsigma]$, $[\varsigma']$, $[\varsigma'']$ etc., alterum has $[\eta]$, $[\eta']$, $[\eta'']$ etc., supponamusque (quod licet), omnes numeros ς, ς', ς'' etc., η, η', η'' etc. esse positiuos et $< n$; manifesto omnes etiam diuersi erunt, nullusque $= 0$. Designetur functio $x^{\varsigma} +$

$x^{\xi'} + x^{\xi''}$ + etc. $- x^{\eta} - x^{\eta'} - x^{\eta''}$ — etc., cuius terminus summus non vltra x^{n-1} ascendet, per Y, patetque fieri $Y = 0$ si statuatur $x = [1]$; hinc Y implicabit factorem $x - [1]$, quem cum functione in praec. per X denotata *communem* habebit; hoc vero absurdum esse facile monstrari poterit. Si enim Y cum X vllum factorem communem haberet, diuisor communis *maximus* functionum X, Y (quem certo vsque ad $n - 1$ dimensiones ascendere non posse iam inde patet, quod Y per x est diuisibilis), omnes coëfficientes suos rationales haberet, vt e natura operationum, diuisorem communem maximum duarum talium functionum inuestigandi quarum coëfficientes omnes sunt rationales, sponte sequitur. Sed in art. 341 ostendimus, X implicare non posse factorem pauciorum quam $n - 1$ dimensionum, cuius coëfficientes omnes sint rationales: quamobrem suppositio, esse $\mathfrak{N} = 0$, consistere nequit.

Ex. Pro $n = 19$, $f = 6$, fit $pp = 6 + 2p + p' + 2p''$, vnde et ex $0 = 1 + p + p' + p''$ deducitur $p' = 4 - pp$, $p'' = -5 - p + pp$. Quare $(6, 2) = 4 - (6, 1)^2$, $(6, 4) = -5 - (6, 1) + (6, 1)^2$; $(6, 4) = 4 - (6, 2)^2$, $(6, 1) = -5 - (6, 2) + (6, 2)^2$; $(6, 1) = 4 - (6, 4)^2$, $(6, 2) = -5 - (6, 4) + (6, 4)^2$.

347. Theorema. *Si* $F = \varphi(t, u, v \ldots)$ *est functio inuariabilis**) *algebraica rationalis integra*

*) Functiones inuariabiles eas vocari constat, quibus omnes indeterminatae eodem modo insunt, siue clarius, quae non

f indeterminatarum t, u, v etc., atque substituendo pro his f radices in periodo (f, λ) *contentas valor ipsius F per praecepta art.* 340 *ad formam* $A + A'[1] + A''[2] +$ *etc.* $\equiv W$ *reducitur: radices quae in hac expressione ad eandem periodum quamcunque f terminorum pertinent coëfficientes aequales habebunt.*

Dem. Sint $[p]$, $[q]$ duae radices ad vnam eandemque periodum pertinentes, supponanturque p, q positiui et minores quam n, ita vt demonstrare oporteat, $[p]$ et $[q]$ in W eundem coëfficientem habere. Sit $q \equiv pg'^e \pmod{n}$; sint porro radices in (f, λ) contentae $[\lambda]$, $[\lambda']$, $[\lambda'']$ etc., vbi numeros λ, λ', λ'' etc. positiuos et minores quam n supponimus; denique sint residua minima positiua numerorum $\lambda g'^e$, $\lambda' g'^e$, $\lambda'' g'^e$ etc., secundum modulum n, haec μ, μ', μ'' etc., quae manifesto cum numeris λ, λ', λ'' etc. identici erunt, etsi ordine transposito. Iam ex art. 340 patet, $\Phi(\lambda g'^e, \lambda' g'^e, \lambda'' g'^e \ldots) =$ (I) reduci ad $A + A'[g'^e] + A''[2g'^e] +$ etc. aut ad $A + A'[\theta] + A''[\theta'] +$ etc. $\equiv (W')$, designando per θ, θ' etc. residua minima numerorum g'^e, $2g'^e$ etc. secundum modulum n, vnde manifestum est, $[q]$ habere eundem coëfficientem in (W'), quem $[p]$ habeat in (W). Sed nullo negotio perspicitur, ex euolutione expressionis (I) idem prouenire atque ex euolutione huius $\Phi(\mu, \mu', \mu''$ etc.) quoniam $\mu \equiv \lambda g'^e$, $\mu' \equiv \lambda' g'^e$ etc. (mod. n); haec vero expressio idem producit ac haec $\Phi(\lambda, \lambda', \lambda''$

mutantur, quomodocunque indeterminatae inter se permutentur; cuiusmodi sunt e. g. summa omnium, productum ex omnibus, summa productorum e binis etc.

etc.), quoniam numeri μ, μ', μ'' etc. ordine tantum ab his λ, λ', λ'' etc. discrepant, cuius in functione inuariabili nihil interest. Hinc colligitur, W' omnino identicam fore cum W; quamobrem radix $[q]$ eundem coëfficientem in W habebit vt $[p]$. *Q. E. D.*

Hinc manifestum est, W reduci posse sub formam $A + a(f, 1) + a'(f, g) + a''(f, gg) \ldots + a^{\varepsilon}(f, g^{\varepsilon-1})$, ita vt coëfficientes A, $a \ldots a^{\varepsilon}$ sint quantitates determinatae, quae insuper integri erunt, si omnes coëfficientes rationales in F sunt integri. — Ita e. g. si $n = 19$, $f = 6$, $\lambda = 1$, atque functio φ designat aggregatum productorum e binis indeterminatis, eius valor reducitur ad $3 + (6, 1) + (6, 4)$.

Porro facile perspicietur, si postea pro t, u, v etc. radices ex alia periodo $(f, k\lambda)$ substituantur, valorem ipsius F fieri $A + a(f, k) + a'(f, kg) + a''(f, kgg) +$ etc.

348. Quum in aequatione quacunque $x^f - \alpha x^{f-1} + \mathfrak{G} x^{f-2} - \gamma x^{f-3} \ldots = 0$ coëfficientes α, $\mathfrak{G}$, γ etc. sint functiones inuariabiles radicum, puta α summa omnium, $\mathfrak{G}$ summa productorum e binis, γ summa productorum e ternis etc.: in aequatione cuius radices sunt radices in periodo (f, λ) contentae coëfficiens primus erit $= (f, \lambda)$, singuli reliqui vero sub formam talem $A + a(f, 1) + a'(f, g) \ldots + a^{\varepsilon}(f, g^{\varepsilon-1})$ reduci poterunt, vbi omnes A, a, a' etc. erunt integri; praetereaque patet, aequationem cuius radices sint radices in quacunque alia periodo $(f, k\lambda)$ contentae ex illa

deriuari, si in singulis coëfficientibus pro $(f, 1)$ substituatur (f, k); pro (f, g), (f, kg) et generaliter pro (f, p), (f, kp). Hoc itaque modo assignari poterunt e aequationes $z = 0$, $z' = 0$, $z'' = 0$ etc., quarum radices sint radices contentae in $(f, 1)$, in (f, g), (f, gg) etc., quamprimum e aggregata $(f, 1)$, (f, g), (f, gg) etc. innotuerunt, aut potius quamprimum *vnum* quodcunque eorum inuentum est, quoniam per art. praec. ex vno omnia reliqua rationaliter deducere licet. Quo pacto simul functio X in e factores f dimensionum resoluta habetur: productum enim e functionibus z, z', z'' etc. manifesto erit $= X$.

Ex. Pro $n = 19$ summa omnium radicum in periodo $(6, 1)$ est $= (6, 1) = \alpha$; summa productorum e binis fit $= 3 + (6, 1) + (6, 4) = \mathfrak{G}$; similiter summa productorum e ternis inuenitur $= 2 + 2(6, 1) + (6, 2) = \gamma$; summa productorum e quaternis $= 3 + (6, 1) + (6, 4) = \delta$; summa productorum e quinis $= (6, 1) = \varepsilon$; productum ex omnibus $= 1$; quare aequatio $z = x^6 - \alpha x^5 + \mathfrak{G}x^4 - \gamma x^3 + \delta xx - \varepsilon x + 1 = 0$ omnes radices in $(6, 1)$ contentas complectitur. Quodsi in coëfficientibus α, $\mathfrak{G}$, γ etc. pro $(6, 1)$, $(6, 2)$, $(6, 4)$ resp. substituantur $(6, 2)$, $(6, 4)$, $(6, 1)$, prodibit aequatio $z' = 0$, quae radices in $(6, 2)$ complectetur; et si eadem commutatio hic denuo applicatur, habebitur aequatio $z'' = 0$, radices in $(6, 4)$ complectens, productumque $zz'z''$ erit $= X$.

349. Plerumque commodius est, praesertim quoties f est numerus magnus, coëfficientes

$\mathfrak{G}$, $\mathfrak{H}$ etc. secundum theorema Newtonianum e summis potestatum radicum deducere. Scilicet sponte patet, summam quadratorum radicum in (f, λ) contentarum esse $= (f, 2\lambda)$, summam cuborum $= (f, 3\lambda)$ etc. Scribendo itaque breuitatis caussa pro (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc. q, q', q'' etc. erit $\alpha = q$, $2\mathfrak{E} = \alpha q - q'$, $3\mathfrak{H} = \mathfrak{E}q - \alpha q' + q''$ etc., vbi producta e duabus periodis per art. 345 statim in summas periodorum sunt conuertenda. Ita in exemplo nostro, scribendo pro $(6, 1)$, $(6, 2)$, $(6, 4)$ resp. p, p', p'' fiunt q, q', q'', q''', q^{IV}, q^{V} resp. $= p$, p', p', p'', p', p''; hinc $\alpha = p$, $2\mathfrak{E} = pp - p' = 6 + 2p + 2p''$; $3\mathfrak{H} = (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'$; $4\mathfrak{D} = (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p''$ etc. Ceterum sufficit semissem coëfficientium tantum hoc modo computare; etenim non difficile probatur, vltimos ordine inuerso primis vel aequales esse puta vltimum $= 1$, penultimum $= \alpha$, antepenultimum $= \mathfrak{E}$ etc., vel ex iisdem resp. deduci, si pro $(f, 1)$, (f, g) etc. substituantur $(f, -1)$, $(f, -g)$ etc. siue $(f, n - g)$, $(f, n - 1)$ etc. Casus prior locum habet quando f est par; posterior quando f impar; coëfficiens vltimus autem semper fit $= 1$. Fundamentum huius rei innititur theoremati art. 79; sed breuitatis caussa huic argumento non immoramur.

350. Theorema. *Sit $n - 1$ productum e tribus integris positiuis α, $\mathfrak{E}$, γ; constet periodus $(\mathfrak{H}\gamma, \lambda)$, quae est $\mathfrak{H}\gamma$ terminorum, ex $\mathfrak{E}$ periodis minoribus γ terminorum his (γ, λ), (γ, λ'), (γ, λ'') etc., supponamusque, si in functione $\mathfrak{E}$ indeterminatarum, si-*

militer affecta vt in art. praec., puta in $F = \varphi(t, u, v \ldots)$ *pro indeterminatis* t, u, v *etc. substituantur aggregata* (γ, λ), (γ, λ'), (γ, λ'') *etc. resp., eius valorem per praecepta art. praec. reduci ad* $A + a(\gamma, 1) + a'(\gamma, g) \ldots + a^{\zeta}(\gamma, g^{\alpha\zeta - \alpha}) \ldots + a^{\theta}(\lambda, g^{\alpha\zeta - 1}) = W$. *Tum dico, si* F *sit functio inuariabilis, eas periodos in* W, *quae sub eadem periodo* $\zeta\gamma$ *terminorum contentae sunt, i. e. generaliter tales* (γ, g^{μ}) *et* $(\gamma, g^{\alpha\nu + \mu})$ *designante* ν *integrum quemcunque, coëfficientes eosdem habituras esse.*

Dem. Quum periodus $(\zeta\gamma, \lambda g^{\alpha})$ identica sit cum hac $(\zeta\gamma, \lambda)$, minores hae $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda' g^{\alpha})$, $(\gamma, \lambda'' g^{\alpha})$ etc., e quibus manifesto prior constat, necessario cum iis conuenient e quibus posterior constat, etsi alio ordine. Quodsi itaque, illis pro t, u, v etc. resp. substitutis, F in W' transire supponitur, W' coincidet cum W. At per art. 347 erit $W' = A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{\zeta}(\gamma, g^{\alpha\zeta}) \ldots + a^{\theta}(\gamma, g^{\alpha\zeta + \alpha - 1}) = A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) \ldots + a^{\zeta}(\gamma, 1) \ldots + a^{\beta}(\gamma, g^{\alpha-1})$; quare quum haec expressio cum W conuenire debeat, coëfficiens primus, secundus, tertius etc. in W (incipiendo ab a) necessario conueniet cum $\alpha + 1^{\text{to}}$, $\alpha + 2^{\text{to}}$, $\alpha + 3^{\text{to}}$ etc., vnde nullo negotio concluditur, generaliter coëfficientes periodorum (γ, g^{μ}), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu}) \ldots (\gamma, g^{\nu\alpha+\mu})$, qui sunt $\mu + 1^{\text{tus}}$, $\alpha + \mu + 1^{\text{tus}}$, $2\alpha + \mu + 1^{\text{tus}} \ldots \nu\alpha + \mu + 1^{\text{tus}}$, inter se conuenire debere. *Q. E. D.*

Hinc manifestum est, W reduci posse ad formam $A + a(\zeta\gamma, 1) + a'(\zeta\gamma, g) \ldots + a^{\varepsilon}(\zeta\gamma, g^{\alpha-1})$, vbi omnes coëfficientes A, a etc. integri

erunt, si omnes coëfficientes determinati in F sunt integri. Porro facile perspicietur, si postea pro indeterminatis in F substituantur $\mathfrak{G}$ periodi γ terminorum in alia periodo $\mathfrak{G}\gamma$ terminorum puta in $(\mathfrak{G}\gamma, \lambda k)$ contentae, quae manifesto erunt $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$ etc., valorem inde prodeuntem fore $A + a(\mathfrak{G}\gamma, k) + a'(\mathfrak{G}\gamma, gk) \ldots + a^{(\alpha-1)}(\mathfrak{G}\gamma, g^{\alpha-1}k)$.

Ceterum patet, theorema ad eum quoque casum extendi posse, vbi $\alpha = 1$, siue $\mathfrak{G}\gamma = n - 1$; scilicet hic *omnes* coëfficientes in W aequales erunt, vnde W reducetur sub formam $A + a(\mathfrak{G}\gamma, 1)$.

351. Retentis itaque omnibus signis art. praec., manifestum est, singulos coëfficientes aequationis, cuius radices sunt $\mathfrak{G}$ aggregata (γ, λ), (γ, λ'), (γ, λ'') etc., sub formam talem $A + a(\mathfrak{G}\gamma, 1) + a'(\mathfrak{G}\gamma, g) \ldots + a^{(\alpha-1)}(\mathfrak{G}\gamma, g^{\alpha-1})$ reduci posse, atque numeros A, a etc. omnes fieri integros; aequationem autem, cuius radices sint $\mathfrak{G}$ periodi γ terminorum in alia periodo $(\mathfrak{G}\gamma, k_\lambda)$ contentae, ex illa deriuari, si vbique in coëfficientibus pro qualibet periodo $(\mathfrak{G}\gamma, \mu)$ substituatur $(\mathfrak{G}\gamma, k_\mu)$. Si igitur $\alpha = 1$, omnes $\mathfrak{G}$ periodi γ terminorum determinabuntur per aequationem $\mathfrak{G}^{\text{ti}}$ gradus, cuius singuli coëfficientes sub formam $A + a(\mathfrak{G}\gamma, 1)$ rediguntur, *adeoque sunt quantitates cognitae*, quoniam $(\mathfrak{G}\gamma, 1) = (n - 1, 1) = -1$. Si vero $\alpha > 1$, coëfficientes aequationis, cuius radices sunt omnes periodi γ terminorum in aliqua periodo data $\mathfrak{G}\gamma$ terminorum contentae, quantitates cognitae erunt,

simulac valores numerici omnium α periodorum ζ_γ terminorum innotuerunt. — Ceterum calculus coëfficientium harum aequationum saepe commodius instituitur, praesertim quando ζ non est valde paruus, si primo summae potestatum radicum eruuntur, ac dein ex his per theorema Newtonianum coëfficientes deducuntur, simili modo vt supra art. 349.

Ex. I. Quaeritur pro $n = 19$ aequatio cuius radices sint aggregata $(6, 1)$, $(6, 2)$, $(6, 4)$. Designando has radices per p, p', p'' resp., et aequationem quaesitam per $x^3 - Axx + Bx - C = 0$, fit $A = p + p' + p''$, $B = pp' + pp'' + p'p''$, $C = pp'p''$. Hinc $A = (18, 1) = -1$; porro habetur $pp' = p + 2p' + 3p''$, $pp'' = 2p + 3p' + p''$, $p'p'' = 3p + p' + 2p''$, vnde $B = 6(p + p' + p'') = 6(18, 1) = -6$; denique fit $C = (p + 2p' + 3p'')\, p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$; quare aequatio quaesita $x^3 + xx - 6x - 7 = 0$. — Vtendo methodo altera habemus $p + p' + p'' = -1$; $pp = 6 + 2p + p' + 2p''$, $p'p' = 6 + 2p' + p'' + 2p$, $p''p'' = 6 + 2p'' + p + 2p'$, vnde $pp + p'p' + p''p'' = 18 + 5(p + p' + p'') = 13$; similiterque $p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2$; hinc per theorema Newtonianum eadem aequatio deriuatur vt ante.

II. Quaeritur pro $n = 19$ aequatio cuius radices sint aggregata $(2, 1)$, $(2, 7)$, $(2, 8)$. Quibus resp. per q, q', q'' designatis, inuenitur $q + q' + q'' = (6, 1)$, $qq' + qq'' + q'q'' = (6, 1) + (6, 4)$, $qq'q'' = 2 + (6, 2)$, vnde,

retentis signis ex. praec., aequatio quaesita erit $x^3 - pxx + (p + p'')x - 2 - p' = 0$. — Aequatio cuius radices sunt aggregata (2, 2), (2, 3), (2, 5), sub (6, 2) contenta, e praecedente deducitur, substituendo pro p, p', p'' resp. p', p'', p, eademque substitutione iterum facta, prodit aequatio, cuius radices sunt aggregata (2, 4), (2, 6), (2, 9) sub (6, 4) contenta.

352. Theoremata praecedentia cum consectariis annexis praecipua totius theoriae momenta continent, modusque valores radicum Ω inueniendi paucis iam tradi poterit.

Ante omnia accipiendus est numerus g, qui pro modulo n sit radix primitiua, residuaque minima potestatum ipsius g vsque ad g^{n-2} secundum modulum n eruenda. Resoluatur $n - 1$ in factores, et quidem, si problema ad aequationes gradus quam infimi reducere lubet, in factores primos; sint hi (ordine prorsus arbitrario) α, β, $\gamma \ldots \zeta$, ponaturque $\frac{n-1}{\alpha} = \beta\gamma \ldots \zeta = a$, $\frac{n-1}{\alpha\beta} = \gamma \ldots \zeta = b$ etc. Distribuantur omnes radices Ω in α periodos a terminorum; hae singulae rursus in β periodos b terminorum; hae singulae denuo in γ periodos etc. Quaeratur per art. 350 aequatio α^{ti} gradus (A), cuius radices sint illa α aggregata a terminorum, quorum itaque valores per resolutionem huius aequationis innotescent.

At hic difficultas oritur, quum incertum videatur, cuinam radici aequationis (A) quoduis aggregatum aequale statuendum sit, puta quae-

nam radix per $(a, 1)$, quaenam per (a, g) etc. denotari debeat: huic rei sequenti modo remedium afferri poterit. Per $(a, 1)$ designari potest radix quaecunque aequationis (A); quum enim quaeuis radix huius aequ. sit aggregatum a radicum ex Ω, omninoque arbitrarium sit, quaenam radix ex Ω per $[1]$ denotetur, manifesto supponere licebit, aliquam ex iis radicibus, e quibus radix quaecunque data aequ. (A) constat, per $[1]$ exprimi, vnde illa radix aequ. (A) fiet $(a, 1)$; radix $[1]$ vero hinc nondum penitus determinatur, sed etiamnum prorsus arbitrarium seu indefinitum manet, quamnam radicem ex iis quae $(a, 1)$ constituunt pro $[1]$ adoptare velimus. Simulac vero $(a, 1)$ determinatum est, etiam omnia reliqua aggregata a terminorum rationaliter inde deduci poterunt (art. 346). Hinc simul patet, vnicam tantummodo radicem per huius resolutionem eruere oportere. — Potest etiam methodus sequens, minus directa, ad hunc finem adhiberi. Accipiatur pro $[1]$ radix determinata, i. e. ponatur $[1] = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$, integro k ad lubitum electo, ita tamen vt per n non sit diuisibilis; quo facto etiam $[2]$, $[3]$ etc. radices determinatas indicabunt, vnde etiam aggregata $(a, 1)$, (a, g) etc. quemtitates determinatas designabunt. Quibus e tabulis sinuum leui tantum calamo computatis, puta ea praecisione, vt quae maiore quaeue minora sint decidi possit, nullum dubium superesse poterit, quibusnam signis singulae radices aequ. (A) sint distinguendae.

Quando hoc modo omnia α aggregata a terminorum innenta sunt, inuestigetur per art. 350

aequatio (B) $\mathfrak{e}^{\text{ti}}$ gradus, cuius radices sint $\mathfrak{e}$ aggregata b terminorum sub $(a, 1)$ contenta; coëfficientes huius aequationis omnes erunt quantitates cognitae. Quum adhuc arbitrarium sit, quaenam ex $a = \mathfrak{e}b$ radicibus sub $(a, 1)$ contentis per [1] denotetur, quaelibet radix data aequ. (B) per $(b, 1)$ exprimi poterit, quia manifesto supponere licet, aliquam b radicum e quibus composita est per [1] denotari. Inuestigetur itaque vna radix quaecunque aequationis (B) per eius resolutionem, statuatur $= (b, 1)$, deriuenturque inde per art. 346 omnia reliqua aggregata b terminorum. Hoc modo simul calculi confirmationem nanciscimur, quum semper ea aggregata b terminorum, quae ad easdem periodos a terminorum pertinent, summas notas conficere debeant. — In quibusdam casibus aeque expeditum esse potest, $\alpha - 1$ alias aequationes $\mathfrak{e}^{\text{ti}}$ gradus eruere, quarum radices sint resp. singula $\mathfrak{e}$ aggregata b terminorum in reliquis periodis a terminorum, (a, g), (a, gg) etc. contenta, atque *omnes* radices tum harum aequationum tum aequationis B per resolutionem inuestigare: tunc vero simili modo vt supra adiumento tabulae sinuum decidere oportebit, quibusnam periodis b terminorum singulae radices hoc modo prodeuntes aequales statui debeant. Ceterum ad hocce iudicium varia alia artificia adhiberi possunt, quae hoc loco complete explicare non licet; vnum tamen, pro eo casu vbi $\mathfrak{e} = 2$, quod imprimis vtile est, ac per exempla breuius quam per praecepta declarari poterit, in exemplis sequentibus cognoscere licebit.

Postquam hoc modo valores omnium $\alpha\zeta$ aggregatorum b terminorum inuenti sunt, prorsus simili modo hinc per aequationum γ^{ti} gradus omnia $\alpha\zeta\gamma$ aggregata c terminorum determinari poterunt. Scilicet *vel vnam* aequationem γ^{ti} gradus cuius radices sint γ aggregata c terminorum sub $(b, 1)$ contenta, per art. 350 eruere; per eius resolutionem vnam radicem quamcunque elicere, et $= (c, 1)$ statuere, tandemque hinc per art. 346 omnia reliqua similia aggregata deducere oportebit; *vel* simili modo omnino $\alpha\zeta$ aequationes γ^{ti} gradus euoluere, quarum radices sint resp. γ aggregata c terminorum in singulis periodis b terminorum contenta, valores omnium radicum omnium harum aequationum per resolutionem extrahere, tandemque ordinem harum radicum perinde vt supra adiumento tabulae sinuum, vel, pro $\gamma = 2$, per artificium infra in exemplis ostendendum determinare.

Hoc modo pergendo, manifesto tandem omnia $\frac{n-1}{\zeta}$ aggregata ζ terminorum habebuntur; euoluendo itaque per art. 348 aequationem ζ^{ti} gradus, cuius radices sint ζ radices ex Ω in $(\zeta, 1)$ contentae, huius coëfficientes omnes erunt quantitates cognitae; quodsi per resolutionem vna eius radix quaecunque elicitur, hanc $= [1]$ statuere licebit, omnesque reliquae radices Ω per huius potestates habebuntur. Si magnis placet, etiam *omnes* radices illius aequationis per resolutionem erui, praetereaquae per solutionem $\frac{n-1}{\zeta} - 1$ aliarum aequationum ζ^{ti} gradus, quae resp. omnes ζ radices in singulis reliquis perio-

dis ζ terminorum contentas exhibent, omnes reliquae radices Ω inueniri poterunt.

Ceterum patet, simulac prima aequatio (A) soluta sit, siue simulac valores omnium α aggregatorum a terminorum habeantur, etiam resolutionem functionis X in α factores a dimensionum per art. 348 sponte haberi; porroque post solutionem aequ. (B), siue postquam valores omnium $\alpha\zeta$ aggregatorum b terminorum inuenti sint, singulos illos factores iterum in ζ, siue X in $\alpha\zeta$ factores b dimensionum resolui etc.

353. *Exemplum primum pro* $n = 19$. Quum hic fiat $n - 1 = 3.3.2$, inuentio radicum Ω ad solutionem duarum aequationum cubicarum vniusque quadraticae est reducenda. Hoc exemplum eo facilius intelligetur, quod operationes necessariae ad maximam partem in praecedentibus iam sunt contentae. Accipiendo pro radice primitiua g numerum 2, residua minima eius potestatum haec prodeunt (exponentes potestatum in serie prima residuis sunt suprascripti).

0.1.2.3. 4. 5.6. 7.8. 9.10.11.12.13.14.15.16.17
1.2.4.8.16.13.7.14.9.18.17.15.11. 3. 6.12. 5.10

Hinc per artt. 344, 345 facile deducitur distributio sequens omnium radicum Ω in tres periodos senorum, harumque singularum in ternas binorum terminorum:

$$\Omega = (18,1)\begin{cases}(6,1)\begin{cases}(2,\ 1)\ldots[1],[18]\\(2,\ 8)\ldots[8],[11]\\(2,\ 7)\ldots[7],[12]\end{cases}\\(6,2)\begin{cases}(2,\ 2)\ldots[2],[17]\\(2,16)\ldots[3],[16]\\(2,14)\ldots[5],[14]\end{cases}\\(6,4)\begin{cases}(2,\ 4)\ldots[4],[15]\\(2,13)\ldots[6],[13]\\(2,\ 9)\ldots[9],[10]\end{cases}\end{cases}$$

Aequatio (A), cuius radices sunt aggregata $(6, 1)$, $(6, 2)$, $(6, 4)$, inuenitur $x^3 + xx - 6x - 7 = 0$, cuius vna radix eruitur $= 1{,}2218761623$. Hanc per $(6, 1)$ exprimendo fit $(6, 2) = 4 - (6, 1)^2 = 2{,}5070186441$, $(6, 4) = -5 - (6, 1) + (6, 1)^2 = -2{,}2851424818$. Hinc X in tres factores 6 dimensionum resoluta erit, si hi valores in art. 348 substituuntur.

Aequatio (B), cuius radices sunt aggregata $(2, 1)$, $(2, 7)$, $(2, 8)$, prodit haec $x^3 - (6, 1)\,xx + ((6, 1) + (6, 4))\,x - 2 - (6, 2) = 0$ siue

$$x^3 + 1{,}2218761623xx - 3{,}5070186441x - 4{,}5070186441 = 0$$

cuius vna radix elicitur $= -1{,}3545631433$, quam per $(2, 1)$ exprimemus. Per methodum art. 346 autem inueniuntur aequationes sequentes, vbi breuitatis caussa q pro $(2, 1)$ scribitur: $(2, 2) = qq - 2$, $(2, 3) = q^3 - 3q$, $(2, 4) = q^4 - 4qq + 2$, $(2, 5) = q^5 - 5q^3 + 5q$, $(2, 6) =$

$q^6 - 6q^4 + 9qq - 2$, $(2, 7) = q^7 - 7q^5 + 14q^3 - 7q$, $(2, 8) = q^8 - 8q^6 + 20q^4 - 16qq + 2$, $(2, 9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q$. Commodius quam per praecepta art. 346 hae aequationes in casu praesenti per reflexiones sequentes euolui possunt. Supponendo $[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$, fit $[18] = \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} = \cos\frac{kP}{19} - i\sin\frac{kP}{19}$, adeoque $(2, 1) = 2\cos\frac{kP}{19}$; nec non generaliter $[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19}$, adeoque $(2, \lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$. Quare si $\frac{1}{2}q = \cos\omega$, erit $(2, 2) = 2\cos 2\omega$, $(2, 3) = 2\cos 3\omega$ etc., vnde per aequationes notas pro cosinubus angulorum multiplicium eaedem formulae vt supra deriuantur. — Iam ex his formulis valores numerici sequentes eliciuntur:

$(2,2) = -0{,}1651586909$	$(2,6) = 0{,}4909709743$
$(2,3) = 1{,}5782810188$	$(2,7) = -1{,}7589475024$
$(2,4) = -1{,}9727226068$	$(2,8) = 1{,}8916344834$
$(2,5) = 1{,}0938963162$	$(2,9) = -0{,}8033908493$

Valores ipsorum $(2, 7)$, $(2, 8)$ etiam ex aequatione (B), cuius duae reliquae radices sunt, elici possunt, dubiumque, *vtra* harum radicum fiat $(2, 7)$ et vtra $(2, 8)$, vel per calculum approximatum secundum formulas praecc., vel per tabulas sinuum tolletur, quae obiter tantum consultae ostendunt, fieri $(2, 1) = 2\cos\omega$ po-

nendo $\omega = \frac{7}{19}P$, vnde fieri oportet $(2, 7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P$, et $(2, 8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$. — Similiter aggregata $(2, 2)$, $(2, 3)$, $(2, 5)$ etiam per aequationem $x^3 - (6, 2)xx + ((6, 1) + (6, 2))x - 2 - (6, 4) = 0$, cuius radices sunt, inuenire licet, incertitudoque, quaenam radices illis aggregatis *resp.* aequales statuendae sint, prorsus eodem modo remouebitur, vt ante; et perinde etiam aggregata $(2, 4)$, $(2, 6)$, $(2, 9)$ per aequationem $x^3 - (6, 4)xx + ((6, 2) + (6, 4))x - 2 - (6, 1) = 0$ elici poterunt.

Denique [1] et [18] sunt radices aequationis $xx - (2, 1)x + 1 = 0$, quarum altera fit $= \frac{1}{2}(2, 1) + i\sqrt{(1 - \frac{1}{4}(2, 1)^2)} = \frac{1}{2}(2, 1) + i\sqrt{(\frac{1}{2} - \frac{1}{4}(2, 2))}$, altera $= \frac{1}{2}(2, 1) - i\sqrt{(\frac{1}{2} - \frac{1}{4}(2, 2))}$, hinc valores numerici $= -0{,}6772815716 \pm 0{,}7357239107i$. Sedecim radices reliquae vel ex euolutione potestatum vtriusuis harum radicum, vel e solutione octo aliarum similium aequationum deduci possunt, vbi in methodo posteriori vel per tabulas sinuum vel per artificium in ex. sq. explicandum decidi debebit, pro vtra radice parti imaginariae signum positiuum et pro vtra negatiuum praefigendum sit. Hoc modo inuenti sunt valores sequentes, vbi signum superius radici priori, inferius posteriori respondere supponitur.

$$[1] \text{ et } [18] = -0{,}6772815716 \pm 0{,}7357239107i$$
$$[2] \text{ et } [17] = -0{,}0825793455 \mp 0{,}9965844930i$$
$$[3] \text{ et } [16] = \;\;0{,}7891405094 \pm 0{,}6142127127i$$
$$[4] \text{ et } [15] = -0{,}9863613034 \pm 0{,}1645945903i$$
$$[5] \text{ et } [14] = \;\;0{,}5469481581 \mp 0{,}8371664783i$$
$$[6] \text{ et } [13] = \;\;0{,}2454854871 \pm 0{,}9694002659i$$
$$[7] \text{ et } [12] = -0{,}8794737512 \mp 0{,}4759473930i$$
$$[8] \text{ et } [11] = \;\;0{,}9458172417 \mp 0{,}3246994692i$$
$$[9] \text{ et } [10] = -0{,}4016954247 \pm 0{,}9157733267i$$

354. *Exemplum secundum pro* $n = 17$. Hic habetur $n - 1 = 2.2.2.2$, quamobrem calculus radicum Ω ad quatuor aequationes quadraticas reducendus erit. Pro radice primitiua hic accipiemus numerum 3, cuius potestates residua minima sequentia secundum modulum 17 suppeditant:

0.1.2. 3. 4.5. 6. 7. 8. 9.10.11.12.13.14.15
1.3.9.10.13.5.15.11.16.14. 8. 7. 4.12. 2. 6

Hinc emergunt distributiones sequentes complexus Ω in periodos duas octonorum, quatuor quaternorum, octo binorum terminorum:

$$\Omega = (16,1)\begin{cases}(8,1)\begin{cases}(4,1)\begin{pmatrix}(2,1)\ldots[1],[16]\\(2,13)\ldots[4],[13]\end{pmatrix}\\(4,9)\begin{pmatrix}(2,9)\ldots[8],[9]\\(2,15)\ldots[2],[15]\end{pmatrix}\end{cases}\\(8,3)\begin{cases}(4,3)\begin{pmatrix}(2,3)\ldots[3],[14]\\(2,5)\ldots[5],[12]\end{pmatrix}\\(4,10)\begin{pmatrix}(2,10)\ldots[7],[10]\\(2,11)\ldots[6],[11]\end{pmatrix}\end{cases}\end{cases}$$

Aequatio (A), cuius radices sunt aggregata $(8, 1)$, $(8, 3)$, per praecepta art. 351 inuenitur haec $xx + x - 4 = 0$; huius radices computantur $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}561552812\,8$, et $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}561552812\,8$; priorem statuemus $= (8, 1)$, vnde necessario posterior ponenda erit $= (8, 3)$.

Porro aequatio, cuius radices sunt aggregata $(4, 1)$ et $(4, 9)$, eruitur haec (B): $xx - (8, 1)x - 1 = 0$; huius radices sunt $\frac{1}{2}(8, 1) \pm \frac{1}{2}\sqrt{(4 + (8, 1)^2)} = \frac{1}{2}(8, 1) \pm \frac{1}{2}\sqrt{(12 + 3(8, 1) + 4(8, 3))}$; eam in qua quantitati radicali signum positiuum tribuitur, et cuius valor numericus est $2{,}049481\,1777$, statuemus $= (4, 1)$, vnde sponte altera, vbi quantitas radicalis negatiue sumitur et cuius valor est $-0{,}487928\,3649$, per $(4, 9)$ exprimi debebit. Aggregata autem reliqua quatuor terminorum, puta $(4, 3)$ et $(4, 10)$ duplici modo indagari possunt. Scilicet *primo* per methodum art. 346, quae formulas sequentes suppeditat, vbi ad abbreuiandum pro $(4, 1)$ scribitur p:

$$(4, 3) = -\tfrac{3}{2} + 3p - \tfrac{1}{2}p^3 = 0{,}344\,150\,7314$$
$$(4, 10) = \tfrac{3}{2} + 2p - pp - \tfrac{1}{2}p^3 = -2{,}905\,703\,5442$$

Eadem methodus etiam hanc formulam largitur $(4, 9) = -1 - 6p + pp + p^3$, vnde valor idem elicitur quem ante tradidimus. *Secundo* vero aggregata $(4, 3)$, $(4, 10)$ etiam per resolutionem aequationis cuius radices sunt determinare licet, quae aequatio fit $xx - (8, 3)x - 1 = 0$, vnde eius radices sunt $\frac{1}{2}(8, 3)$

$\pm \frac{1}{2}\sqrt{(4 + (8,3)^2)}$, siue $\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{(12 + 4(8,1) + 3(8,3))}$ et $\frac{1}{2}(8,3) - \frac{1}{2}\sqrt{(12 + 4(8,1) + 3(8,3))}$; dubium vero, *vtram* radicem per $(4,3)$ et vtram per $(4,10)$ exprimere oporteat, per artificium sequens cuius mentionem in art. 352 iniecimus tolletur. Euoluatur productum ex $(4,1) - (4,9)$ in $(4,3) - (4,10)$, vnde emergere inuenietur $2(8,1) - 2(8,3)$*); iam huius expressionis valor manifesto est positiuus puta $= +2\sqrt{17}$, praetereaque etiam producti factor primus $(4,1) - (4,9)$ positiuus est puta $= +\sqrt{(12 + 3(8,1) + 4(8,3))}$, quare necessario etiam alter factor $(4,3) - (4,10)$ positiuus esse debebit, et proin $(4,3)$ radici *priori* in qua signum positiuum radicali praefigitur, et $(4,10)$ posteriori aequale statui. Ceterum hinc iidem valores numerici deriuantur vt supra.

Cunctis aggragatis quatuor terminorum inuentis progredimur ad aggregata duorum terminorum. Aequatio (C), cuius radices sunt haec $(2,1)$, $(2,13)$, sub $(4,1)$ contenta, eruitur haec $xx - (4,1)x + (4,3) = 0$; huius radices sunt $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(-4(4,3) + (4,1)^2)}$ siue $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(4 + (4,9) - 2(4,3))}$; eam vbi quantitas radicalis positiue sumitur et cuius valor reperitur $= 1{,}86499444588$, statuimus $= (2,1)$,

*) Vera indoles huius artificii in eo consistit, quod a priori praeuideri poterat, hocce productum euolutum aggregata quatuor terminorum non continere sed per sola aggregata octo terminorum exhiberi posse, cuius rei rationem hic breuitatis caussa praetereundam periti facillime deprehendent.

vnde $(2, 13)$ aequale fiet alteri, cuius valor $=$ 0,1845367189. — Si aggregata reliqua duorum terminorum per methodum art. 346 inuestigare placet, pro $(2, 2)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 6)$, $(2, 7)$, $(2, 8)$ eaedem formulae adhiberi poterunt, quae in ex. praec. pro quantitatibus similiter disignatis tradidimus, puta $(2, 2)$, (siue $(2, 15)$), $= (2, 1)^2 - 2$ etc. Si vero magis arridet, binas per resolutionem aequationis quadraticae computare, pro his $(2, 9)$, $(2, 15)$ inuenitur aequatio $xx - (4, 9)x + (4, 10) = 0$, cuius radices euoluuntur $\frac{1}{2}(4, 9) \pm \frac{1}{2}\sqrt{(4 + (4, 13))}$; quo pacto vero signum ambiguum hic definire oporteat, simili modo decidetur vt supra. Scilicet per euolutionem producti $(2, 1) - (2, 13)$ in $(2, 9) - (2, 15)$ producitur $- (4, 1) + (4, 9) - (4, 3) + (4, 10)$; quod quum manifesto sit negatiuum, factor $(2, 1) - (2, 13)$ vero positiuus, necessario $(2, 9) - (2, 15)$ negatiuus esse debebit, quocirca in expressione ante data signum superius positiuum pro $(2, 15)$, pro $(2, 9)$ inferius negatiuum adoptandum erit. Hinc computatur $(2, 9) = -1,9659461994$, $(2, 15) = 1,4780178344$. — Perinde quum ex euolutione producti ex $(2, 1) - (2, 13)$ in $(2, 3) - (2, 5)$ prodeat $(4, 9) - (4, 10)$, adeoque quantitas positiua, factorem $(2, 3) - (2, 5)$ positiuum esse concludimus; hinc simili calculo vt ante instituto inuenitur

$$(2, 3) = \tfrac{1}{2}(4, 3) + \tfrac{1}{2}\sqrt{(4 + (4, 10) - 2(4, 9))} = 0,8914767116$$

$$(2, 5) = \tfrac{1}{2}(4, 3) - \tfrac{1}{2}\sqrt{(4 + (4, 10) - 2(4, 9))} = -0,5473259801$$

Denique per operationes omnino analogas eruitur

$$(2, 10) = \tfrac{1}{2}(4, 10) - \tfrac{1}{2}\sqrt{(4 + (4, 3) - 2(4, 1))}$$
$$= -1{,}7004342715$$
$$(2, 11) = \tfrac{1}{2}(4, 10) + \tfrac{1}{2}\sqrt{(4 + (4, 3) - 2(4, 1))}$$
$$= -1{,}2052692728$$

Superest vt ad radices Ω ipsas descendamus. Aequatio (D) cuius radices sunt [1] et [16] prodit $xx - (2, 1)\, x + 1 = 0$, vnde radices $\tfrac{1}{2}(2, 1) \pm \tfrac{1}{2}\sqrt{((2, 1)^2 - 4)}$ aut potius $\tfrac{1}{2}\sqrt{(2, 1)} \pm i\sqrt{(4 - (2, 1)^2)}$ siue $\tfrac{1}{2}(2, 1) \pm \tfrac{1}{2}i\sqrt{(2 - (2, 15))}$; signum superius pro [1], inferius pro [16] adoptamus. Quatuordecim reliquae radices vel per potestates ipsius [1] habebuntur; vel per resolutionem septem aequationum quadraticarum, quae singulae binas exhibent, vbi incertitudo de signis quantitatum radicalium per idem artificium tolli poterit vt in praecedentibus. Ita [4] et [13] sunt radices aequationis $xx - (2, 13)\, x + 1 = 0$, adeoque $\tfrac{1}{2}(2, 13) \pm \tfrac{1}{2}i\sqrt{(2 - (2, 9))}$; per euolutionem producti ex [1] — [16] in [4] — [13] autem prodit $(2, 5) - (2, 3)$, adeoque quantitas realis negatiua, quare quum [1] — [16] sit $+ i\sqrt{(2 - (2, 15))}$, i. e. productum ex imaginaria i in realem *positiuam*, etiam [4] — [13] esse debet productum ex i in realem *positiuam* propter $ii = -1$; hinc colligitur, pro [4] signum superius, pro [13] inferius accipiendum esse. Simili modo pro radicibus [8] et [9] inuenitur $\tfrac{1}{2}(2, 9) \pm \tfrac{1}{2}i\sqrt{(2 - (2, 1))}$, vbi, quoniam productum ex [1] — [16] in [8] — [9] fit $(2, 9) - (2, 10)$ adeoque negatiuum,

pro [8] signum superius, pro [9] inferius accipere oportet. Computando perinde radices reliquas, sequentes valores numericos obtinemus, vbi radicibus prioribus signa superiora, posterioribus inferiora respondere subintelligendum est:

$$
\begin{array}{ll}
[1], [16] \ldots & 0{,}9324722294 \pm 0{,}3612516662i \\
[2], [15] \ldots & 0{,}7390089172 \pm 0{,}6736956436i \\
[3], [14] \ldots & 0{,}4457383558 \pm 0{,}8951632914i \\
[4], [13] \ldots & 0{,}0922683595 \pm 0{,}9957341763i \\
[5], [12] \ldots & -0{,}2736629901 \pm 0{,}9618256432i \\
[6], [11] \ldots & -0{,}6026346364 \pm 0{,}7980172273i \\
[7], [10] \ldots & -0{,}8502171357 \pm 0{,}5264321629i \\
[8], [\ 9] \ldots & -0{,}9829730997 \pm 0{,}1837495178i
\end{array}
$$

* * *

Possent quidem ea quae in praecc. sunt tradita ad solutionem aequationis $x^n - 1 = 0$ adeoque etiam ad inuentionem functionum trigonometricarum arcubus cum peripheria commensurabilibus respondentium sufficere: attamen, propter rei grauitatem, finem huic disquisitioni imponere non possumus, quin antea ex magna copia quum obseruationum hoc argumentum illustrantium tum positionum ei affinium vel inde pendentium quaedam hic annectamus. Inter quae talia potissimum eligemus, quae sine magno aliarum disquisitionum apparatu absolue-re licet, aliterque ea considerari nolimus quam vt *specimina* huius amplissimae doctrinae, in posterum copiose pertractandae.

355. Quum n semper supponatur impar, erit 2 inter factores ipsius $n - 1$, complexusque Ω ex $\frac{1}{2}(n-1)$ periodis duorum terminorum formatus. Talis periodus, vt $(2, \lambda)$, e radicibus $[\lambda]$ et $[\lambda g^{\frac{1}{2}(n-1)}]$ constabit, denotante g vt supra radicem primitiuam quamcunque pro modulo n. Sed fit $g^{\frac{1}{2}(n-1)} \equiv -1 \pmod{n}$ adeoque $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (V. art. 62), vnde $[\lambda g^{\frac{1}{2}(n-1)}] \equiv [-\lambda]$. Quare supponendo $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, et proin $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, fit aggregatum $(2, \lambda) = 2\cos\frac{kP}{n}$. Vnde hoc loco hanc tantummodo conclusionem deducimus, valorem cuiusuis aggregati duorum terminorum esse quantitatem realem. Quum quaeuis periodus, cuius terminorum multitudo par $= 2a$, in a periodos binorum terminorum discerpi possit, patet generalius, valorem cuiusuis aggregati cuius terminorum multitudo par semper esse quantitatem realem. Quodsi itaque in art. 352 inter factores α, β, γ etc. binarius ad vltimum locum reseruatur, omnes operationes vsquedum ad aggregata duorum terminorum perueniatur per quantitates reales absoluentur, imaginariaeque tunc demum introducentur, quando ab his aggregatis ad radices ipsas progredieris.

356. Summam attentionem merentur aequationes auxiliares, per quas pro quolibet valore ipsius n aggregata complexum Ω constituentia determinantur, quae mirum in modum cum proprietatibus maxime reconditis numeri n

connexae sunt. Hoc vero loco disquisitionem ad duos casus sequentes restringemus: *primo* de aequatione quadratica cuius radices sunt aggregata $\frac{1}{2}(n-1)$ terminorum, *secundo*, pro eo casu vbi $n-1$ factorem 3 implicat, de cubica cuius radices sunt aggregata $\frac{1}{3}(n-1)$ terminorum agemus.

Scribendo breuitatis caussa m pro $\frac{1}{2}(n-1)$ et designando per g radicem primitiuam quamcunque pro modulo n, complexus Ω e duabus periodis $(m, 1)$ et (m, g) constabit, continebitque prior radices $[1]$, $[gg]$, $[g^4] \ldots [g^{n-3}]$, posterior has $[g]$, $[g^3]$, $[g^5] \ldots [g^{n-2}]$. Supponendo residua minima positiua numerorum gg, $g^4 \ldots g^{n-3}$ secundum modulum n esse, ordine arbitrario, R, R', R'' etc.; nec non residua horum g, g^3, $g^5 \ldots g^{n-2}$ haec N, N', N'' etc., radices e quibus $(m, 1)$ constat conuenient cum his $[1]$, $[R]$, $[R']$, $[R'']$ etc., radicesque periodi (m, g) cum his $[N]$, $[N']$, $[N'']$ etc. Iam patet, omnes numeros 1, R, R', R'' etc. esse *residua quadratica* numeri n, et quum omnes diuersi ipsoque n minores sint ipsorumque multitudo $= \frac{1}{2}(n-1)$ adeoque multitudini cunctorum residuorum positiuorum ipsius n infra n aequalis, haec residua cum illis numeris omnino conuenient. Hinc sponte sequitur, omnes numeros N, N', N'' etc., qui tum inter se tum ab ipsis 1, R, R' etc. diuersi sunt, et cum his simul sumti omnes numeros $1, 2, 3 \ldots n-1$ exhauriunt, cum omnibus non residuis quadraticis positiuis ipsius n infra n conuenire debere. Quodsi iam supponitur, aequationem cuius ra-

dices sunt aggregata $(m, 1)$, (m, g) esse $xx - Ax + B = 0$, fit $A = (m + 1) + (m, g) = -1$, $B = (m, 1) \times (m, g)$. Productum ex $(m, 1)$, in (m, g) per art. 345 fit $= (m, N + 1) + (m, N' + 1) + (m, N'' + 1) +$ etc. $= W$, atque hinc reducetur sub formam talem $\alpha(m, 0) + \mathfrak{G}(m, 1) + \gamma(m, g)$. Ad determinationem coëfficientium α, $\mathfrak{G}$, γ obseruamus, *primo*, fieri $\alpha + \mathfrak{G} + \gamma = m$ (scilicet quoniam multitudo aggregatorum in W est $= m$); *secundo*, esse $\mathfrak{G} = \gamma$ (hoc sequitur ex art. 350 quum productum $(m, 1) \times (m, g)$ sit functio inuariabilis aggregatorum $(m, 1)$, (m, g), e quibus aggregatum maius $(n - 1, 1)$ compositum est); *tertio*, quum omnes numeri $N + 1$, $N' + 1$, $N'' + 1$ etc. infra limites 2 et $n + 1$ excl. contineantur, manifestum est, *vel* nullum aggregatum in W ad $(n, 0)$ reduci adeoque esse $\alpha = 0$, quando inter numeros N, N', N'' etc. non occurrat $n - 1$, *vel* vnum puta (m, n), et proin haberi $\alpha = 1$, quando $n - 1$ inter numeros N, N', N'' etc. reperiatur. Hinc colligitur, in casu priori fieri $\alpha = 0$, $\mathfrak{G} = \gamma = \frac{1}{2}m$, in posteriori $\alpha = 1$, $\mathfrak{G} = \gamma = \frac{1}{2}(m - 1)$, simul hinc sequitur, quum numeri $\mathfrak{G}$ et γ necessario fiant integri, casum priorem locum habere, siue $n - 1$ (aut quod idem est -1) inter non residua ipsius n non reperiri, quando m sit par siue n formae $4k + 1$; casum posteriorem vero adesse, siue $n - 1$ aut -1 inter non residua ipsius n reperiri, quoties m sit impar siue n formae $4k + 3$ *). Hinc productum

*) Hoc modo nacti sumus demonstrationem nouam theorematis, — 1 esse residuum omnium numerorum primorum

quaesitum fit, propter $(m, 0) = m$, $(m, 1) + (m, g) = -1$, in casu priori $= -\frac{1}{2}m$, in posteriori $= \frac{1}{2}(m + 1)$, adeoque aequatio quaesita in illo casu $xx + x - \frac{1}{4}(n - 1) = 0$, cuius radices sunt $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$, in hoc vero $xx + x + \frac{1}{4}(n + 1) = 0$, cuius radices $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$.

Quaecunque itaque radix ex Ω pro [1] adoptata est, differentia inter summas $\Sigma[\mathfrak{R}]$ et $\Sigma[\mathfrak{N}]$, vbi pro $\mathfrak{R}$ omnia residua pro $\mathfrak{N}$ omnia non residua quadratica positiua ipsius n infra n substituenda sunt, erit $= \pm\sqrt{n}$, pro $n \equiv 1$, et $= \pm i\sqrt{n}$, pro $n \equiv 3 \pmod 4$. Nec non hinc facile sequitur, denotante k integrum quemcunque per n non diuisibilem, fieri $\Sigma \cos \frac{k\mathfrak{R}P}{n} - \Sigma \cos \frac{k\mathfrak{N}P}{n} = \pm\sqrt{n}$ et $\Sigma \sin \frac{k\mathfrak{R}P}{n} - \Sigma \sin \frac{k\mathfrak{N}P}{n} = 0$ pro $n \equiv 1 \pmod 4$; contra pro $n \equiv 3 \pmod 4$ differentiam illam $= 0$, hanc $= \pm\sqrt{n}$, quae theoremata propter elegantiam suam valde sunt memorabilia. Ceterum obseruamus, signa superiora semper valere quando pro k accipiatur vnitas aut generalius residuum quadraticum ipsius n, inferiora quando pro k non residuum assumatur, nec non haecce theoremata salua vel potius aucta elegantia sua

formae $4k + 1$, non residuum omnium formae $4k + 3$, quod supra (art. 108, 109, 262) iam pluribus modis diuersis comprobatum fuit. Si magis arridet, hoc theorema supponere, non necessarium erit ad distinctionem duorum casum diuersorum eius conditionis rationem habere, quod 6, γ iam per se fiunt integri.

etiam ad valores quosuis compositos ipsius n extendi posse: sed de his rebus quae altioris sunt indaginis hoc loco tacere earumque considerationem ad aliam occasionem nobis reseruare oportet.

357. Sit aequatio m^{ti} gradus, cuius radices sunt m radices in periodo $(m, 1)$ contentae haec $x^m - ax^{m-1} + bx^{m-2} -$ etc. $= 0$ siue $z = 0$, eritque $a = (m, 1)$, singulique reliqui coëfficientes b etc. sub forma tali $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ comprehensi, ita vt $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ sint integri (art. 348); denotandoque per z' functionem, in quam z transit, si pro $(m, 1)$ vbique substituitur (m, g), pro (m, g) vero (m, gg) siue quod idem est $(m, 1)$, radices aequationis $z' = 0$ erunt radices in (m, g) contentae, productumque $zz' = \frac{x^n - 1}{x - 1} = X$. Potest itaque z ad formam talem $R + S(m, 1) + T(m, g)$ reduci, vbi R, S, T erunt functiones integrae ipsius x, quarum omnes coëfficientes etiam integri erunt; quo facto habebitur $z' = R + S(m, g) + T(m, 1)$. Hinc fit scribendo breuitatis caussa p et q pro $(m, 1)$ et (m, g) resp., $2z = 2R + (S + T)(p + q) - (T - S)(p - q) = 2R - S - T - (T - S)(p - q)$ similiterque $2z' = 2R - S - T + (T - S)(p - q)$, vnde ponendo $2R - S - T = Y$, $T - S = Z$, fit $4X = YY - (p - q)^2 ZZ$, adeoque quum $(p - q)^2 = \pm n$, $4X = YY \mp nZZ$, signo superiori valente quando n est formae $4k + 1$, inferiori quando n formae $4k + 3$. Hoc est theorema, cuius demonstrationem supra (art. 124) polliciti sumus. Terminos duos summos functionis Y semper fieri

$2x^m + x^{m-1}$; summumque functionis Z, x^{m-1} facile perspicietur; coëfficientes reliqui autem, qui manifesto omnes erunt integri, variant pro diuersa indole numeri n, nec formulae analyticae generali subiici possunt.

Ex. Pro $n = 17$ aequatio cuius radices sunt octo adices in $(8, 1)$ contentae per praecepta art. 348 eruitur $x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 - (4p + 3q)x^3 + (4 + p + 2q)xx - px + 1 = 0$, vnde $R = x^8 + 4x^5 + 6x^4 + 4xx + 1$, $S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$, $T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$, atque hinc $Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5xx + x + 2$, $Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + xx + x$. Ecce adhuc alia quaedam exempla:

n	Y	Z
3	$2x + 1$	1
5	$2xx + x + 2$	x
7	$2x^3 + xx - x - 2$	$xx + x$
11	$2x^5 + x^4 - 2x^3 + 2xx - x - 2$	$x^4 + x$
13	$2x^6 + x^5 - 4x^4 - x^3 - 4xx + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4xx - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5xx - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + xx + x$

358. Progredimus ad considerationem aequationum cubicarum, per quas in eo casu vbi n est formae $3k + 1$ tria aggregata $\frac{1}{3}(n - 1)$ terminorum complexum Ω componentia determinantur. Sit g radix primitiua quaecunque pro modulo n, atque $\frac{1}{3}(n - 1) = m$, qui erit integer par. Tunc tria aggregata e quibus Ω constat erunt $(m, 1)$, (m, g), (m, gg) pro quibus resp. scribemus p, p', p'', patet que primum continere radices $[1]$, $[g^3]$, $[g^6]$ $\ldots$ $[g^{n-4}]$, secundum has $[g]$, $[g^4]$ $\ldots$ $[g^{n-3}]$, tertium has $[gg]$, $[g^5]$ $\ldots$ $[g^{n-2}]$. Supponendo, aequationem quaesitam esse $x^3 - Axx + Bx - C = 0$, fit $A = p + p' + p''$, $B = pp' + p'p'' + pp''$, $C = pp'p''$, vnde protinus habetur $A = -1$. Sint residua minima positiua numerorum g^3, $g^6 \ldots g^{n-3}$ secundum modulum n ordine arbitrario haec $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc., atque $\mathfrak{K}$ ipsorum complexus superadiecto numero 1; similiter sint $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ etc. residua minima numerorum g, g^4, g^7 $\ldots$ g^{n-3}, atque $\mathfrak{K}'$ illorum complexus; denique $\mathfrak{A}''$, $\mathfrak{B}''$, $\mathfrak{C}''$ etc. residua minima ipsorum gg, g^5, g^8 $\ldots$ g^{n-2} et $\mathfrak{K}''$ eorum complexus, vnde omnes numeri in $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ diuersi erunt et cum his $1, 2, 3 \ldots n - 1$ conuenient. Ante omnia hic obseruandum est, numerum $n - 1$ necessario in $\mathfrak{K}$ reperiri, quippe quem esse residuum ipsius $g^{\frac{3}{2}m}$ facile perspicitur. Hinc facile quoque consequitur, duos numeros tales h, $n - h$ semper in *eodem* trium complexuum $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ reperiri, si enim alter est residuum potestatis g^λ, alter erit residuum potestatis $g^{\lambda + \frac{3}{2}m}$, aut huius $g^{\lambda - \frac{3}{2}m}$ si $\lambda > \frac{3}{2}m$. Denotemus hocce signo $(\mathfrak{K}\mathfrak{K})$ multitudinem nume-

rorum in seriei 1, 2, 3 ... $n - 1$ qui tum ipsi tum simul numeri proximi vnitate maiores in $\mathfrak{K}$ continentur; similiter sit $(\mathfrak{K}\mathfrak{K}')$ multitudo numerorum in eadem serie qui ipsi in $\mathfrak{K}$ proxime sequentes vero in $\mathfrak{K}'$ continentur, vnde simul significatio signorum $(\mathfrak{K}\mathfrak{K}'')$, $(\mathfrak{K}'\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}')$, $(\mathfrak{K}'\mathfrak{K}'')$, $(\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}''\mathfrak{K}')$, $(\mathfrak{K}''\mathfrak{K}'')$ sponte innotescet. Quo facto dico *primo*, fieri $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$. Supponendo enim, h, h', h'' etc. esse omnes numeros seriei 1, 2, 3 ... $n - 1$ qui ipsi in $\mathfrak{K}$ proxime maiores $h + 1$, $h' + 1$, $h'' + 1$ etc. autem in $\mathfrak{K}'$ continentur, et quorum ideo multitudo $= (\mathfrak{K}\mathfrak{K}')$, manifestum est omnes numeros $n - h - 1$, $n - h' - 1$, $n - h'' - 1$ etc. in $\mathfrak{K}'$ contineri, proxime maiores vero $n - h$, $n - 1'$ etc. in $\mathfrak{K}$; quare quum tales numeri omnino dentur $(\mathfrak{K}'\mathfrak{K})$, certo nequit esse $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$, et perinde demonstratur, esse non posse $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$, quocirca hi numeri necessario aequales erunt. Prorsus eodem modo probatur $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. Secundo, quum necessario quemuis numerum ex $\mathfrak{K}$, maximo $n - 1$ excepto, sequi debeat proxime maior vel in $\mathfrak{K}$, vel in $\mathfrak{K}'$ vel in $\mathfrak{K}''$ contentus, summa $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ fiet aequalis multitudini omnium numerorum in $\mathfrak{K}$ vnitate deminutae puta $= m - 1$, et simili ratione erit $(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m$.

His ita praeparatis euoluimus per praecepta art. 345 productum pp' in $(m, \mathfrak{A}' + 1) + (m, \mathfrak{B}' + 1) + (m, \mathfrak{C}' + 1) +$ etc., quam expressionem facile perspicietur reduci ad $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$, et quum per art. 345 I productum

$p'p''$ ex illo oriatur, substituendo pro $(m, 1)$, (m, g), (m, gg) resp. (m, g), (m, gg), (mg^3) i. e. pro p, p', p'' resp. p', p'', p, fiet $p'p'' = (\mathfrak{R}'\mathfrak{R})\,p' + (\mathfrak{R}'\mathfrak{R}')\,p'' + (\mathfrak{R}'\mathfrak{R}'')\,p$, et prorsus simili modo $p''p = (\mathfrak{R}'\mathfrak{R})\,p'' + (\mathfrak{R}'\mathfrak{R}')\,p + (\mathfrak{R}'\mathfrak{R}'')\,p'$. Hinc protinus sequitur *primo* $B = m(p + p' + p'') = -m$; *secundo* quum simili ratione, vt antea pp' euolutum est, etiam pp'' ad $(\mathfrak{R}''\mathfrak{R})\,p + (\mathfrak{R}''\mathfrak{R}')\,p' + (\mathfrak{R}''\mathfrak{R}'')\,p''$ reducatur, atque haec expressio cum praecedente identica esse debeat, necessario erit $(\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}'\mathfrak{R}')$ et $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R})$. Hinc colligitur, statuendo $(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a$, $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}') = b$, $(\mathfrak{R}'\mathfrak{R}') = (\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}'') = c$, fieri $m - 1 = (\mathfrak{R}\mathfrak{R}) + (\mathfrak{R}\mathfrak{R}') + (\mathfrak{R}\mathfrak{R}'') = (\mathfrak{R}\mathfrak{R}) + b + c$, atque $a + b + c = m$, vnde $(\mathfrak{R}\mathfrak{R}) = a - 1$, ita vt illae nouem quantitates incognitae ad tres, a, b, c siue potius propter aequationem $a + b + c = m$ ad duas reductae sint. Denique patet, quadratum pp euolui in $(m, 1 + 1) + (m, \mathfrak{A} + 1) + (m, \mathfrak{B} + 1) + (m, \mathfrak{C} + 1) +$ etc.; inter partes huius expressionis reperietur (m, n) quae reducitur ad $(m, 0)$ siue ad m, reliquas vero facile perspicietur reduci ad $(\mathfrak{R}\mathfrak{R})p + (\mathfrak{R}\mathfrak{R}')p' + (\mathfrak{R}\mathfrak{R}'')p''$, vnde habetur $pp = m + (a - 1)p + bp' + cp''$.

Hoc itaque modo per disquisitiones praecedentes quatuor hasce reductiones nacti sumus:

$$\begin{aligned} pp &= m + (a-1)p + bp' + cp'' \\ pp' &= \quad\; bp + cp' + ap'' \\ pp'' &= \quad\; cp + ap' + bp'' \\ p'p'' &= \quad\; ap + bp' + cp'' \end{aligned}$$

vbi inter tres incognitas a, b, c aequatio conditionalis $a + b + c = m$ ... (I) intercedit, insuperque certum est ipsas esse numeros integros. Hinc colligitur $C = p \times p'p'' = app + bpp' + cpp'' = am + (aa + bb + cc - a)p + (ab + bc + ac)p' + (ab + bc + ac)p''$. At quum $pp'p''$ sit functio inuariabilis aggregatorum p, p', p'', coëfficientes per quos haec in expr. praec. multiplicata sunt necessario aequales erunt (art. 350), vnde habetur aequatio noua $aa + bb + cc - a = ab + bc + ac$ ... (II), atque hinc $C = am + (ab + bc + ac)(p + p' + p'')$, siue (propter I, et $p + p' + p'' = -1$), $C = aa - bc$ ... (III). Iam etsi C hic a tribus incognitis pendeat, inter quas duae tantum aequationes habentur, tamen hae, adiumento conditionis ex qua a, b, c sunt integri, ad plenam determinationem ipsius C sufficiunt. Quod vt ostendamus, aequationem II ita exhibemus $12a + 12b + 12c + 4 = 36aa + 36bb + 36cc - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4$; pars prior, per I, fit $= 12m + 4 = 4n$; posterior vero reducitur ad $(6a - 3b - 3c - 2)^2 + 27(b - c)^2$, aut scribendo k pro $2a - b - c$, ad $(3k - 2)^2 + 27(b - c)^2$. Hinc patet, numerum $4n$ (i. e. generaliter quadruplum cuiuslibet primi formae $3n + 1$) per formam $xx + 27yy$ repraesentari posse, quod quidem sine difficultate e theoria generali formarum binariarum deduci potest, attamen satis mirum est, talem discerptionem cum valoribus ipsarum a, b, c cohaerere. At numerus $4n$ semper vnico tantum modo in quadratum et quadratum 27^{plex} discerpi potest,

quod ita demonstramus *). Si supponatur $4n = tt + 27uu = t't' + 27u'u'$, fieret *primo* $(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16nn$, *secundo* $(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16nn$, *tertio* $(tu' + t'u)(tu' - t'u) = 4n(u'u' - uu)$; ex aequatione tertia sequitur, ipsum n, quoniam est numerus primus, alterutrum numerorum $tu' + t'u$, $tu' - t'u$ metiri; e prima et secunda vero patet, vtrumque hunc numerum esse minorem quam n; quare is quem n metitur necessario esse debet $= 0$, adeoque etiam $u'u' - uu = 0$, vnde $u'u' = uu$ et $t't' = tt$, i. e. duae illae discerptiones non different. Si itaque discerptionem ipsius $4n$ in quadratum et quadratum 27^{plex} notam supponimus (quam vel per methodum directam sect. V vel per indirectam in artt. 323, 324 traditam eruere licet) puta si habetur $4n = MM + 27NN$, quadrata $(3k - 2)^2$, $(b - c)^2$ determinata erunt, et loco aequationis II duas iam nacti erimus. Sed facile patet, non solum quadratum $(3k - 2)^2$ sed etiam radicem ipsam $3k - 2$ penitus determinatam esse; quum enim necessario sit vel $= +M$ vel $= -M$, ambiguitas inde tolletur quod k fieri debet integer, quamobrem statuetur $3k - 2 = +M$ vel $= -M$, prout M est formae $3z + 1$ vel $3z + 2$ **). Iam quum fiat k

*) Magis directe haecce propositio e principiis sect. V probari posset.

**) Manifesto M nequit esse formae $3z$, alioquin enim $4n$ per 3 diuisibilis euaderet. — Ad ambiguitatem, vtrum $b - c$ statui debeat $= N$, an $= -N$, hic non opus est respicere, neque etiam per rei naturam vllo modo

$= 2a - b - c = 3a - m$, erit $a = \frac{1}{3}(m + k)$, $b + c = m - a = \frac{1}{3}(2m - k)$, vnde $C = aa - bc = aa - \frac{1}{4}(b + c)^2 + \frac{1}{4}(b - c)^2 = \frac{1}{9}(m + k)^2 - \frac{1}{36}(2m - k)^2 + \frac{1}{4}NN = \frac{1}{12}kk + \frac{1}{3}km + \frac{1}{4}NN$, atque sic omnes coëfficientes aequ. quaesitae inuenti. *Q. E. F.* — Haec formula adhuc simplicior euadit, si pro NN eius valor ex aequ. $(3k - 2)^2 + 27NN = 4n = 12m + 4$ substituitur, vnde elicitur calculo facto $C = \frac{1}{9}(m + k + 3km) = \frac{1}{9}(m + kn)$. Idem valor etiam ad $(3k - 2)\,NN + k^3 - 2kk + k - km + m$ reduci potest, quae expressio, ad vsum quidem minus idonea, protinus monstrat, C vt par est certo euadere integrum.

Ex. Pro $n = 19$, fit $4n = 49 + 27$, vnde $3k - 2 = +7$, $k = 3$, $C = \frac{1}{9}(6 + 57) = 7$ et aequatio quaesita $x^3 + xx - 6x - 7 = 0$ vt supra (art. 351). — Simili modo pro $n = 7, 13, 31, 37, 43, 61, 67$ valor ipsius k eruitur resp. $1, -1, 2, -3, -2, 1, -1$, vnde $C = 1, -1, 8, -11, -8, 9, -5$.

Ceterum etsi problema in hoc art. solutum satis intricatum sit, tamen id supprimere noluimus, tum propter solutionis elegantiam, tum quod variis artificiis in vsum vocandis occasionem dedit, quae in aliis quoque quaestionibus insigni cum fructu adhiberi poterunt.

auferri potest, quum ab electione radicis primitiuae g pendeat, ita vt pro aliis radicibus primitiuis differentia $b - c$ positiua euadat, pro aliis negatiua.

359. Disquisitiones praecc. circa *inuentionem* aequationum auxiliarium versabantur: iam de earum *solutione* proprietatem magnopere insignem explicabimus. Constat, omnes summorum geometrarum labores, aequationum ordinem quartum superantium resolutionem generalem, siue (vt accuratius quid desideretur definiam) AFFECTARVM REDVCTIONEM AD PVRAS, inueniendi semper hactenus irritos fuisse, et vix dubium manet, quin hocce problema non tam analyseos hodiernae vires superet, quam potius aliquid impossibile proponat (Cf. quae de hoc argumento annotauimus in *Demonstr. noua* etc. *p.* 22). Nihilominus certum est, innumeras aequationes affectas cuiusque gradus dari, quae talem reductionem ad puras admittant, geometrisque gratum fore speramus, si nostras aequationes auxiliares semper huc referendas esse ostenderimus. Sed propter amplum ambitum huius disquisitionis, praecipua tantum momenta, quae ad possibilitatem ostendendam necessaria sunt, hoc loco tradimus, vberioremque tractationem qua hoc argumentum perdignum est ad aliud tempus differimus. Praemittendae sunt quaedam obseruationes generales circa radices aequ. $x^e - 1 = 0$, quae eum quoque casum complectantur, vbi e est numerus compositus.

I. Exhibentur hae radices (vt ex libris elementaribus notum est) per $\cos\frac{kP}{e} + i \sin\frac{kP}{e}$, vbi pro k accipiendi sunt e numeri $0, 1, 2, 3 \ldots e - 1$, aut quicunque alii his secundum modulum e congrui. Vna radix, pro $k = 0$ aut ge-

neraliter pro k per e diuisibili fit $= 1$; cuiuis alii valori ipsius k radix ab 1 diuersa respondet.

II. Quum sit $(\cos \frac{kP}{e} + i \sin \frac{kP}{e})^{\lambda} = \cos \frac{\lambda kP}{e} + i \sin \frac{\lambda kP}{e}$, patet, si R sit radix talis quae respondeat valori ipsius k ad e primo, in progressione R, RR, R^3 etc. terminum e^{tum} quidem esse $= 1$, omnes antecedentes vero ab 1 diuersos. Hinc statim sequitur, omnes e quantitates 1, R, RR, $R^3 \ldots R^{e-1}$ inaequales esse, et quum manifesto omnes aequationi $x^e - 1 = 0$ satisfaciant, exhibebunt omnes radices huius aequationis.

III. Denique in eadem suppositione aggregatum $1 + R^{\lambda} + R^{2\lambda} \ldots + R^{\lambda(e-1)}$ fit $= 0$, pro quouis valore integro ipsius λ per e non diuisibili; etenim est $= \frac{1 - R^{\lambda e}}{1 - R^{\lambda}}$, cuius fractionis numerator fit $= 0$, denominator vero non $= 0$. Quando vero λ per e diuisibilis est, illud aggregatum manifesto fit $= e$.

360. Sit, vt semper in praecc., n numerus primus, g radix primitiua pro modulo n, atque $n - 1$ productum e tribus integris positiuis; breuitatis caussa disquisitionem ita statim instituemus, vt etiam ad casus vbi α aut $\gamma = 1$ pateat; quando $\gamma = 1$, pro aggregatis $(\gamma, 1)$, (γ, g) etc. radices $[1]$, $[g]$ etc. accipere oportebit. Supponamus itaque, ex omnibus α aggregatis $\mathfrak{G}\gamma$ terminorum cognitis $(\mathfrak{G}\gamma, 1)$, $(\mathfrak{G}\gamma, g)$,

$(\mathfrak{C}\gamma, gg) \ldots (\mathfrak{C}\gamma, g^{\alpha-1})$ deducenda esse aggregata γ terminorum, quod negotium supra ad aequationem affectam $\mathfrak{C}^{\text{ti}}$ gradus reduximus, nunc vero per puram aeque altam absoluere docebimus. Ad abbreuiandum pro aggregatis $(\gamma, 1)$, (γ, g^{α}), $(\gamma, g^{2\alpha}) \ldots (\gamma, g^{\alpha\mathfrak{c}-\alpha})$, quae sub $(\mathfrak{C}\gamma, 1)$ contenta sunt, scribemus $a, b, c \ldots m$ resp.; pro his (γ, g), $(\gamma, g^{\alpha+1}) \ldots (\gamma, g^{\alpha\mathfrak{c}-\alpha+1})$ sub $(\mathfrak{C}\gamma, g)$ contentis resp. $a', b' \ldots m'$; pro his (γ, gg), $(\gamma, g^{\alpha+2}) \ldots (\gamma, g^{\alpha\mathfrak{c}-\alpha+2})$ resp. $a'', b'' \ldots m''$ etc. vsque ad ea quae sub $(\mathfrak{C}\gamma, g^{\alpha-1})$ continentur.

I. Iam designet R indefinite radicem aequationis $x^{\mathfrak{c}} - 1 = 0$, supponamusque ex euolutione potestatis $\mathfrak{C}^{\text{tae}}$ functionis $t = a + Rb + RRc \ldots + R^{\mathfrak{c}-1}m$ oriri per praecepta art. 345.

$$\begin{array}{l} N + Aa + Bb + Cc \ldots + Mm \\ \quad + A'a' + B'b' + C'c' \ldots + M'm' \\ \quad + A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ \quad + \text{etc.} = T \end{array}$$

vbi omnes coëfficientes N, A, B, A' etc. erunt functiones rationales integrae ipsius R. Supponantur etiam potestates $\mathfrak{C}^{\text{tae}}$ duarum aliarum functionum $u = R^{\mathfrak{c}}a + Rb + RRc \ldots + R^{\mathfrak{c}-1}m$, $u' = b + Rc + R''d \ldots + R^{\mathfrak{c}-2}m' + R^{\mathfrak{c}-1}a$ resp. euolui in U et U', perspicieturque facile ex art. 350., quum u' oriatur ex t commutando aggregata $a, b, c \ldots m$ resp. cum $b, c, d \ldots a$, fore $U' =$

$$\begin{array}{l} N + Ab + Bc + Cd \ldots + Ma \\ + A'b' + B'c' + C'd' \ldots + M'a' \\ + A''b'' + B''c'' + C''d'' \ldots + M''a'' \\ + \text{etc.} \end{array}$$

Porro patet quum sit $u = Ru'$, fore $U = R^{\mathfrak{e}}U'$, quare propter $R^{\mathfrak{e}} = 1$ coëfficientes correspondentes in U et U' aequales erunt; denique quum t et u in eo tantum differant, quod a in t per vnitatem, in u per $R^{\mathfrak{s}}$ multiplicatur, facile intelligetur, omnes coëfficientes correspondentes (i. e. qui eadem aggregata multiplicant) in T et U aequales esse, et proin etiam omnes coëfficientes correspondentes in T et U'. Hinc tandem colligitur $A = B = C$ etc. $= M$; $A' = B' = C'$ etc., $A'' = B'' = C''$ etc. etc., vnde T reducitur ad formam talem $N + A(^{\mathfrak{e}}\gamma, 1) + A'(^{\mathfrak{e}}\gamma, g) + A''(^{\mathfrak{e}}\gamma, gg)$ etc., vbi singuli coëfficientes N, A, A' etc. sub formam talem reducere licet $pR^{\mathfrak{e}-1} + p'R^{\mathfrak{e}-2} + p''R^{\mathfrak{e}-3} +$ etc. ita vt p, p', p'' etc. sint numeri integri dati.

II. Si pro R accipitur radix determinata aequationis $x^{\mathfrak{e}} - 1 = 0$ (cuius solutionem iam haberi supponimus), et quidem talis cuius nulla inferior potestas quam $\mathfrak{e}^{\text{ta}}$ vnitati aequalis est, etiam T quantitas determinata erit, ex qua t per aequationem puram $t^{\mathfrak{e}} - T = 0$ deriuare licet. At quum haec aequatio $\mathfrak{e}$ radices habeat, quae erunt t, Rt, $RRt \ldots R^{\mathfrak{e}-1}t$, dubium videri potest, quamnam radicem adoptare oporteat. Hoc vero prorsus rbitrarium esse, ita facile apparebit. Meminisse oportet, postquam omnia aggregata

$\mathfrak{e}\gamma$ terminorum determinata sint, radicem [1] eatenus tantum definitam esse, vt aliqua ex $\mathfrak{e}_\gamma$ radicibus in $(\mathfrak{e}\gamma, 1)$ contentis hoc signo denotari debeat; et perin omnino arbitrarium esse, quidnam ex $\mathfrak{e}$ aggregatis ipsum $(\mathfrak{e}\gamma, 1)$ constituentibus per a designare velimus. Quodsi iam, aliquo aggregato determinato per a expresso supponatur fieri $t = \mathfrak{T}$, facile perspicietur, si postea aggregatum id, quod modo designabatur per b, per a denotare lubeat, ea quae antea erant $c, d \ldots a, b$ nunc fieri $b, c \ldots m, a$, adeoque valorem ipsius t nunc $= \frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\mathfrak{e}-1}$. Simili modo si per a id aggregatum exprimere placet quod ab initio erat c, valor ipsius t fiet $= \mathfrak{T}R^{\mathfrak{e}-2}$, et ita porro t cuicunque quantitatum $\mathfrak{T}, \mathfrak{T}R^{\mathfrak{e}-1}, \mathfrak{T}R^{\mathfrak{e}-2}$ etc. aequalis censeri potest, i. e. cuilibet radici aequ. $x^{\mathfrak{e}} - T = 0$, prout aliud aliudue aggregatum sub $(\mathfrak{e}\gamma, 1)$ contentum per $(\gamma, 1)$ expressum supponatur. *Q. E. D.*

III. Postquam quantitas t hoc modo determinata est, $\mathfrak{e} - 1$ alias inuestigare oportet, quae ex t prodeunt, si in eius expressione pro R successiue $RR, R^3, R^4 \ldots R^{\mathfrak{e}}$ substituuntur, puta $t' = a + RRb + R^4c \ldots + R^{2\mathfrak{e}-2}m$, $t'' = a + R^3b + R^6c \ldots + R^{3\mathfrak{e}-3}m$ etc. Vltima quidem iam habetur, quum manifesto fiat $= a + b + c \ldots + m = (\mathfrak{e}\gamma, 1)$; reliquae vero sequenti modo erui possunt. Si per praecepta art. 345, simili modo vt $t^{\mathfrak{e}}$ antea in I, productum $t^{\mathfrak{e}-2}t'$ euoluitur, probabitur per methodum praecedenti prorsus analogam, quod inde prodeat ad formam talem $\mathfrak{N} + \mathfrak{A}(\mathfrak{e}_\gamma, 1) + \mathfrak{A}'(\mathfrak{e}\gamma, g) +$

$\mathfrak{A}''(6\gamma, gg)$ etc. $= T'$ reduci posse, ita vt $\mathfrak{N}$, $\mathfrak{A}$, $\mathfrak{A}'$ etc. sint functiones rationales integrae ipsius R, adeoque T' quantitas nota, vnde habebitur $t' = \frac{T'tt}{T}$. Prorsus eodem modo, si ex euolutione producti $t^{6-3}t''$ prodire supponitur T'', haec expressio similem formam habebit et proin ex eius valore noto deriuabitur t'' per aequationem $t'' = \frac{T''t^3}{T}$; perinde t''' per aequationem talem inuenietur $t''' = \frac{T'''t^4}{T}$ ita vt T''' sit quantitas nota etc.

Haec methodus non foret applicabilis, si fieri posset $t = 0$, vnde etiam esse deberet $T = T' = T''$ etc. $= 0$; sed probari potest hoc esse impossibile, etsi demonstrationem propter prolixitatem hoc loco supprimere oporteat. — Dantur etiam artificia peculiaria per quae fractiones $\frac{T'}{T}$, $\frac{T''}{T}$ etc. in functiones rationales *integras* ipsius R conuertere licet; nec non methodi breuiores pro eo casu vbi $\alpha = 1$ valores ipsarum t', t'' etc. eruendi, quae omnia hic silentio praeterire debemus.

IV. Denique simulac t, t', t'' etc. inuentae sunt, habebitur statim per obs. III art. praec. $t + t' + t''$ + etc. $= 6a$, vnde valor ipsius a notus erit, ex quo per art. 346 valores omnium reliquorum aggregatorum γ terminorum deriuari poterunt. — Valores ipsorum b, c, d etc. etiam per aequationes sequentes elici possunt, quarum ratio cuiuis attendenti facile patebit: $6b = R^{6-1}t +$

$R^{\mathfrak{c}-2}t' + R^{\mathfrak{c}-3}t'' + \text{etc.}$, $\mathfrak{c}c = R^{2\mathfrak{c}-2}t + R^{2\mathfrak{c}-4}t' + R^{2\mathfrak{c}-6}t''$ etc., $\mathfrak{c}d = R^{3\mathfrak{c}-3}t + R^{3\mathfrak{c}-6}t' + \text{etc. etc.}$

Ex magno numero obseruationum ad disquisitionem praec. pertinentium hic vnam tantum attingimus. Quod attinet ad solutionem aequationis purae $x^{\mathfrak{c}} - T = 0$, facile patet, T in plerisque casibus valorem imaginarium $P + iQ$ habere, vnde illa solutio partim a sectione anguli (cuius tangens $= \frac{Q}{P}$) partim a sectione rationis (vnitatis ad $\sqrt{(PP + QQ)}$) in $\mathfrak{c}$ partes, vt constat, pendebit. Vbi valde mirabile est (quod tamen fusius hic non exsequimur), valorem ipsius $\sqrt[\mathfrak{c}]{(PP + QQ)}$ semper *rationaliter* per quantitates iam notas exprimi posse, ita vt, praeter extractionem radicis quadraticae, ad solutionem *sola* sectio anguli requiratur, e. g. pro $\mathfrak{c} = 3$ sola trisectio anguli, quum pro plerisque aliis aequationibus cubicis, quarum radices omnes reales sunt, simul anguli et rationis trisectio euitari nequeat.

Tandem quum nihil obstet, quo minus statuamus $\alpha = 1$, $\gamma = 1$ adeoque $\mathfrak{c} = n - 1$: manifestum est, solutionem aequationis $x^n - 1 = 0$ statim reduci posse ad solutionem aequationis purae $n - 1^{ti}$ gradus $x^{n-1} - T = 0$, vbi T per radices aequationis $x^{n-1} - 1 = 0$ determinabitur. Vnde adiumento obseruationis modo factae colligitur, sectionem circuli integri in n partes requirere 1° sectionem circuli integri in $n - 1$ partes, 2° sectionem alius arcus, qui illa sectione facta construi potest, in $n - 1$ partes, 3° extractionem vnius radicis quadraticae, et quidem ostendi potest, hanc semper esse $\sqrt{n}$.

361. Superest vt nexum inter radices Ω atque functiones trigonometricas angulorum $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$ ... $\frac{(n-1)P}{n}$ adhuc propius contemplemur. Methodus quam pro inueniendis radicibus Ω exposuimus ita comparata est, vt adhuc incertum relinquat (nisi tabulae sinuum inter laborem ita vt supra diximus consultae fuerint, quod tamen minus directum foret), *quaenam* radices *singulis* illis angulis respondeant i. e. quaenam radix sit $= \cos\frac{P}{n} + i\sin\frac{P}{n}$, quaenam $= \cos\frac{2P}{n} + i\sin\frac{2P}{n}$ etc. Haec vero incertitudo facile discutitur, reflectendo, cosinus angulorum $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$ ... $\frac{(n-1)P}{2n}$ continuo decrescere (siquidem etiam signorum ratio habeatur), sinus omnes positiuos esse; angulos $\frac{(n-1)P}{n}$, $\frac{(n-2)P}{n}$, $\frac{(n-3)P}{n}$ ... $\frac{(n+1)P}{2n}$ vero eosdem resp. cosinus habere vt illos, sinus autem negatiuos ceterum magnitudine absoluta sinubus illorum aequales. Quare e radicibus Ω duae istae, quae partes reales maximas (inter se aequales) habent, respondebunt angulis $\frac{P}{n}$, $\frac{(n-1)P}{n}$, et quidem priori ea vbi quantitas imaginaria i per quantitatem positiuam, posteriori ea vbi i per quantitatem negatiuam multiplicata est. Ex $n - 3$ reliquis radicibus istae rursus quae maximas partes reales habent angulis $\frac{2P}{n}$, $\frac{(n-2)P}{n}$ respondebunt et sic porro.

— Simulac ea radix cui angulus $\frac{P}{n}$ respondet agnota est, eae quae angulis reliquis respondent etiam inde distingui poterunt, quod, si illa supponatur esse $=$, [1] angulis $\frac{2P}{n}$, $\frac{3P}{n}$, $\frac{4P}{n}$ etc. manifesto respondebunt radices $[\Omega^\lambda]$, $[3^\lambda]$, $[4^\lambda]$ etc. Ita in exemplo art. 353 illico videtur, angulo $\frac{1}{19}P$ aliam radicem respondere non posse quam hanc [11] anguloque $\frac{18}{19}P$ radicem [8]; similiter angulis $\frac{2}{19}P$, $\frac{17}{19}P$, $\frac{3}{19}P$, $\frac{16}{19}P$ etc. respondent radices [3], [16], [14], [5] etc. In exemplo art. 354 angulo $\frac{1}{17}P$ manifesto respondet radix [1], angulo $\frac{2}{17}P$ haec [2] etc. Hoc itaque modo cosinus et sinus angulorum $\frac{P}{n}$, $\frac{2P}{n}$ etc. plene determinati erunt.

362. Quod vero attinet ad reliquas functiones trigonometricas horum angulorum, possent eae quidem e cosinubus et sinubus respondentibus per methodos vulgo notas facile deriuari, puta secantes et tangentes, diuidendo vnitatem et sinus per cosinus; nec non cosecantes et cotangentes, diuidendo vnitatem et cosinus per sinus. Sed commodius plerumque idem obtinetur adiumento formularum sequentium absque diuisionibus per meras additiones. Sit ω angulus quicunque ex his $\frac{P}{n}$, $\frac{2P}{n}$ ... $\frac{(n-1)P}{n}$ atque $\cos\omega + i\sin\omega = R$, vnde R erit aliqua e radicibus Ω, $\cos\omega = \frac{1}{2}(R + \frac{1}{R}) = \frac{1+RR}{2R}$, $\sin\omega = \frac{1}{2i}(R - \frac{1}{R}) = \frac{i(1-RR)}{2R}$. Hinc fit $\sec\omega =$

$\frac{2R}{1+RR}$, $\text{tang}\,\omega = \frac{i(1-RR)}{1+RR}$, $\text{cosec}\,\omega = \frac{2Ri}{RR-1}$, $\text{cotang}\,\omega = \frac{i(RR-1)}{RR-1}$. Iam numeratores harum quatuor fractionum ita transformare ostendemus, vt per denominatores diuisibiles euadant.

I. Propter $R = R^{n+1} = R^{2n+1}$, fit $2R = R + R^{2n+1}$, quam expressionem per $1 + RR$ diuisibilem esse patet, quum n sit numerus impar. Hinc fit $\sec\omega = R - R^3 + R^5 - R^7 \ldots + R^{2n-1}$, adeoque (quum propter $\sin\omega = \sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega$ etc. manifesto fiat $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$), $\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega$, siue tandem, (quoniam $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$ etc), $= 2(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega) \pm \cos n\omega$, signo signo superiori vel inferiori valente prout n est formae $4k+1$ vel $4k+3$. Manifesto haec formula etiam ita exhiberi potest

$$\sec\omega = \pm(1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega).$$

II. Simili modo substituendo $1 - R^{2n+2}$ pro $1 - RR$, prodit $\text{tang}\,\omega = i(1 - RR + R^4 - R^6 \ldots - R^{2n})$, siue (quoniam $1 - R^{2n} = 0$, $RR - R^{2n-2} = 2i\sin 2\omega$, $R^4 - R^{2n-4} = 2i\sin 4\omega$ etc.),

$$\text{tang}\,\omega = 2(\sin 2\omega - \sin 4\omega + \sin 6\omega \ldots \mp \sin(n-1)\omega).$$

III. Quum habeatur $1 + RR + R^4 \ldots + R^{2n-2} = 0$ fit $n = n - 1 - RR - R^4 \ldots$

$R^{2n-2} = (1 - 1) + (1 - RR) + (1 - R^4) \ldots + (1 - R^{2n-2})$ cuius aggregati partes singulae per $1 - RR$ sunt diuisibiles. Hinc $\frac{n}{1-RR} = 1 + (1 + RR) + (1 + RR + R^4) \ldots + (1 + RR + R^4 \ldots + R^{2n-4}) = (n - 1) + (n - 2)RR + (n - 3)R^4 \ldots + R^{2n-4}$; quocirca multiplicando per 2, subtrahendo $0 = (n - 1)(1 + RR + R^4 \ldots + R^{2n-2})$ rursusque per R multiplicando fit $\frac{2nR}{1-RR} = (n - 1)R + (n - 3)R^3 + (n - 5)R^5 \ldots - (n - 3)R^{2n-3} - (n - 1)R^{2n-1}$, vnde protinus deducitur $\text{cosec}\omega = \frac{1}{n}((n - 1)\sin\omega + (n - 3)\sin 3\omega \ldots - (n - 1)\sin(2n - 1)\omega) = \frac{2}{n}((n - 1)\sin\omega + (n - 3)\sin 3\omega$ — etc. $+ 2\sin(n - 2)\omega)$, quae formula etiam ita exhiberi potest

$$\text{cosec}\omega = -\frac{2}{n}(2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n - 1)\sin(n - 1)\omega).$$

IV. Multiplicando valorem ipsius $\frac{n}{1-RR}$ supra traditum per $1 + RR$ et substrahendo $0 = (n - 1)(1 + RR + R^4 \ldots + R^{2n-2})$, prodit $\frac{n(1+RR)}{1-RR} = (n - 2)RR + (n - 4)R^4 + (n - 6)R^6 \ldots - (n - 2)R^{2n-2}$, vnde statim sequitur $\text{cotang}\omega = \frac{1}{n}((n - 2)\sin 2\omega + (n - 4)\sin 4\omega + (n - 6)\sin 6\omega \ldots - (n - 2)\sin(n - 2)\omega) = \frac{2}{n}((n - 2)\sin 2\omega + (n - 4)\sin 4\omega \ldots + 3\sin(n - 3)\omega + \sin(n -$

$1)\omega$), quam formulam etiam hocce modo exhibere licet

$$\text{cotang}\omega = -\frac{2}{n}(\sin\omega + 3\sin 3\omega \ldots + (n-2)\sin(n-2)\omega).$$

363. Quemadmodum, supponendo $n - 1 = ef$, functio X in e factores f dimensionem resolui potest, simulac valores omnium e aggregatorum f terminorum innotuerunt (art. 348): ita tunc etiam, supponendo $Z = 0$ esse aequationem $n - 1^{\text{ti}}$ ordinis cuius radices sint sinus aut quaelibet aliae functiones trigonometricae aegulorum $\frac{P}{n}, \frac{2P}{n}, \frac{(n-1)P}{n}$, functio Z in e factores f dimensionum resolui poterit, cuius rei praecipua momenta haec sunt.

Constet Ω ex e periodis f terminorum his $(f, 1) = P, P', P''$ etc., periodusque P e radicibus $[1], [a], [b], [c]$ etc.; P' ex his $[a'], [b'], [c']$ etc.; P'' ex his $[a'']$, $[b'']$, $[c'']$ etc. etc. Respondeat radici $[1]$ angulus ω, adeoque radicibus $[a]$, $[b]$ etc. anguli $a\omega$, $b\omega$ etc., radicibus $[a']$, $[b']$ etc. anguli $a'\omega$, $b'\omega$ etc., radicibus $[a'']$, $[b'']$ etc. anguli $a''\omega$, $b''\omega$ etc. etc: perspicieturque facile, omnes hos angulos simul sumtos cum angulis $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$ respectu functionum trigonometricarum *) con-

*) Hoc respectu duo anguli conueniunt, quorum differentia vel peripheriae integrae vel alicui eius multiplo aequalis est, quales secundum peripheriam congruos vocare possemus, si congruentiam sensu aliquantum latiori intelligere luberet.

uenire. Quodsi itaque functio de qua agitur per characterem φ angulo praefixum denotetur; productum ex e factoribus $x - \varphi\omega$, $x - \varphi a\omega$ etc. statuatur $= Y$, productum ex his $x - \varphi a'\omega$, $x - \varphi b'\omega$ etc. $= Y'$, productum ex his $x - \varphi a''\omega$, $x - \varphi b''\omega$ etc. $= Y''$ etc.: necessario erit productum $YY'Y'' \ldots = Z$. Superest iam, vt demonstremus, omnes coëfficientes in functionibus Y, Y', Y'' etc. ad formam talem $A + B(f, 1) + C(f, g) + D(f, gg) \ldots + L(f, g^{e-1})$ reduci posse, quo facto manifesto omnes pro cognitis habendi erunt, simulac valores omnium aggregatorum f terminorum innotuerunt: hoc sequenti modo efficiemus.

Sicuti $\cos\omega = \frac{1}{2}[1] + \frac{1}{2}[1]^{n-1}$, $\sin\omega = -\frac{1}{2}i[1] + \frac{1}{2}i[1]^{n-1}$, ita per art. praec. reliquae quoque functiones trigonometricae anguli ω ad formam talem reduci possunt $\mathfrak{A} + \mathfrak{B}[1] + \mathfrak{C}[1]^2 + \mathfrak{D}[1]^3 +$ etc., nulloque negotio perspicietur, functionem anguli $k\omega$ tunc fieri $= \mathfrak{A} + \mathfrak{B}[k] + \mathfrak{C}[k]^2 + \mathfrak{D}[k]^3 +$ etc. denotante k integrum quemcunque. Iam quum singuli coëfficientes in Y sint functiones rationales integrae inuariabiles ipsarum $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc., perspicuum est, si pro his quantitatibus valores sui substituantur, singulos coëfficientes fieri functiones rationales integras inuariabiles ipsarum $[1]$, $[a]$, $[b]$ etc.; quamobrem per art. 347 ad formam $A + B(f, 1) + C(f, g) +$ etc. reducentur. Et prorsus simili ratione etiam omnes coëfficientes in Y', Y'' etc. ad formam similem reducere licebit. *Q. E. D.*

364. Circa problema art. praec. quasdam adhuc obseruationes adiicimus.

I. Quum singuli coëfficientes in Y' sint functiones tales radicum in periodo P' (quam $= (f, a')$ statuere licet) contentarum, quales functiones radicum in P sunt coëfficientes respondentes in Y, ex art. 347 manifestum est, Y' ex Y deriuari posse, si modo vbique in Y pro $(f, 1)$, (f, g), (f, gg) etc. resp. substituantur (f, a'), $(f, a'g)$, $(f, a'gg)$ etc. Et perinde Y'' ex Y deriuabitur substituendo vbique in Y pro $(f, 1)$, (f, g), (f, gg) etc. resp. (f, a''), $(f, a''g)$, $(f, a''gg)$ etc. etc. Simulatque igitur functio Y euoluta est, reliquae Y', Y'' etc. nullo negotio inde sequuntur.

II. Supponendo $Y = x^f - \alpha x^{f-1} + \mathfrak{G} x^{f-2}$ — etc., coëfficientes α, $\mathfrak{G}$ etc. erunt resp. summa radicum aequ. $Y = 0$ i. e. quantitatum $\Phi\omega$, $\Phi a\omega$, $\Phi b\omega$ etc., summa productorum e binis etc. At plerumque hi coëfficientes multo commodius eruntur per methodum ei quae art. 349 tradita est similem, computando summam radicum $\Phi\omega$, $\Phi a\omega$, $\Phi b\omega$ etc., summam quadratorum, cuborum etc., atque hinc per theorema Newtonianum illos coëfficientes deducendo. — Quoties Φ designat tangentem, secantem, cotangentem aut cosecantem adhuc alia compendia dantur, quae tamen silentio hic praeterimus.

III. Considerationem peculiarem meretur is casus vbi f est numerus par, adeoque quaeuis periodus P, P', P'' etc. ex $\frac{1}{2}f$ periodis binorum terminorum composita. Constet P ex his $(2, 1)$ $(2, a)$, $(2, b)$, $(2, c)$ etc., conuenientque numeri 1, a, b, c etc. atque $n - 1$, $n - a$, $n - b$, $n - c$ etc. simul sumti, cum his $1, a, b, c$

etc. aut saltem (quod hic eodem redit) his secundum modulum n congrui erunt. Sed est $\varphi(n - 1)\omega = \pm \varphi\omega$, $\varphi(n - a)\omega = \pm \varphi a\omega$ etc., signis superioribus valentibus quoties φ designat cosinum aut secantem, inferioribus quando φ exprimit sinum, tangentem, cotangentem aut cosecantem. Hinc colligitur, in duobus casibus prioribus inter factores e quibus compositus est Υ binos semper aequales, adeoque Υ quadratum esse, et quidem $\Upsilon = yy$, si y ponatur aequalis producto ex $x - \varphi\omega$, $x - \varphi a\omega$, $x - \varphi b\omega$ etc. Similiter in iisdem casibus functiones reliquae Υ', Υ'' etc. quadrata erunt, et quidem supponendo P' constare ex $(2, a')$, $(2, b')$, $(2, c')$ etc.; P'' ex $(2, a'')$, $(2, b'')$, $(2, c'')$ etc. etc., productum ex $x - \varphi a'\omega$, $x - \varphi b'\omega$, $x - \varphi c'\omega$ etc. esse $= y'$, productum ex $x - \varphi a''\omega$, $x - \varphi b''\omega$ etc., $= y''$ etc. erit $\Upsilon' = y'y'$, $\Upsilon'' = y''y''$ etc.; nec non etiam functio Z quadratum erit (conf. supra art. 337), et radix producto ex y, y', y'' etc. aequalis. Ceterum facile perspicietur, y', y'' etc. perinde ex y deriuari, vt Υ', Υ'' etc. ex Υ sequi ante in I diximus; nec non singulos coëfficientes in y quoque ad formam $A + B(f, 1) + C(f, g) +$ etc. posse, quum summae singularum potestatum aequ. $y = 0$ manifesto sint semisses potestatum aequ. $\Upsilon = 0$, adeoque ad talem formam reducibiles. — In quatuor casibus posterioribus autem Υ erit productum e factoribus $xx - (\varphi\omega)^2$, $xx - (\varphi a\omega)^2$, $xx - (\varphi b\omega)^2$ etc., adeoque formae $x^f - \lambda x^{f-2} + \mu x^{f-4} -$ etc., patetque coëfficientes λ, μ etc. e summis quadratorum, biquadratorum etc. radicum $\varphi\omega$, $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc. deduci posse; et similiter se habebunt functiones Υ', Υ'' etc.

Ex. I. Sit $n = 17$, $f = 8$ atque designet φ cosinum. Hinc fit $Z = (x^8 + \frac{1}{2}x^7 - \frac{7}{4}x^6 - \frac{3}{4}x^5 + \frac{15}{16}x^4 + \frac{5}{16}x^3 - \frac{5}{32}xx - \frac{1}{32}x + \frac{1}{256})^2$, oportetque adeo $\sqrt{Z}$ in duos factores quaternorum dimensionum y, y' resoluere. Periodus $P = (8, 1)$ constat ex $(2, 1)$, $(2, 9)$, $(2, 13)$, $(2, 15)$ vnde y erit productum e factoribus $x - \varphi\omega$ $x - \varphi 9\omega$, $x - \varphi 13\omega$, $x - \varphi 15\omega$. Substituendo $\frac{1}{2}[k] + \frac{1}{2}[n - k]$ pro $\varphi k\omega$, inuenitur $\varphi\omega + \varphi 9\omega + \varphi 13\omega + \varphi 15\omega = \frac{1}{2}(8, 1)$; $(\varphi\omega)^2 + (\varphi 9\omega)^2 + (\varphi 13\omega)^2 + (\varphi 15\omega)^2 = 2 + \frac{1}{4}(8, 1)$; perinde summa cuborum $= \frac{3}{8}(8, 1) + \frac{1}{8}(8, 3)$, summa biquadratorum $= 1\frac{1}{2} + \frac{5}{16}(8, 1)$; hinc per theorema Newtonianum coëfficientibus in y determinatis prodit $y = x^4 - \frac{1}{2}(8, 1)x^3 + \frac{1}{4}((8, 1) + 2(8, 3))xx - \frac{1}{8}((8, 1) + 3(8, 3))x + \frac{1}{16}((8, 1) + (8, 3))$; y' vero ex y deriuatur commutando $(8, 1)$ cum $(8, 3)$; substituendo itaque pro $(8, 1)$, $(8, 3)$ valores $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$, $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$ fit

$$y = x^4 + (\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} + \tfrac{1}{8}\sqrt{17})xx + (\tfrac{1}{4} + \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$

$$y' = x^4 + (\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} - \tfrac{1}{8}\sqrt{17})xx + (\tfrac{1}{4} - \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$

Simili modo $\sqrt{Z}$ in quatuor factores binarum dimensionum resolui potest, quorum primus erit $(x - \varphi\omega)(x - \varphi 13\omega)$, secundus $(x - \varphi 9\omega)(x - \varphi 15\omega)$, tertius $(x - \varphi 3)(x\omega - \varphi 5\omega)$, quartus $(x - \varphi 10\omega)(x - \varphi 11\omega)$, omnesque coëfficientes in his factoribus per quatuor aggregata $(4, 1)$ $(4, 9)$, $(4, 3)$, $(4, 10)$ exprimi poterunt. Manifesto autem productum e factore

primo in secundum erit y, productum e tertio in quartum y'.

Ex. II. Si, omnibus reliquis manentibus, φ sinum indicare supponitur, ita vt $Z = x^{16} - \frac{17}{4}x^{14} + \frac{119}{16}x^{12} - \frac{221}{32}x^{10} + \frac{935}{256}x^8 - \frac{561}{512}x^6 + \frac{357}{2048}x^4 - \frac{51}{4096}xx + \frac{1}{65536}$ in duos factores 8 dimensionum y, y' resoluere oporteat, erit y productum e quatuor factoribus duplicibus $xx - (\varphi\omega)^2$, $xx - (\varphi 9\omega)^2$, $xx - (\varphi 13\omega)^2$, $xx - (\varphi 15\omega)^2$. Iam quum sit $\varphi k\omega = -\frac{1}{2}i[k] + \frac{1}{2}i[n - k]$, erit $(\varphi k\omega)^2 = -\frac{1}{4}[2k] + \frac{1}{2}[n] - \frac{1}{4}[2n - 2k] = \frac{1}{2} - \frac{1}{4}[2k] - \frac{1}{4}[2n - 2k]$; hinc deducitur summa quadratorum radicum $\varphi\omega$, 9ω, $\varphi 13\omega$, $\varphi 15\omega$ haec $2 - \frac{1}{4}(8, 1)$, earundem biquadratorum summa $= \frac{3}{2} - \frac{3}{16}(8, 1)$, summa potestatum sextarum $= \frac{5}{4} - \frac{9}{64}(8, 1) - \frac{1}{64}(8, 3)$, summa octauarum $\frac{35}{32} - \frac{25}{256}(8, 1) - \frac{1}{32}(8, 3)$. Hinc fit $y = x^8 - (2 - \frac{1}{4}(8, 1))x^6 + (\frac{3}{2} - \frac{5}{16}(8, 1) + \frac{1}{8}(8, 3))x^4 - (\frac{1}{2} - \frac{9}{64}(8, 1) + \frac{5}{64}(8, 3))xx + \frac{1}{16} - \frac{5}{256}(8, 1) + \frac{3}{256}(8, 3)$; y' deriuatur ex y commutando $(8, 1)$, $(8, 3)$, ita vt per substitutionem valorum horum aggregatorum habeatur

$$y = x^8 - (\tfrac{17}{8} - \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} - \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{17}{32} - \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} - \tfrac{1}{64}\sqrt{17}$$

$$y' = x^8 - (\tfrac{17}{8} + \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{51}{32} + \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{17}{32} + \tfrac{7}{64}\sqrt{17})xx + \tfrac{17}{256} + \tfrac{1}{64}\sqrt{17}$$

Perinde Z in quatuor factores resolui potest, quo-

rum coëfficientes per aggregata quatuor terminorum exprimi possunt, et quidem productum e duobus erit y, productum e duobus reliquis y'.

365. Reduximus itaque, per disquisitiones praecedentes, sectionem circuli in n partes, si n est numerus primus, ad solutionem tot aequationum, in quot factores resoluere licet numerum $n - 1$, quarum aequationem gradus per magnitudinem factorum determinantur. Quoties itaque $n - 1$ est potestas numeri 2, quod euenit pro valoribus ipsius n his 3, 5, 17, 257, 65537 etc., sectio circuli ad solas aequationes quadraticas reducetur, functionesque trigonometricae angulorum $\frac{P}{n}, \frac{2P}{n}$ etc. per radices quadraticas plus minusue complicatas (pro magnitudine ipsius n) exhiberi poterunt; quocirca in his casibus sectio circuli in n partes, siue descriptio polygoni regularis n laterum manifesto per constructiones geometricas absolui poterit. Ita e. g. pro $n = 17$ ex artt. 354, 361 facile pro cosinu anguli $\frac{1}{17}P$ expressio haec deriuatur:

$$-\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34 - 2\sqrt{17})} - \tfrac{1}{8}\sqrt{(17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{(34 + 2\sqrt{17})})}$$

cosinus multiplorum illius anguli formam similem, sinus autem vno signo radicali plus habent. Magnopere sane est mirandum, quod, quum iam Euclidis temporibus circuli diuisibilitas geometrica in tres et quinque partes nota fuerit, nihil his inuentis interuallo 2000 annorum adiectum sit, omnesque geometrae tamquam certum

pronunciauerint, praeter illas sectiones easque quae sponte inde demanant, puta sectiones in 15, 3.2^{μ}, 5.2^{μ}, 15.2^{μ} nec non in 2^{μ} partes, nullas alias per constructiones geometricas absolui posse. — Ceterum facile probatur, si numerus primus n sit $= 2^m + 1$, etiam exponentem m alios factores primos quam numerum 2 implicare non posse, adeoque vel $= 1$ vel $= 2$ vel altiori potestati numeri 2 aequalem esse debere; si enim m per vllum numerum imparem ζ (vnitate maiorem) diuisibilis esset atque $m = \zeta\eta$, foret $2^m + 1$ diuisibilis per $2^{\eta} + 1$, adeoque necessario compositus. Omnes itaque valores ipsius n, pro quibus ad meras aequationes quadraticas deferimur, sub forma $2^{2^{\nu}} + 1$ continentur; ita quinque numeri 3, 5, 17, 257, 65537 prodeunt statuendo $\nu = 0, 1, 2, 3, 4$ siue $m = 1, 2, 4, 8, 16$. Neutiquam vero pro *omnibus* numeris sub illa forma contentis sectio circuli geometrice perficitur, sed pro iis tantum qui sunt numeri primi. Fermatius quidem inductione deceptus affirmauerat, omnes numeros sub illa forma contentos necessario primos esse; at ill. Euler hanc regulam iam pro $\nu = 5$ siue $m = 32$ erroneam esse, numero $2^{32} + 1 = 4294967297$ factorem 641 inuoluente, primus animaduertit.

Quoties autem $n - 1$ alios factores primos praeter 2 implicat, semper ad aequationes altiores deferimur; puta ad vnam pluresue cubicas quando 3 semel aut pluries inter factores primos ipsius $n - 1$ reperitur; ad aequationes quinti gradus, quando $n - 1$ diuisibilis est per 5 etc., OMNIQVE RIGORE DEMONSTRARE POSSVMVS, HAS AEQVATIONES

ELEVATAS NVLLO MODO NEC EVITARI NEC AD INFERIORES REDVCI POSSE, etsi limites huius operis hanc demonstrationem hic tradere non patiantur, quod tamen monendum esse duximus, ne quis adhuc alias sectiones praeter eas quas theoria nostra suggerit, e. g. sectiones in 7, 11, 13, 19 etc. partes, ad constructiones geometricas perducere speret, tempusque inutiliter terat.

366. Si circulus in a^α partes secandus est, designante a numerum primum, manifesto hoc geometrice perficere licet, quando $a = 2$, neque vero pro vllo alio valore ipsius a, siquidem $\alpha > 1$; tunc enim praeter eas aequationes quae ad sectionem in a partes requiruntur necessario adhuc $\alpha - 1$ alias a^{ti} gradus soluere oportet; etiam has nullo modo nec euitare nec deprimere licet. Gradus itaque aequationum necessariarum e factoribus primis numeri $(a-1)a^{\alpha-1}$ generaliter (scilicet pro eo quoque casu vbi $\alpha = 1$) cognosci possunt.

Denique si circulus in $N = a^\alpha b^\beta c^\gamma \ldots$ partes secandus est, denotantibus a, b, c etc. numeros primos inaequales, sufficit, sectiones in a^α, b^β, c^γ etc. partes perfecisse (art. 336); quare vt gradus aequationum ad hunc finem necessariarum cognoscantur, factores primos numerorum $(a-1)a^{\alpha-1}$, $(b-1)b^{\beta-1}$, $(c-1)c^{\gamma-1}$ etc., siue quod hic eodem redit producti ex his numeris considerare oportet. Obseruetur, hoc productum exprimere multitudinem numerorum ad N primorum ipsoque minorum (art. 38). Geometrice itaque sectio tunc tantummodo absoluitur,

quando hic numerus est potestas binarii; quando vero factores primos alios quam 2 puta p, p' etc. implicat; aequationes gradus p^{ti}, p'^{ti} etc. nullo modo euitari possunt. Hinc colligitur generaliter, vt circulus geometrice in N partes diuidi possit, N esse debere *vel* 2 aut altiorem potestatem ipsius 2, *vel* numerum primum formae $2^m + 1$, *vel* productum e pluribus huiusmodi numeris primis, *vel* productum ex vno tali primo aut pluribus in 2 aut potestatem altiorem ipsius 2; siue breuius, requiritur, vt N neque vllum factorem primum imparem qui non est formae $2^m + 1$ implicet, neque etiam vllum factorem primum formae $2^m + 1$ pluries. Huiusmodi valores ipsius N infra 300 reperiuntur hi 38:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

ADDITAMENTA.

Ad art. 28. Solutio aequationis indeterminatae $ax = by \pm 1$ non primo ab ill. Eulero (vt illic dicitur) sed iam a geometra 17^{mi} saeculi Bachet de Meziriac, celebri Diophanti editore et commentatore, perfecta est, cui ill. La Grange hunc honorem vindicauit (Add. à l'Algebre d' Euler p. 525, vbi simul methodi indoles indicata est). Bachet inuentum suum in editione secunda libri *Problêmes plaisans et delectables qui se font par les nombres*, 1624, tradidit; in editione prima (à Lyon 1612), quam solam mihi videre licuit, nondum exstat, verumtamen iam annunciatur.

Ad artt. 151, 296, 297. Ill. Le Gendre demonstrationem suam denuo exposuit in opere praeclaro *Essai d'une theorie des nombres* p. 214 sqq., attamen ita, vt nihil essentiale mutatum sit: quamobrem haec methodus etiamnum omnibus obiectionibus in art. 297 prolatis obnoxia manet. Theorema quidem (cui vna suppositio innititur), in quauis progressione arithmetica $l, l + k, l + 2k$ etc., numeros primos reperiri, si k et l diuisorem

communem non habeant, fusius in hoc opere consideratum est p. 12 sqq.: sed rigori geometrico nondum satisfactum esse videtur. Attamen tunc quoque, quando hoc theorema plene demonstratum erit: suppositio altera supererit (dari numeros primos formae $4n + 3$, quorum non residuum quadraticum sit numerus primus datus formae $4n + 1$ positiue sumtus), quae an *rigorose* demonstrari possit, nisi theorema fundamentale ipsum iam *supponatur*, nescio. Ceterum obseruare oportet, ill. Le Gendre hanc posteriorem suppositionem non tacite assumsisse, sed ipsum quoque eam non dissimulauisse, p. 221.

Ad artt. 288–293. De eodem argumento, quod hic tamquam applicatio specialis theoriae formarum ternariarum exhibetur, et respectu rigoris et generalitatis ita absolutum esse videtur, vt nihil amplius desiderari possit, ill. Le Gendre in parte III operis sui p. 321–400 disquisitionem multo ampliorem instituit *). Principiis et methodis vsus est a nostris prorsus diuersis: attamen hac via compluribus difficultatibus implicatus est, quae effecerunt, vt theoremata palmaria demonstratione rigorosa munire non licuerit. Has difficultates ipse candide indicauit: sed ni fallimur hae quidem facilius forsan auferri poterunt, quam ea, quod in hac quoque disquisitione theorema modo memoratum (In quauis progressione

*) Vel nobis non monentibus lectores cauebunt, ne nostras formas ternarias cum eo, quod ill. Le Gendre forme trinaire d'un nombre dixit, confundant. Scilicet per hanc expressionem indicauit decompositionem numeri in tria quadrata.

arithmetica etc.) suppositum est, p. 371 annot. in fine.

Ad art. 306 VIII. In chiliade tertia determinantium negatiuorum reperti sunt 37 irregulares, inter quos 18 habent indicem irregularitatis 2, et 19 reliqui indicem 3.

Ad eundem X. Quaestionem hic propositam plene soluere nuper successit, quam disquisitionem plures partes tum Arithmeticae sublimioris tum Analyseos mirifice illustrantem in continuatione huius operis trademus quam primum licebit. Eadem docuit, coëfficientem m in art. 304 p. 504 esse $= \gamma = 2{,}3458847616$, designante γ eandem quantitatem vt in art. 302, et π vt ibidem semicircumferentiam circuli cuius radius 1.

* * *

In regulam art. 256 IV error irrepsit, qui vt emendetur, in linea pen. p. 394, pro $Anabc\ldots$ legatur $\frac{Anabc\ldots}{2\mathfrak{ABC}\ldots}$; et in linea vlt. verba *tum si* $\nu = 0$, *tum*, in l. prima et secunda p. 395 vero haec $\nu > 0$ *simulque* deleantur.

Tabvla I (artt. 58, 91)

		2. 3. 5. 7.11	13.17.19.23.29	31.37.41.43.47
3	2	1		
5	2	1. 3		
7	3	2. 1. 5		
9	2	1. *. 5. 4		
11	2	1. 8. 4. 7		
13	6	5. 8. 9. 7.11		
16	5	*. 3. 1. 2. 1	3	
17	10	10.11. 7. 9.13	12	
19	10	17. 5. 2.12. 6	13. 8	
23	10	8.20.15.21. 3	12.17. 5	
25	2	1. 7. *. 5.16	19.13.18.11	
27	2	1. *. 5.16.13	8.15.12.11	
29	10	11.27.18.20.23	2. 7.15.24	
31	17	12.13.20. 4.29	23. 1.22.21.27	
32	5	*. 3. 1. 2. 5	7. 4. 7. 6. 3	0
37	5	11.34. 1.28. 6	13. 5.25.21.15	27
41	6	26.15.22.39. 3	31.33. 9.36. 7	28.32
43	28	39.17. 5. 7. 6	40.16.29.20.25	32.35.18
47	10	30.18.17.38.27	3.42.29.39.43	5.24.25.37
49	10	2.13.41. *.16	9.31.35.32.24	7.38.27.36.23
53	26	25. 9.31.38.46	28.42.41.39. 6	45.22.33.30. 8

		2. 3. 5. 7.11 53.59.61.67.71	13.17.19.23.29 73.79.83.89	31.37.41.43.47
59	10	25.32.34.44.45 28	23.14.22.27. 4	7.41. 2.13.53
61	10	47.42.14.23.45 51.17	20.49.22.39.25	13.33.18.41.40
64	5	*. 3. 1.10. 5 5. 1. 3	15.12. 7.14.11	8. 9.14.13.12
67	12	29. 9.39. 7.61 3.54. 5	23. 8.26.20.22	43.44.19.63.64
71	62	58.18.14.33.43 59.29.37.11	27. 7.38. 5. 4	13.30.55.44.17
73	5	8. 6. 1.33.55 53. 5.58.50.44	59.21.62.46.35	11.64. 4.51.31
79	29	50.71.34.19.70 7.17.75.54.33	74. 9.10.52. 1 4	76.23.21.47.55
81	11	25. *.35.22. 1 45.53. 4.20.33	38.15.12. 5. 7 48.52	14.24.29.10.13
83	50	3.52.81.24.72 13.20.34.53.17	67. 4.59.16.36 43.47	32.60.38.49.69
89	30	72.87.18. 7. 4 10.45.19.32.26	65.82.53.31.29 68.46.27	57.77.67.59.34
97	10	86. 2.11.53.82 14.65.32.51.25	83.19.27.79.47 20.42.91.18	26.41.71.44.60

Tabvla II (art. 99)

	−1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37
3			−		−		−		−			−	−
5	−			−		−			−		−	−	
7		−			−	−				−	−		−
11			−	−		−				−		−	−
13	−		−				−	−		−	−		
17	−	−					−	−	−				
19				−	−	−		−	−	−			
23		−	−				−			−	−	−	
29	−			−	−		−			−	−		
31		−		−	−				−			−	
37	−		−		−	−							−
41	−	−		−						−		−	−
43						−	−	−		−		−	
47		−	−		−			−					−
53	−				−	−	−	−			−		−
59			−	−	−			−	−		−		
61	−		−	−			−		−				
67								−	−	−	−		−
71		−	−	−					−		−		−
73	−	−	−						−	−			−
79		−		−		−	−		−	−		−	
83			−		−	−		−		−	−	−	−
89	−	−		−		−		−					
97	−	−	−			−						−	

	+41	+43	+47	+53	+59	+61	+67	+71	+73	+79	+83	+89	+9
3		—				—	—		—	—			—
5	—				—	—		—		—		—	
7		—		—			—	—		—			
11			—	—	—		—	—				—	—
13		—		—		—				—			
17		—	—	—	—		—				—	—	
19		—	—			—			—		—		
23	—		—		—			—	—				
29				—	—		—	—			—		
31	—		—		—		—	—					—
37	—		—	—			—	—	—		—		
41	—	—			—	—			—		—		
43	—	—	—	—	—		—			—	—		—
47			—	—	—	—		—		—	—	—	—
53		—	—	—	—							—	—
59	—			—	—			—		—			
61	—		—			—			—		—		—
67			—		—		—	—	—		—	—	
71		—						—	—	—	—	—	
73	—					—	—	—	—	—		—	—
79							—		—	—	—	—	—
83	—				—	—					—		
89			—	—			—	—	—	—		—	—
97		—	—	—		—			—	—		—	—

Tabvla III (art. 316)

3 (0)..3; (1)..6
7 (0)..142857
9 (0)..1; (1)..2; (2)..4; (3)..8; (4)..7; (5)..5
11 (0)..09; (1)..18; (2)..36; (3)..72; (4)..45
13 (0)..076923; (1)..461538
17 (0)..0588235294 117647
19 (0)..0526315789 4736842 1
23 0)..0434782608 6956521739 13
27 (0)..037; (1)..074; (2)..148; (3)..296; (4)..592; (5)..185
29 (0)..0344827586 2068965517 24137931
31 (0)..0322580645 16129
(1)..5483870967 74193
37 (0)..027; (1)..135; (2)..675; (3)..378; (4)..891; (5)..459; (6)..297; (7)..486; (8)..432; (9)..162; (10)..810; (11)..054
41 (0)..02439; (1)..14634; (2)..87804; (3)..26829; (4)..60975; (5)..65853; (6)..95121; (7)..70731
43 (0)..0232558139 5348837209 3
(1)..6511627906 9767441860 4
47 (0)..0212765957 4468085106 3829787234 0425531914 893617
49 (0)..0204081632 6530612244 8979591836 7346938775 51
53 (0)..0188679245 283; (1)..4905660377 358 (2)..7547169811 320; (3)..6226415094 339
59 (0)..0169491525 4237288135 5932203389 8305084745 7627118644 06779661
61 (0)..0163934426 2295081967 2131147540 9836065573 7704918032 7868852459

67	(0)..0149253731	3432835820	8955223880
	597		
	1)..1791044776	1194029850	7462686567
	164		
71	0)..0140845070	4225352112	6760563380
	28169		
	(1)..8732394366	1971830985	9154929577
	46478		
73	(0)..01369863; (1)..06849315; (2)..34246575		
	(3)..71232876; (4)..56164383; (5)..80821917		
	(6..04109589; (7)..20547945; (8)..02739726		
79	(0)..0126582278	481; (1)..3670886075	949
	(2)..6455696202	531; (3)..7215189873	417
	(4)..9240506329	113; (5)..7974683544	303
81	(0)..012345679; (1)..135802469		
	(2)..493827160; (3)..432098765		
	4)..753086419; (5)..283950617		
83	(0)..0120481927	7108433734	9397590361
	4457831325	3	
	(1)..6024096385	5421686746	9879518072
	2891566265	0	
89	(0)..0112359550	5617977528	0898876404
	4943820224	7191	
	1)..3370786516	8539325842	6966292134
	8314606741	5730	
97	(0)..0103092783	5051546391	7525773195
	8762886597	9381443298	9690721649
	4845360824	7422680412	3711340206
	185567		

Goslariae ex Officina E. W. G. Kircher.

Errata Typographica.

P. 2. l. 9 a calce pro $\frac{A-a}{m}$ l. $\frac{a-A}{m}$. P. 4. l. 20 pro Ab l. AB. P. 6. l. 19 factores 100 et c quos iungere oportuisset separati sunt. Similiter aliis passim locis. P. 16. l. vlt pro $\dagger$ l. $\equiv$. P. 16 l. penult. literae α et B commate separentur. P. 19 l. 3. a. c. l. $\frac{b-av}{m}$. P. 20 l. 3 pro m l. n. Ibid l. 16 pro $30x'$ l. $38x'$. P. 22. l. 10, 12, 19 et 20 pro Av l. $a \dagger Av$. Ib. l. 19 pro $\frac{C}{\delta}$ l. $\frac{C}{\varepsilon}$. Ib. l. 21 pro $\frac{ABC}{\varepsilon}$ l. $\frac{ABC}{\delta^2}$. P. 31 l. 20 l. φN, φP. P. 33 l. 18 pro $\cdot M$ l. $= \cdot M$. P. 38. l. pen. l. incongruas. P. 39. l. 18 deleatur *deberi*. P. 40 l. 24 l. Comm. *nou*. P. 43 l. 10 incongruae. Ib. l. 22 pro praec. l. 45. P. 48. l. 3 pro $p-1$ factores l. factores numeri $p-1$. P. 52 l. 14 pro $\equiv$ l. $=$. P. 55 l. 9 pro $-$ l. $\dagger$. P. 59 l. 17 l. et $\sqrt[\delta]{A}$. Ib. l. 25 l. x^δ. P. 60 l. 5 l. posterioris. P. 62 l. 5 l. vnusque valor. Ib. l. 7 l. $\sqrt[n]{1}$ hi: $1, r, rr \ldots$ Ib. l. 13 pro vnitati l. ipsi A. P. 65 l. 3 l. etiam $kn-1$ per $\frac{t}{d}$. P. 69 l. 4 a. c. in fractionis numeratore pro p l. $p-1$. P. 70 l. 16 l. elegimus. P. 78 l. 17 pro p l. $p-1$. P. 82 l. 13 l. $x^t \equiv 1$. Ib. l. 20 pro $p^{\nu-1}$ l. $p^\nu - 1$. P. 83 l. 20 l. mod. $p^{\mu+2}$. Ib. l. vlt. pro t l. e. P. 84 l. 6 pro indeterminatum l. integrum. P. 85 l. 4 et 7 a calce pro μ l. n. P. 88 l. 12 pro $m \dagger 1$ l. $m \dagger 2$. P. 89 l. 3 pro $\dagger 7$ l. $\dagger 5$ aut $8n \dagger 7$. P. 92 l. 6 a. c. pro $\frac{1}{2}(m-1)^2$ l. $(\frac{1}{2}m-1)^2$. P. 93 art. 95 cum praecedente vniatur, numerusque 95 sequenti praeponatur. P. 97 l. 8 pro 95 l. 96. P. 99 l. 7 pro μ l. m. P. 100 l. 8 a. c. l. ipsius p^n. P. 101 l. 3 pro $2\varkappa \dagger 1$ l. $\varkappa \dagger 1$. P. 105 l. 8 a. c. l. Sect. praec. P. 107 l. 1 l. numerorum primorum. P. 108 inter l. penult. et vlt. exciderunt haec: $4n \dagger 1$; impar quando p est formae. P. 111 l. 7. insere numerum 43. P. 119 l. 13 l. non-residuum impar. P. 120 l. 17 l. numerorum imparium.

P. 123 l. 6 l. numeri qui ipsius 7. Ib. l. 7, 6 et 5 a. c. pro $(a^2 - a)^2$ l. $(a^2 + a)^2$. Ib. l. vlt. pro 1 l. — 1. P. 124 l. 1 et 2 pro -- l. +. P. 126 l. 10 l. Praemittimus. Ib. l. 13 pro *idem* l. *eadem*. P. 127 l 3 a. c. l. $n = he + f$. P. 128 l. vlt. dele (I) *et*. P. 130 l. 7 et 8 pro $a - rr$ l. $b - rr$. P. 131 l. 11 factor primus debet esse $\frac{1}{m+1}$. P. 133 l. vlt. pro a l. b. P 134 in theor. 14 signum superius debet esse +, inf. --. P. 140 l. 8 pro $+ A$ l. $-A$ et pro $-A$ l. $+A$. P. 146 l. 17 pro a' l. p et pro p l. a'. P. 148 l. 3 a. c. l. $-pRh$. Ib. l. pen. l. sequitur. P. 155 l. 22 pro primorum l. priorum. P. 161 l. 1 l. $xx - A$ contentorum impar est, B quoque in forma non diuisorum contentus erit. P. 166 l. 4 pro comperti l. experti. P. 168 l. 9 pro , l. $\surd$. Ib. l. vlt. pro $\mu m''$ l. $\mu' m'$. P. 170 l. 4 pro $x =$ l. $y =$. P. 174 l. 14 pro $+ y'$ l. $- y'$. P. 177 in aequ. 9 ante parenth. excidit factor D. P. 183 fin. in valoribus 2 et 4 ipsarum x et y signa + mutentur in --. P. 186 l. 4 pro $+ bc$ l. $- bc$. P. 187 l. 6 pro $Cm\mu$ l. $Cn\mu$. P. 188 l. pen. pro 8 l. 7. P. 189 l. 10 pro $\mathfrak{E}e'$ l. $-\mathfrak{E}'e$. P. 192 l. 11 pro $\mu m'$ l. $\mu' m'$. Ib. l. 15 l. μ', ν', m', n'. P. 194 l. 13 pro $n'b$ l. $m'b$, linea sq. vero pro $m'b$ l. $n'b$. P. 195 l. 3 a. c. pro mb l. nb. Ib. l. pen. pro nc l. nb. P. 204 l. 10 pro $\triangleright$ l. $\triangleleft$. P. 205 l. 19 et 20 l. externi. P. 207 l. 1 pro a, a', a'' l. a', a'', a'''. P. 210 l. 9 pro q l. u. P. 213 l. 6 post *adeoque* insere *haec forma*. Ib. l. 7 l. (± 2, ∓ 1, ∓ 2). Ib. l. 12 pro 1 l. 2. P. 221 l. 6 l. $73 = 25 + 48'$ P. 222 l. 2 pro $\surd D$ l. $\surd D + B$. Ib. l. 11 pro a l. a'. P. 223 l. 21 pro $\triangleleft C$ l. $\triangleright C$. P. 225 l. 9 pro B l. b. P. 227 l. 18 pro a l. $-a$. P. 228 l. 3 et 2 a. c. pro ± 5, ∓ 15, ± 5 l. ∓ 5, ± 15, ∓ 5. P. 232 l. 5 pro b l. b'. Ib. l. 6 pro $b + b''$ l. $b'' + b'''$. P. 233 l. 4 forma prima debet esse (1, 8, -- 15). P. 237 l. 12 pro $--''\alpha$ l. $--'\alpha$ Ib. l. 13 pro $--'''\alpha$ l. $--''\alpha$. P. 240 l. 11 verbum contra ponatur *post* semicolon. P. 241 l. 3 pro $,nm$ l. $,nm'$. P. 242 in aequ. 5 pro aA' l. $a'A$, in aequ. 6 pro $a'A$ l. $a'A'$. P. 253 l. 4 pro $\mp$ l. $\pm$. P 260 l. pen. pro m l. n. P. 261 l. 8 pro $a'uu$ l. $aa'uu$. P. 262 l. 12 et 13 pro hac, illa l. his, illis. Ib. l. 4. a. c. pro a' l. a. Ib. l. vlt. pro a l.

a'. P. 263 l. 9 l. U vero fit $= [2, 2, 7, 2, 2] = \frac{1}{3}[2, 7, 2, 2, 7]$. P. 272 l. 17 pro u^{λ} † l. u' †. P. 278 l. 11 l. non primus. Ib. l. 14 pro † 12 l. -- 12 Ib. l. 22 pro -- 12 l. † 12. Ib. l. vlt. pro † l. --. P. 279 l. 5 pro -- l. †. P. 280 l. 22 pro r l. 3. P. 282 l. l. 16 l. (a, b, c). Ib. l. 3 a. c. pro $2b_{\alpha\delta}$ l. $2b_{\alpha\gamma\delta}$ et pro $2_{\alpha\delta}$ l. $2_{\gamma\delta}$. P. 284 l. 3 pro $=$ 4 l. † 4. P. 297 l. 7 pro $\mathfrak{h} =$ l. $\gamma =$ Ib. l 12 l. quos. P. 299 l. 13 et 15 pro $\mathfrak{h}\mathfrak{z}$ l. $h\mathfrak{z}$; ib. l. 14 et 15 pro $\mathfrak{g}\mathfrak{z}$ l. $g\mathfrak{z}$. P. 300 post lineam 5, iterumque l. 7. post verbum *numero* insere $f(bb - ac)^2$ --. P. 307 l. 3 et bis in l. 5 pro f l. mf. P. 319 l. 11 a. c. pro *tum* si l. si *tum*. P. 328 l. 17 pro 27 l. 23. P. 335 l. 8 pro 9 l. -- 9. P. 347 l. 5 pro q'' l. q'''. P. 348 l. 5 pro $q'q'$ l. $p'q'$ et l 6 pro $q''q''$ l. $p''q''$. Ib. l. 20 l $k =$ 1. P. 360 l. 11, 12 pro $n\mathfrak{N}$, $n'\mathfrak{N}$ l. $n\mathfrak{N}$, $n'\mathfrak{N}$. Ibid. in valore ipsius (5. 8) muta -- in †. P. 361 l. 20 pro $\mathfrak{p}\mathfrak{q}'$ -- $\mathfrak{q}\mathfrak{p}'$ l. $\mathfrak{p}\mathfrak{q}'$ -- $\mathfrak{q}\mathfrak{p}'$. P. 363 l. 3 pro $\mathfrak{F}$ l. $\mathfrak{F}'$. P. 366 l. 1 pro p''' l. $\mathfrak{P}'''$. P. 371 l. 7 a c. pro † $\mathfrak{P}'$ l. -- $\mathfrak{P}'$. P. 380 l. 7. a c. pro mm' l. mm'. P. 381 l. 1 post verbum formam insere *ex f', g' compositam*. P. 387 l. 20 pro quatuor l. tres. P. 388 l. 12 pro W l. W'. P. 389 l. 7 a c. pro A l. AA. P. 390 l. 5 l. B est vel o vel $\frac{1}{2}A$. Ibid. l. 9, 11 et 12 pro a l. a -- $\frac{qqC}{A}$, et l. 10, 11 et 13 pro c l. c -- $\frac{q''q''C}{A}$. P. 394 l. 16 pro 2, l. 2'. P. 399 l. 2 pro 869 l. 867. Ib. l. 12 post classium insere proprie primitiuarum. P. 406 l. 11 a c. pro expressos l. expressio. P. 408 l 9 pro omnium characterem l. multitudinis omnium characterum. P. 410 l. 4 pro H' l. † H'. P. 415 l. 5 a c. pro † $2Rp$ l. -- $2Rp$. P. 416 l. 13 pro p l. -- p. Ibid post l. vlt. omissa sunt haec: $4n$ † 1, hoc statim sequitur ex VIII; si vero q est formae. P. 419 l. 8 a c. pro determinantes l. characteres. P. 420 l. 9 a c. l. vel 3, 4, vel 3, 8, vel 7, 8. P. 430 l. 13 pro substitutionis; Si l. substitutionis S; P. 437 l. 21 post *certe* insere *vel infra*. P. 442 in forma f' pro 4 l. -- 4. P. 444 l. 11 et 10 a c. deleantur signa negatiua. P. 453 l. 6 pro $_{\alpha}h$ l. h. P. 458 l. 17 l. quae forma adiuncta erit ei, quae oritur etc. P. 463 l. 17 et 18 pro 44 l. 39. P 471 l. 21 pro semicolo scribe comma. P. 477 l. 3 a c. pro -- 1 l. 1. P. 478 l. 9 pro -- 17 l. † 17. Ib. l.

11 pro 9 l. -- 18 et pro 1 l. 2. Ib. l. vlt. pro p l. p'. P. 479 l. 13, 22 et 23 pro 5 l. -- 5. Ib. l. 14 pro -- 17 l. 17. P. 491 l. 10 a c. l. 6, *aut* 12, *aut* 8. P. 495 l. 3 pro -- 61 l. 61. P. 496 l. 13 l. resolubile. Ib. l. 5 a c. l. theoremata quae praecedentium. P. 505 l. 11 post verbum formae omissa sunt haec: $4n + 1$, q numerus primus formae. P. 511 l. 15 adde: *puta pro* $x'' = 0$ Ib. l. vlt. et p. sq. l. 5, 8 et 11 pro A' l. A''. P. 513 l. 9 pro $d''dq$ l. $d''pq$. P. 516 l. 14 pro 4, 01 l. 4, 03. Ib. l. 7 a c. l. $\mathfrak{C} = 2ag +$. P. 517 l. 23 pro 7108 l. 7112. P. 519 l. 18 l. 37092 *classes*, *formula dat* 37074,3. P. 542 l. pen. pro $m =$ l. $n =$. P. 545 l. 8 et 9 pro 59 l. 69, et pro 1557 l. 1587. P. 550 l. potestatibus. P. 551 l. 20 l. $\frac{11}{16} = 0{,}6875$. P. 554 l. 3 a c. pro sit l. fit. P. 556 deleatur comma post sint. P. 563 l. 9 a c. pro si l. is. P. 568 l. 13 pro $2erap$ l. $2erap'$. Ib. l. 16 pro eap^{μ} l. eap'. Ib. l. 18 l. $uep^{\mu+\nu-1}$. P. 579 l. 24 pro omnes l. scilicet omnes. P. 584 l. 10 l. -- 2.3.5.11.29. P. 586 l. 16 l. priora sunt eadem. P. 590 l. 2 pro 102 l. 408. P. 591 l. vlt. l. alii. P. 599 l. 6 a c. pro $\mathfrak{P}$ l. P; ibid. l. 5 a c. pro $\mathfrak{Q}$ l. Q. P. 607 l. 6 pro λg l. λh. P. 608 l. 8. del. $b(f, k)$. Ib. l. 17 pro $d(f, g)$ l. $d(f, 1)$. P. 616 l. 1 et 4 pro praec. l. 347. P. 619 l. 6 a c. pro a^{ti} l. α^{ti}. P. 630 l. 13 l. $\frac{1}{2}\sqrt{(4 + (4, 13) - 2(4, 3))}$. P. 632 l. $\pm 0{,}3612416662i$. P. 638 in valore ipsius $\mathfrak{T}$ pro $n = 13$ terminis $4x^4$ et $4xx$ signum $+$ praefigi debet. P. 646 l. 7 a c. post *positius* insere α, $\mathfrak{C}$, γ. P. 647 l. 5 a c. pro R'' l. R^2. P. 653 l. 4 pro $=$, [1] l. $=$ [λ],. P. 654 l. 2 numerator pro cot. ω esse debet $i(RR + 1)$.

Erratorum multitudinem lector beneuolus, qui quam difficile in huiusmodi scriptis a typothetis tali labori minus adsuetis auctore absente euitentur nouerit, benigne ignoscet, et si quae alia vel minoris momenti vel sensum non turbantia offenderit, facile corriget.

Gauss, Carl F.
Disquisitiones
arithmeticae ...
1801.