SECTIO SEXTA.

VARIAE DISQUISITIONUM PRAECEDENTIUM APPLICATIONES.

308.

Quam fertilis sit arithmetica sublimior veritatibus, quae in aliis quoque matheseos partibus usum praestent, pluribus iam passim locis addigitavimus; quasdam vero applicationes, quae expositionem ampliorem merentur, seorsim tractare non inutile duximus, non tam ut hoc argumentum, quo plura volumina facile impleri possent, exhauriatur, quam potius ut per aliqua specimina illustretur. In hacce quidem Sectione primo de resolutione fractionum in simpliciores agemus; dein de conversione fractionum communium in decimales; tum methodum novam exclusionis explicabimus, solutioni aequationum indeterminatarum secundi gradus inservientem; tandem methodos novas 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 hactenus innotuerunt, novis incrementis amplificare studebimus.

Resolutio fractionum in simpliciores.

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, unica vero tantum positiva minorque quam a dabitur; fieri autem potest etiam, ut y evadat negativus. Vix necesse erit monere, y etiam per congruentiam $ay\equiv m \pmod{b}$, atque x per aequationem $x=\frac{m-ay}{b}$ inveniri posse. — *E. g.* proposita fractione $\frac{3}{5}\frac{8}{7}$, erit 4 valor expr. $\frac{1}{1}\frac{8}{7} \pmod{7}$, unde $\frac{3}{5}\frac{8}{7}$ resolvitur in $\frac{4}{5}+\frac{2}{11}$.

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 resolvi potest, quarum denominatores sint a et bcd etc.; secunda iterum in duas denominatorum b et cd etc.; posterior rursus in duas et sic porro, unde tandem fractio proposita sub hanc formam redigetur

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\frac{\delta}{d}+\text{ etc.}$$

Numeratores α, β, γ, δ etc. manifesto positivos ac denominatoribus suis minores accipere licebit, praeter ultimum, qui reliquis determinatis non amplius est arbitrarius, atque etiam negativus 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 ut ε sit positivus ac minor quam e, k vero integer. Denique patet, a, b, c etc. ita accipi posse, ut sint vel numeri primi vel numerorum primorum potestates.

Ex. Fractio $\frac{3}{5}\frac{8}{7}\frac{1}{1}$, cuius denominator $=4.3.7.11$ hoc modo resolvitur in $\frac{1}{4}+\frac{40}{231}$; $\frac{40}{231}$ in $\frac{3}{7}-\frac{38}{77}$; $-\frac{38}{77}$ in $\frac{1}{11}-\frac{7}{11}$; unde, scribendo $\frac{4}{11}-1$ pro $-\frac{7}{11}$ fit $\frac{3}{5}\frac{8}{7}\frac{1}{1}=\frac{1}{4}+\frac{2}{3}+\frac{1}{7}+\frac{4}{11}-1$.

311.

Fractio $\frac{m}{n}$ *unico tantum modo* sub formam $\frac{\alpha}{a}+\frac{\beta}{b}+$ etc. $\mp k$ reduci potest, ita ut α, β etc. sint positivi ac minores quam a, b etc. scilicet supponendo

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\text{ etc. }\mp k=\frac{\alpha'}{a}+\frac{\beta'}{b}+\frac{\gamma'}{c}+\text{ etc. }\mp K$$

atque etiam α', $\mathfrak{b}'$ etc. positivos ac minores quam a, b etc., necessario erit $\alpha = \alpha'$, $\mathfrak{b} = \mathfrak{b}'$, $\gamma = \gamma'$ etc., $k = K'$. Multiplicando enim per $n = abc$ etc., patet fieri $m \equiv \alpha bcd$ etc. $\equiv \alpha' bcd$ etc. (mod. a), unde, quoniam bcd etc. ad a primus est, necessario $\alpha \equiv \alpha'$ adeoque $\alpha = \alpha'$, et perinde $\mathfrak{b} = \mathfrak{b}'$ etc., unde etiam sponte $k = K'$. Iam quum prorsus arbitrarium sit, cuiusnam denominatoris numerator primus supputetur, manifestum est, *omnes* numeratores ita investigari posse ut α in art. praec., puta $\mathfrak{b}$ per congruentiam $\mathfrak{b}acd$ etc. $\equiv m$ (mod. b), γ per hanc γabd etc. $\equiv m$ (mod. c) etc.; summa omnium fractionum sic inventarum vel propositae $\frac{m}{n}$ aequalis erit, vel differentia numerus integer $= k$, qua via simul confirmationem calculi nanciscemur. Ita in ex. art. praec. valores expr. $\frac{2}{3}\frac{3}{4}\frac{1}{1}$ (mod. 4), $\frac{2}{2}\frac{3}{3}\frac{1}{1}$ (mod. 3), $\frac{2}{1}\frac{3}{2}\frac{1}{1}$ (mod. 7), $\frac{3}{8}\frac{5}{4}\frac{1}{1}$ (mod. 11) statim suppeditant numeratores 1, 2, 1, 4 denominatoribus 4, 3, 7, 11 respondentes, summaque harum fractionum propositam unitate superare invenitur.

Conversio fractionum communium in decimales.

312.

Definitio. Si fractio communis in decimalem convertitur, seriem figurarum decimalium *) (excluso si quis adest numero integro), sive finita sit, sive in infinitum excurrat, fractionis *mantissam* vocamus, expressionem, alias tantummodo apud logarithmos usitatam, in significatione latiori accipientes. Ita *e. g.* fractionis $\frac{1}{8}$ mantissa est 125, mantissa fractionis $\frac{3}{16}$ 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 diversas mantissas habere, prout numeratores l, m secundum n 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 $\frac{10^\nu m}{n}$ invenitur rescindendo ν figuras primas mantissae ipsius $\frac{m}{n}$. Mantissa fractionis $\frac{1}{n}$ statim figura significativa (*i. e.* a cifra diversa) incipit, si n non > 10; si vero $n > 10$ ac nulli potestati ipsius 10 aequalis, multitudoque figurarum e quibus constat est k, primae $k-1$ figurae mantissae ipsius $\frac{1}{n}$ erunt cifrae atque demum sequens k^{ta} erit significativa. Hinc facile deducitur, si $\frac{l}{n}$, $\frac{m}{n}$ mantissas diversas habeant (*i. e.* si l, m sec. n incongrui), has certo in primis k figuris convenire non posse, sed saltem in k^{ta} discrepare debere.

*) Brevitatis causa disquisitionem sequentem ad systema vulgare decadicum restringimus, quum facile ad quodvis aliud extendi possit.

313.

Problema. *Dato denominatore fractionis $\frac{m}{n}$ atque primis k figuris ex ipsius mantissa, invenire numeratorem m, quem ipso n minorem supponimus.*

Sol. Considerentur illae k figurae tamquam numerus integer, qui per n multiplicetur, productumque per 10^k dividatur (sive k ultimae figurae resecentur). Si quotiens est integer (sive figurae resectae cifrae), ipse manifesto erit numerator quaesitus atque mantissa data completa; sin minus, numerator quaesitus erit integer proxime maior, sive ille quotiens unitate auctus, postquam figurae decimales sequentes reiectae sunt. Ratio huius regulae tam facile ex iis, quae ad finem art. praec. observavimus, cognoscitur, ut explicatione uberiori opus non sit.

Ex. Si constat, duas figuras primas mantissae fractionis, cuius denominator 23, esse 69, habemus productum $23.69 = 1587$, a quo duas ultimas figuras abiiciendo, unitatemque 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 observamus, mantissam fractionis $\frac{a}{p^\mu}$ (cuius numeratorem a per numerum primum p non divisibilem 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 obvia sunt, ut expositione non egeant.

Si vero p est alius numerus primus, $10^r a$ per p^μ numquam divisibilis erit, quantumvis magnus accipiatur r, unde sponte sequitur, mantissam fractionis $F = \frac{a}{p^\mu}$ necessario in infinitum progredi. Supponamus, 10^e esse potestatem infimam numeri 10, quae unitati secundum modulum p^μ congrua fit (Conf. Sectio III, ubi 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 man-

tissae fractionis F figuram primam, duas . . . e figuras primas resp., manifestum est, in hac mantissa post primas e figuras, neque prius, easdem iterum repeti. Has primas e figuras, e quibus infinities repetitis mantissa formata est, *periodum* huius mantissae sive fractionis F vocare possumus, patetque, magnitudinem periodi, *i. e.* multitudinem figurarum, 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 $\frac{2}{7}$ periodus 428571 *).

315.

Simulac igitur fractionis alicuius periodus habetur, mantissa ad figuras quotcunque produci poterit. Porro patet, si fuerit $b \equiv 10^\lambda a \pmod{p^n}$, periodum fractionis $\frac{b}{p^n}$ oriri, si primae λ figurae periodi fractionis F (supponendo $\lambda < e$ 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^n sint congrui. Ita *e. g.* quum $6 \equiv 3.10^2 \pmod 7$, periodus fractionis $\frac{6}{7}$ statim e periodo fractionis $\frac{2}{7}$ fit 857142.

Quoties itaque pro modulo p^n numerus 10 est radix primitiva (artt. 57, 89), e periodo fractionis $\frac{1}{p^n}$ protinus deduci poterit periodus cuiusvis alius fractionis $\frac{m}{p^n}$ (cuius numerator m per p non divisibilis), tot figuras ab illa a laeva rescecando et ad dextram restituendo, quot unitates 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 primitiva, e periodo fractionis $\frac{1}{p^n}$ earum tantummodo fractionum periodi exscindi possunt, quarum numeratores alicui potestati ipsius 10 secundum p^n sunt congrui. Sit 10^e potestas infima ipsius 10 unitati secundum p^n congrua, $(p-1)p^{n-1} = ef$, atque talis radix primitiva r pro basi accepta, ut index numeri 10 fiat f (art. 71). In hoc itaque systemate numeratores fractionum, quarum periodi e periodo fractionis $\frac{1}{p^n}$ exscindi possunt, habebunt indices f, $2f$, $3f$ . . . $ef-f$; simili modo e periodo fractionis $\frac{r}{p^n}$ 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 derivari 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 $\frac{m}{p^n}$, in systemate ubi r pro basi acceptus est, $= i$ (quem supponimus minorem quam $(p-1)p^{n-1}$); fiat, dividendo per f, $i = \alpha f + \vartheta$, ita ut α, ϑ sint integri positivi (sive etiam 0) atque $\vartheta < f$; quo facto orietur periodus fractionis $\frac{m}{p^n}$ e periodo fractionis, cuius numerator r^ϑ (adeoque 1, quando $\vartheta = 0$), 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.

*) Cel. Robertson periodi initium et finem duobus punctis figurae primae et ultimae suprascriptis indicat (*Theory of circulating fractions*, *Philos. Trans.* 1769 *p.* 267), quod hic non necessarium putamus.

316.

Secundum haec principia pro omnibus denominatoribus formae p^n infra 1000 tabulam periodorum necessariarum construximus, quam integram sive etiam ulterius continuatam occasione data publici iuris faciemus. Hoc loco tabula III usque ad 100 tantum producta tamquam specimen sufficiat, cui explicatione vix opus erit. Pro iis denominatoribus, ubi 10 est radix primitiva, 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 primitiva adoptata est ut in tabula I. Hinc igitur periodus fractionis cuiusvis, cuius denominator in hac tabula continetur, adiumento praeceptorum art. praec. erui poterit, postquam numeratoris index per tabulam I est computatus. Ceterum pro denominatoribus tam parvis negotium aeque facile absque tabula I absolvere poterimus, si per divisionem vulgarem tot figuras initiales mantissae quaesitae computamus, quot per art. 313 necessariae sunt, ut ab omnibus aliis eiusdem denominatoris distingui possit (pro tabula III non plures quam 2), omnesque periodos denominatori dato respondentes perlustramus, usquedum ad illas figuras initiales perveniamus, quae periodi initium haud dubie indicabunt; monere tamen oportet, illas figuras etiam separatas esse posse, ita ut prima (vel plures) finem alicuius periodi constituant, reliqua vel reliquae eiusdem initium.

Ex. Quaeritur periodus fractionis $\frac{1}{19}$. Hic pro modulo 19 per tab. I

habetur ind. $12 = 2$ ind. $2 +$ ind. $3 = 39 \equiv 3 \pmod{18}$ (art. 57); quare quum pro hoc casu unica tantum periodus numeratori 1 respondens habeatur, huius tres primas figuras ad finem translocare oportet, unde fit periodus quaesita 631578947368421052. — Aeque facile periodi initium e duabus primis figuris 63 inventum fuisset.

Si periodus fractionis $\frac{8}{53}$ 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 ultimae, periodusque quaesita fit 849056603773. Figurae initiales 84 in hoc casu separatae sunt in tabula.

Observabimus adhuc, adiumento tabulae III etiam numerum inveniri posse, qui pro modulo dato (in ipsa sub denominatoris titulo contento) indici dato respondeat, ut in art. 59 polliciti sumus. Patet enim per praecc., inveniri 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 sive 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 potestatibus 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 convertere liceat, restat tantummodo, ut hae in summam uniantur. Ceterum vix opus erit monere, summae sic prodeuntis figuram ultimam iusto minorem evadere posse; manifesto autem defectus ad tot unitates adscendere nequit, quot fractiones particulares adduntur, unde hae ad aliquot figuras ulterius computare conveniet, 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 invenitur $F = 1 + \frac{1}{16} + \frac{1}{9} + \frac{1}{5} + \frac{37}{49} + \frac{5}{13} + \frac{7}{47} + \frac{33}{59}$, quae fractiones particulares, ita ut sequitur, in decimales convertuntur:

*) Haec fractio est una ex iis, quae ad radicem quadratam ex 23 quam proxime appropinquant, et quidem excessus est minor quam septem unitates in loco figurae decimalis vigesimae.

1	$= 1$		
$\frac{1}{16}$	$= 0,6875$		
$\frac{1}{9}$	$= 0,8$		
$\frac{1}{5}$	$= 0,4444444444$	4444444444	44
$\frac{37}{49}$	$= 0,4489795918$	3673469387	75
$\frac{5}{13}$	$= 0,3846153846$	1538461538	46
$\frac{7}{47}$	$= 0,1489361702$	1276595744	68
$\frac{33}{59}$	$= 0,8813559322$	0338983050	84
F	$= 4,7958315233$	1271954166	17

Defectus huius summae a iusto certo minor est quinque unitatibus in figura ultima vigesima secunda, quare viginti primae inde mutari nequeunt. Calculum ad plures figuras producendo, pro duabus figuris ultimis 17 prodit 1893936 . . . — Ceterum vel nobis non monentibus quisque videbit, hanc methodum, fractiones communes in decimales convertendi, ei potissimum casui accomodatam esse, ubi multae figurae decimales desiderentur; quando enim paucae sufficiunt, divisio vulgaris sive logarithmi aeque expedite plerumque adhiberi poterunt.

318.

Quum itaque resolutio talium fractionum, quarum denominatores e pluribus numeris primis diversis compositi sunt, ad eum casum iam reducta sit, ubi denominator est primus aut primi potestas: de illarum mantissis pauca tantum adiicimus. 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, unitati secundum denominatorem congruum, tandem pervenitur, 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 $2^\alpha 5^\beta N$, designante N numerum ad 10 primum, α et β numeros, quorum unus saltem non est 0, fractionis mantissa post primas α vel β figuras (prout α vel β maior) e periodis constare incipiet, cum periodis fractionum cum denominatore N respectu longitudinis convenienti-

bus; hoc facillime inde derivatur, quod illa fractio in duas alias cum denominatoribus $2^{\varepsilon}5^{\zeta}$ et N resolubilis est, quarum prior post primas α vel $\mathfrak{G}$ figuras abrumpetur. — Ceterum de hoc argumento multas alias observationes adiicere possemus, praesertim circa artificia, talem tabulam ut III quam citissime construendi, quas brevitatis caussa eo lubentius hoc loco supprimimus, quum plura huc pertinentia tum a cel. Robertson l. c., tum a cel. Bernoulli (*Nouv. Mém. de l'Ac. de Berlin* 1771 *p.* 273) iam sint tradita.

Solutio congruentiae $xx \equiv A$ per methodum exclusionis.

319.

Congruentiae $xx \equiv A \pmod{m}$, quae convenit cum aequatione indeterminata $xx = A + my$, *possibilitatem* in Sect. IV (art. 146) ita tractavimus, ut nihil amplius desiderari posse videatur; respectu investigationis incognitae ipsius autem, iam supra (art. 152) observavimus, 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, ut 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 omnia observamus, sufficere, si ii tantummodo valores ipsius x habeantur, qui sint positivi atque non maiores quam $\frac{1}{2}m$, quum quivis alius horum alicui vel ipsi vel negative sumto secundum modulum m congruus sit; pro tali vero valore ipsius x valor ipsius y necessario inter limites $-\frac{A}{m}$ et $\frac{1}{2}m - \frac{A}{m}$ contentus erit. Methodus itaque, quae statim se offert, in eo consisteret, ut 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 parvus (*e. g.* infra 40), hoc tentamen tam breve est, ut contractione vix opus sit; quando autem m est magnus, labor per *methodum exclusionis* sequentem, quantum lubet, abbreviari poterit.

320.

Sit E numerus arbitrarius integer ad m primus ac maior quam 2; omnia eius non-residua quadratica diversa (*i. e.* secundum E incongrua) haec a, b, c etc.;

denique radices congruentiarum

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c \text{ etc., sec. mod. } E$$

hae $\alpha, \mathfrak{b}, \gamma$ etc., quas omnes positivas ac minores quam E accipere licebit. Si itaque ipsi y valor alicui ex his numeris $\alpha, \mathfrak{b}, \gamma$ 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 $Et + \alpha$, $Et + \mathfrak{b}$, $Et + \gamma$ etc. contenti sint, sufficietque, tentamen de reliquis, quorum complexus fit Ω', instituisse. In illa operatione numero E nomen *excludentis* tribui potest.

Accipiendo autem pro excludente numerum idoneum alium E', prorsus simili modo invenientur tot numeri $\alpha', \mathfrak{b}', \gamma'$ etc., quot non-residua diversa quadratica habet, quibus y secundum modulum E' congruus esse nequit. Quare denuo ex Ω' eiicere licebit omnes numeros sub formis $E't + \alpha'$, $E't + \mathfrak{b}'$, $E't + \gamma'$ etc. contentos. Hoc modo continuari poterit, alios aliosque semper excludentes adhibendo, donec multitudo numerorum ex Ω tantum deminuta fuerit, ut non difficilius videatur, omnes superstites tentamini revera subiicere, quam exclusiones novas instituere.

Ex. Proposita aequatione $xx = 22 + 97y$, limites valorum ipsius y erunt $-\frac{2}{9}\frac{2}{7}$ et $24\frac{1}{2} - \frac{2}{9}\frac{2}{7}$, unde (quoniam inutilitas valoris 0 per se est obvia) Ω comprehendet numeros 1, 2, 3 . . . 24. Pro $E = 3$ habetur unicum non-residuum $a = 2$; unde fit $\alpha = 1$; excludendi sunt itaque ex Ω omnes numeri formae $3t + 1$; multitudo remanentium Ω' erit 16. Simili modo pro $E = 4$ habetur $a = 2$, $b = 3$, unde $\alpha = 0$, $\mathfrak{b} = 1$; 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 inveniuntur numeri formarum $5t$ et $5t + 3$; remanentque hi 2, 6, 11, 14. Excludens 6 removeret numeros formarum $6t + 1$ et $6t + 4$, hi vero (qui cum numeris formae $3t + 1$ conveniunt) 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, unde $x = \pm 33$.

321.

Quum operatio cum excludente E instituta e valoribus ipsius V, valoribus ipsius y in Ω respondentibus, omnes eos reliquet, qui sunt non-residua quadratica ipsius E, residua vero eiusdem numeri non attingat; facile intelligitur, usum excludentium E et $2E$ nihil differe, si E sit impar, quum in hoc casu E et $2E$ eadem residua et non-residua habeant. Hinc patet, si successive 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 removere, qui vel utriusque E, E' vel unius non-residua sint, eosque qui sint utriusque residua, remanere. Iam quum in eo casu, ubi E et E' divisorem communem non habent, illi numeri electi omnes sint non-residua, atque hi superstites residua producti EE', manifestum est, usum excludentis EE' in hoc casu omnino tantundem efficere, ac usum duorum E, E', adeoque illum, post hunc, superfluum fieri. Quare eos quoque excludentes omnes praeterire licebit, qui in duos factores inter se primos resolvi possunt, sufficietque iis uti, qui sunt vel numeri primi (ipsum m non metientes) vel primorum potestates. Denique manifestum est, post usum 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 cuiusvis inferioris p^ν 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^ν) atque non-residua ipsius p^μ; quare huiusmodi tantum non-residua ipsius p^μ pro a, b, c etc. accipere sufficiet.

322.

Computus numerorum $\alpha, \mathfrak{b}, \gamma$ etc. cuivis excludenti dato E respondentium multum contrahitur per observationes 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 $\alpha \equiv \mathfrak{A} + k$, $\mathfrak{b} \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k$ etc. Iam si ipsos $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. revera per solutionem illarum congruentiarum eruere oporteret, haec via ipsos $\alpha, \mathfrak{b}, \gamma$ etc. inveniendi nihilo utique brevior 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 valores expr. $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}$ etc. (mod. E), fieri non-residua diversa ipsius E, adeoque cum ipsis $\alpha, \mathfrak{b}, \gamma$ etc. omnino convenire, 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 0, convenient. 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 quae sunt residua ipsius p, *i. e.* numeros $p, 2p, 3p \ldots pp - p$ (scilicet omnes numeros infra pp praeter 0, qui per p sunt divisibiles); hinc vero facile perspicitur, pro $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. omnino eosdem numeros provenire 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 non-residuorum ipsius p in pp, unde pro $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc. provenient 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 $\equiv 3$ (mod. 4). Si post usum excl. 4 statuitur $E = 8$, habemus $\alpha = 5$, unde $\mathfrak{A}$ fit 5, 7, 1, 3, prout $m \equiv 1, 3, 5, 7$ (mod. 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, unde fit $\mathfrak{A} = 2^{\mu-1}$, $\mathfrak{B} = 3.2^{\mu-2}$ vel $= 2^{\mu-2}$ prout $m \equiv 1$ vel $\equiv 3$, quando vero μ est impar, ponendum est $\alpha = 5.2^{\mu-3}$, unde $\mathfrak{A}$ 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 excludentibus quot necessarii videntur numeri $\alpha, \mathfrak{b}, \gamma$ etc. sunt computati; sed de hac re sicut de aliis artificiis laborem contrahendi hic agere non licet.

Solutio aequationis indeterminatae $mxx + nyy = A$ per exclusiones.

323.

Omnes repraesentationes numeri dati A per formam binariam $mxx + nyy$.

sive solutiones aequationis indeterminatae $mxx+nyy=A$, in Sectione V methodo generali inuenire docuimus, cuius brevitas quoque nihil desiderandum relinquere videtur, si omnes valores expr. $\sqrt{-mn}$ secundum modulum A ipsum, et per suos factores quadratos divisum, iam habentur; hic autem pro eo casu, ubi mn est positivus, solutionem explicabimus, directa multo expeditiorem, si ad hanc illos valores antea computare oportet. Supponemus autem, numeros m, n et A esse positivos atque inter se primos, quum casus reliqui ad hunc facile possint reduci. Manifesto quoque sufficit, valores positivos ipsorum x, y eruere, quum reliqui inde per solam signorum mutationem deducantur.

Perspicuum est, x ita comparatum esse debere, ut $\frac{A-mxx}{n}$, pro quo scribemus V, positivus, integer, et quadratus evadat. Conditio prima requirit, ut x non sit maior quam $\sqrt{\frac{A}{m}}$: secunda iam per se locum habet, quando $n=1$, alioquin requirit, ut valor expr. $\frac{A}{m} \pmod{n}$ sit residuum quadraticum ipsius n, designandoque omnes valores diversos expr. $\sqrt{\frac{A}{m}} \pmod{n}$ 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, ut plures numeros, etiam hic *excludentes* vocandos, ad lubitum accipiamus, pro quibusnam valoribus ipsius x valor ipsius V fiat non-residuum qu. horum excludentium, investigemus, 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.

Si itaque excludens $E=p^\mu$ (includendo etiam eum casum ubi $\mu=1$, ubi p est numerus primus ipsum m non metiens, supponamusque *) p^ν esse summam potestatem eiusdem numeri primi per quam n sit divisibilis. Sint a, b, c etc. non-residua quadratica ipsius E (omnia, quando $\mu=1$; necessaria sive 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. $\pmod{Ep^\nu = p^{\mu+\nu}}$, quae sint α, β, γ etc., patetque facile, si pro quo valore ipsius x fiat $xx \equiv \alpha \pmod{Ep^\nu}$, valorem respondentem ipsius V fieri $\equiv a \pmod{E}$ sive non-residuum ipsius E, similiterque de numeris reliquis β, γ etc.; aeque facile vice versa perspicitur, si quis valor ipsius x producat $V \equiv a \pmod{E}$, pro eodem fieri $xx \equiv \alpha \pmod{Ep^\nu}$, adeoque omnes valores ipsius x, pro quibus xx nulli numerorum α, β, 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, β, γ etc. omnia residua quadratica ipsius Ep^ν, quae sint g, g', g'' etc., computentur valores expressionum $\sqrt{g}, \sqrt{g'}, \sqrt{g''}$ etc. $\pmod{Ep^\nu}$, 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, β, γ etc. nulla residua qu. ipsius Ep^ν inveniantur, 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, taliumve numerorum potestates tamquam excludentes adhibere liceat. Sit B valor expr. $\frac{A}{n} \pmod{m}$, patetque, V semper ipsi B secundum mod. m congruum fieri, quicunque valor pro x accipiatur, adeoque ad possibilitatem aequ. prop. necessario requiri, ut B sit residuum quadraticum ipsius m. Designante itaque p divisorem 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 divisibilis, ad aequ. prop. possibilitatem necessario requiritur, ut sit $B \equiv 1 \pmod{8}$, unde etiam V pro valore quocunque ipsius x fiet $\equiv 1 \pmod{8}$, et proin binarii potestates ad exclusionem non idoneae. — Quando au-

*) Brevitatis caussa duos casus, in quibus n per p est divisibilis ac non divisibilis, simul complectimur; in posteriori $\nu = 0$ ponere oportet.

tem m per 4 neque vero per 8 est divisibilis, 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); unde patet, valores pares reiiciendos esse, quando $C = 5$; impares, quando $C = 1$. — Denique quando m per 2, neque vero per 4 est divisibilis, sit ut ante 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) sive residuum cuiusvis 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), sive x accipiatur par sive impar, unde liquet, in his casibus aequationem prop. solutionem omnino non admittere.

Ceterum quum prorsus simili modo, ut hic valorem ipsius x per exclusiones invenire docuimus, etiam, mutatis mutandis, valorem ipsius y elicere possimus, methodum exclusionis ad problematis propositi solutionem duobus semper modis applicare licebit (nisi $m = n = 1$, ubi coincidunt), e quibus is plerumque est praeferendus, pro quo Ω terminorum multitudinem minorem continet, quod facile a priori aestimari poterit. — Denique vix necesse erit observare, si post aliquot exclusiones *omnes* numeri ex Ω abierint, hoc ut certum indicium impossibilitatis aequationis propositae esse considerandum.

325.

Ex. Proposita sit aequatio $3xx + 455yy = 10857362$, quam duplici modo solvemus, *primo* investigando 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 $a = 2$, $b = 3$, unde $\alpha = 0$, $\vec{6} = 3$, $g = 0$, 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 $a = 5$, unde $\alpha = 5$, qui est non-residuum ipsius 8; quare excludens 8 non potest adhiberi. Numerus 9 ex eadem ratione praetereundus est ut 3. Pro $E = 11$ numeri a, b etc. fiunt 2, 6, 7, 8, 10; $\nu = 0$; unde numeri $\alpha, \vec{6}$ 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 $11t$, $11t \pm 1$, $11t \pm 4$, 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 positivos ipsorum x, y admittit, $x = 1083$, $y = 127$, et $x = 1213$, $y = 119$.

Secundo. Si alteram eiusdem aequationis incognitam per exclusiones indagare placet, ponatur haec sub formam $455xx + 3yy = 10857362$, commutando x cum y, ut 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 divisibiles usque ad 154 incl., quorum multitudo est 103; applicando autem praecepta supra data invenitur, pro excl. 3; 4; 9; 11; 17; 19; 23 reiiciendos esse numeros formarum $9t \pm 4$; $4t$, $4t \pm 2$ sive omnes pares; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. His deletis superstites inveniuntur 119, 127, qui duo soli ipsi V valorem quadratum conciliant, easdemque solutiones suggerunt, ad quas supra pervenimus.

326.

Methodus praecedens iam per se tam expedita est, ut 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, ubi excludens est numerus primus impar ipsum A non metiens, sive 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, ϑ, γ etc. inveniuntur per congruentias $\alpha \equiv k + \mathfrak{A}$, $\vartheta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$ etc. (mod. p). Numeri $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. autem per artificium ei prorsus simile, quo in art. 322 usi sumus, sine congruentiarum computatione erui possunt, et vel cum omnibus non-residuis, vel cum omnibus residuis ipsius p (praeter 0) convenient, prout valor expr. $-\frac{m}{n}$ (mod. p), sive (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, ϑ etc. 8, 9, 11, 15, 16, 3, 5, 6; ex his residua sunt 8, 9, 15, 16, unde $\pm h$, h' etc. fiunt ± 5, 3, 7, 4. — Quibus saepius occasio est huiusmodi problemata solvendi, commoditati suae eximie consulent, si pro pluribus numeris primis p, valores ipsorum h, h' etc. singulis valoribus ipsorum k $(1, 2, 3 \ldots p-1)$ respondentes, in duplici suppositione (puta ubi $-mn$ est residuum et ubi non-residuum ipsius p) computent. Ceterum observamus adhuc, multitudinem numerorum h, $-h$, h' etc. semper esse $\frac{1}{2}(p-1)$, quando uterque numerus k et $-mn$ sit residuum vel uterque non-residuum ipsius p; $\frac{1}{2}(p-3)$, quando prior $R.$, posterior $NR.$; $\frac{1}{2}(p+1)$, quando prior $NR.$; posterior $R.$; sed demonstrationem huius theorematis, ne nimis prolixi fiamus, supprimere debemus.

Quod autem, *secundo*, eos casus attinet, ubi 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, omnibusque art. 324 signis retentis ponemus $n = n'p^\nu$, ita ut n' per p non sit divisibilis. Numeri a, b, c etc. erunt producta numeri $p^{\mu-1}$ vel in omnes numeros ipso p minores (praeter 0), 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 divisibilis, quia eadem proprietas in A suppo-

nitur; porro patet, omnes α, ϑ, 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. $\sqrt{k}\,(\mathrm{mod.}\, p^{\mu+\nu})$, qui per p non erit divisibilis, atque e valor huius $-\frac{n'}{2mr}\,(\mathrm{mod.}\, p)$, eritque $\alpha \equiv rr + 2erap^\nu\,(\mathrm{mod.}\, p^{\mu+\nu})$, unde facile colligitur, α esse residuum ipsius $p^{\mu+\nu}$, atque valores expr. $\sqrt{\alpha}\,(\mathrm{mod.}\, p^{\mu+\nu})$ fieri $\pm(r + eap^\nu)$; hinc omnes h, h', h'' etc. exprimentur per $r + uep^{\mu+\nu-1}$. 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 0), puta quando μ par; *vel* in omnia non-residua ipsius p infra hunc limitem, quando μ impar atque eRp sive, quod hic eodem redit, quando $-2mrn'Rp$; *vel* in omnia residua (praeter 0), 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 observare debemus, quamvis aequationem $axx + 2bxy + cyy = M$, in qua $bb - ac$ negativus $= -D$, facile ad eam formam, quam in praecc. consideravimus, reduci posse. Designando enim divisorem communem maximum numerorum a, b per m, et ponendo

$$a = ma', \quad b = mb', \quad \tfrac{D}{m} = a'c - mb'b' = n, \quad a'x + b'y = x'$$

aequ. illa manifesto aequivalet huic $mx'x' + nyy = a'M$, quae per praecepta supra tradita solvi poterit. Ex huius autem solutionibus eae tantum erunt retinendae, in quibus $x' - b'y$ per a' fit divisibilis, sive unde x valores integros nanciscitur.

Alia methodus congruentiam $xx \equiv A$ solvendi pro eo casu, ubi A est negativus.

327.

Quemadmodum solutio directa aequationis $axx + 2bxy + cyy = M$ in Sect. V contenta valores expr. $\sqrt{(bb - ac)}\,(\mathrm{mod.}\, M)$ notos supponit: ita vice versa pro eo casu, ubi $bb - ac$ est negativus, 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 compo-

situs esset, adhuc incognitos; si enim constaret, numerum primum p ipsum M metiri, atque esse $M = p^{\mu}M'$, ita ut 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. $\sqrt{-D}(\mathrm{mod.}\,M)$, ubi D et M positivi supponuntur, atque M sub forma divisorum 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 positivas atque proprie primitivas, *secundo*, omnes ad idem genus pertinere, cuius *character* ex indole numeri M, *i. e.* ex ipsius relationibus ad singulos divisores primos ipsius D (insuperque ad 4 aut 8, quando hae sunt necessariae) facile cognosci possit (art. 230). Quum suppositum sit, M contineri sub forma divisorum ipsius $xx+D$, a priori certi esse possumus, huic characteri necessario genus pos. pr. pr. formarum determ. $-D$ respondere, etiamsi forsan expressioni $\sqrt{-D}(\mathrm{mod.}\,M)$ 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, ut plures classes in $\mathfrak{G}$ inter se, adeoque cum eadem in G identicae sint, et quando G unicam classem continet, certo omnes in $\mathfrak{G}$ cum hac convenient. Quare si e classibus C, C', C'' etc. formae (simplissimae) f, f', f'' etc. eliguntur, (una e singulis): e singulis classibus in $\mathfrak{G}$ una 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 una est $x = m$, $y = n$, altera erit $x = -m$, $y = -n$; unicus casus excipi debet, ubi $D = 1$, in quo quatuor repraesentationes dabuntur (v. art. 180).

Ex his colligitur, si omnes repraesentationes numeri M per singulas formas f, f', f'' etc. investigentur (per methodum indirectam in praecc. traditam), atque

hinc valores expr. $\sqrt{-D}(\mathrm{mod.}\,M)$, 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 observationes 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 divisorem communem μ habent (quod tunc tantummodo accidere potest, ubi $\mu\mu$ metitur ipsum M, certoque accidet, quando $-D \mathrm{R} \frac{M}{\mu\mu}$): hae ad institutum praesens omnino negligi debent, etsi alio respectu utiles esse possint.

II. Ceteris paribus labor manifesto eo facilior erit, quo minor est multitudo classium f, f', f'' etc., adeoque brevissimus, quando D est unus e 65 numeris in art. 303 traditis, pro quibus in singulis generibus unica 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 positivus. *Tales* itaque repraesentationes diversae semper valoribus diversis expr. $\sqrt{-D}(\mathrm{mod.}\,M)$ respondent, unde multitudo omnium valorum diversorum multitudini omnium talium repraesentationum prodeuntium aequalis erit (semper excipiendo casum $D = 1$, ubi illa huius semissis erit).

IV. Quoniam, simulac alter duorum valorum oppositorum $+r$, $-r$, cognitus est, alter sponte innotescit, operationes adhuc aliquantum abbreviari 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 unam, alteram negligendo, e qua valores iis, quos prior suppeditavit, oppositos resultare iam absque calculo praevidere licet. Quando autem C est anceps, ambo valores r et $-r$ simul inde emergent; puta, si ex C forma 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, ubi $D=1$, una tantum classis omnino datur, e qua formam $xx+yy$ electam esse supponere licebit. Quodsi valor r ex repraesentatione $x=m$, $y=n$ provenit, 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 unicam discerptionem constituunt, una sufficit, si modo valori inde resultanti oppositum associemus.

VI. Valor expr. $\sqrt{-D}\,(\mathrm{mod.}\,M)$, ad quem repr. haec $M=amm+2bmn+cnn$ pertinet, per art. 155 est $\mu(mb+nc)-\nu(ma+nb)$ sive numerus quicunque huic secundum M congruus, ipsis μ, ν ita acceptis, ut fiat $\mu m+\nu n=1$. Designando itaque talem valorem per v, erit

$$mv\equiv\mu m(mb+nc)-\nu(M-mnb-nnc)\equiv(\mu m+\nu n)(mb+nc)\equiv mb+nc\,(\mathrm{mod.}\,M)$$

Hinc patet, v esse valorem expr. $\frac{mb+nc}{m}\,(\mathrm{mod.}\,M)$; similique modo invenitur, v esse valorem expr. $-\frac{ma+nb}{n}\,(\mathrm{mod.}\,M)$. Hae formulae saepenumero ei, ex qua deductae fuerunt praeferendae sunt.

328.

Exempla. I. Quaeruntur omnes valores expr. $\sqrt{-1365}\,(\mathrm{mod.}\,5428681=M)$; numerus M hic est $\equiv 1, 1, 1, 6, 11\,(\mathrm{mod.}\,4, 3, 5, 7, 13)$ adeoque sub forma divisorum ipsorum $xx+1$, $xx+3$, $xx-5$, et sub forma non-divisorum ipsorum $xx+7$, $xx-13$, et proin sub forma divisorum ipsius $xx+1365$ contentus; characterque generis, in quo classes $\mathfrak{G}$ reperientur, erit $1,4$; $R3$; $R5$; $N7$; $N13$. In hoc genere unica classis continetur, e qua eligimus formam $6xx+6xy+229yy$; ut omnes repraesentationes numeri M per hanc inveniantur, ponemus $2x+y=x'$, unde fieri debebit $3x'x'+455yy=2M$. Haec aequatio quatuor solutiones admittit, in quibus y est positivus, puta $y=127$, $x'=\pm 1083$, $y=119$, $x'=\pm 1213$. Hinc prodeunt quatuor solutiones aequ. $6xx+6xy+229yy=M$, in quibus y positivus,

x	478	-605	547	-666
y	127	127	119	119

Solutio prima dat pro v valorem expr. $\frac{30617}{478}$ sive $-\frac{3249}{127}\,(\mathrm{mod.}\,M)$, unde invenitur 2350978; secunda producit valorem oppositum -2350978; tertia hunc 2600262, quarta oppositum -2600262.

II. Si quaerendi sunt valores expr. $\sqrt{-286}\,(\mathrm{mod.}\,4272943=M)$, character generis, in quo classes $\mathfrak{G}$ contentae sunt, invenitur $1\,et\,7, 8$; $R11$; $R13$; quare erit genus principale, in quo tres classes continentur, per formas $(1, 0, 286)$, $(14, 6, 23)$, $(14, -6, 23)$ exhibitae; ex his tertiam, utpote secundae oppositam negligere licet. Per formam $xx+286yy$ duae repraesentationes numeri M inveniuntur, in quibus y positivus, puta $y=103$, $x=\pm 1113$, unde prodeunt valores expr. propositae hi 1493445, -1493445. Per formam $(14, 6, 23)$ autem M non repraesentabilis invenitur, unde concluditur, praeter duos valores inventos alios non dari.

III. Proposita expr. $\sqrt{-70}\,(\mathrm{mod.}\,997331)$, classes $\mathfrak{G}$ contentae esse debebunt in genere, cuius character $3\,et\,5, 8$; $R5$; $N7$; in hoc unica classis reperitur, cuius forma repraesentans haec $(5, 0, 14)$. At calculo instituto invenitur, numerum 997331 per formam $(5, 0, 14)$ non esse repraesentabilem, quamobrem -70 necessario erit non-residuum qu. illius numeri.

Duae methodi, numeros compositos a primis dignoscendi, illorumque factores investigandi.

329.

Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resolvendi, ad gravissima ac utilissima totius arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupavisse, tam notum est, ut 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, ut iam pro numeris talibus, qui tabularum a viris meritis constructarum limites non excedunt, *i. e.* pro quibus methodi artificiales supervacuae 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 ulterius continuatum iri sperare licet, in plerisque casibus vulgo occurrentibus utique 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, ut omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur. Propter has rationes non

dubitamus, quin duae methodi sequentes, quarum efficaciam ac brevitatem longa experientia confirmare possumus, arithmeticae amatoribus haud ingratae sint futurae. Ceterum in problematis natura fundatum est, ut methodi *quaecunque* continuo prolixiores evadant, 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 tractati 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 usum vocentur, semper utilissimum est, divisionem numeri cuiusque propositi per aliquot numeros primos minimos tentare; puta per 2, 3, 5, 7 etc. usque ad 19 aut adhuc ulterius, non solum, ne poeniteat, talem numerum, quando divisor est, per methodos subtiles ac artificiosas eruisse, qui multo facilius per solam divisionem inveniri potuisset*), sed etiam, quod tunc, ubi nulla divisio successit, applicatio methodi secundae *residuis* ex illis divisionibus ortis magno cum fructu utitur. Ita *e. g.* si numerus 314159265 in factores suos resolvendus est, divisio per 3 bis succedit, posteaque etiam divisiones per 5 et 7, unde habetur $314159265 = 9.5.7.997331$, sufficitque numerum 997331, qui per 11, 13, 17, 19 non divisibilis invenitur, examini subtiliori subiicere. Similiter proposito numero 43429448, factorem 8 auferemus, methodosque magis artificiales ad quotientem 5428681 applicabimus.

330.

Fundamentum METHODI PRIMAE est theorema, *quemvis numerum positivum seu negativum, qui alius numeri M residuum quadraticum sit, etiam residuum cuiusvis divisoris ipsius M esse.* Vulgo notum est, si M per nullum numerum primum infra $\sqrt{M}$ divisibilis 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* (ipsorumve potestatibus) compositum esse, vel *unum* tantum alium factorem primum maiorem quam $\sqrt{M}$ implicare posse, qui invenitur, dividendo ipsum M per p, q etc., quoties licet. Designando itaque complexum omnium numerorum primorum infra $\sqrt{M}$ (exclusis iis, per quos divisio frustra iam tentata est) per Ω, manifesto

*) Eo magis, quod inter sex numeros, generaliter loquendo, vix *unus* per omnes 2, 3, 5 ... 19 non divisibilis reperitur.

sufficit, si omnes divisores 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 divisor 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 ipsius M, e numeris primis in Ω post primum exclusionem relictis iterum eos excludere poterimus, quorum $NR.$ 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 eveniret, quando rr' esset quadratum). Si adhuc alia residua ipsius M noti sunt, r'', r''' etc., quae omnia a reliquis sunt independentia*), cum singulis exclusiones similes institui possunt, per quas multitudo numerorum in Ω rapidissime diminuetur, ita ut mox vel omnes deleti sint, in quo casu M certo erit numerus primus, vel tam pauci restent (inter quos omnes divisores primi ipsius M, si quos habet, manifesto reperientur), ut divisio per ipsos nullo negotio tentari possit. Pro numero millionem non multum superante plerumque sex aut septem; pro numero ex octo aut novem figuris constante, novem aut decem exclusiones abunde sufficient. Duo iam sunt, de quibus agere oportebit, *primo* quomodo residua ipsius M idonea et satis multa inveniri possint, *deinde* quo pacto exclusionem ipsam commodissime perficere liceat. Sed ordinem harum quaestionum invertemus, 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 divisibilem supponere licet), ab iis, quorum non-residuum est, sive divisores expr. $xx - r$ a non-divisoribus distinguere, in Sect. IV copiose docuimus, scilicet 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 parvus, exclusiones adiumento harum formularum

*) Si productum e numeris quotcunque r, r', r'' etc. quadratum est: quisque ipsorum *e. g.* r erit residuum cuiusvis numeri primi (nullum ex ipsis metientis), qui reliquorum r', r'' etc. residuum est. Ut igitur residua quotcunque tamquam independentia considerari possint, nullum productum nec e binis, nec e ternis etc. quadratum esse oportet.

percommode perfici possunt; *e. g.* excludendi erunt 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 invenire, neque formularum applicatio pro valore magno ipsius r satis commoda sit, ingens lucrum est, laboremque exclusionis mirifice sublevat, si pro multitudine satis magna numerorum (r) per quadratum non divisibilium tum positivorum tum negativorum *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 ut ad institutum praesens utilitatem satis amplam praestet, numeri primi in margine positi (moduli) longe ulterius puta saltem usque ad 1000 aut ad 10000 continuati esse debent, praetereaque commoditas multum augetur, si in facie etiam numeri compositi et negativi recipiuntur, etsi hoc non sit absolute necessarium, ut e Sect. IV perspicuum est. Ad summum autem commoditatis fastigium usus talis tabulae evehetur, si singulae columellae verticales, e quibus constat, exsecantur lamellisque aut baculis (Neperianis similibus) agglutinantur, ita ut eae, quae in quovis casu sunt necessariae *i. e.* quae numeris r, r', r'' etc., residuis numeri propositi in factores resolvendi, respondent, separate examinari possint. Quibus iuxta tabulae columnam primam (quae modulos exhibet) *rite* positis, *i. e.* ita, ut loca singulorum baculorum eidem numero primo columnae primae respondentium cum hoc in directum iaceant, sive 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 convenient cum iis in columna prima, quibus in *omnibus* baculis adiacentibus lineolae respondent, reiicique debent omnes, quibus in *ullo* 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 usque ad 997 continuata esse debet, *i. e.* usque 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		—	—			—
			etc.			
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—			
			etc.			

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 usque ad 997 extensum ostendit, *omnino* nullum alium ex Ω remanere; divisione autem tentata, 997331 per 127 revera divisibilis invenitur. Hoc itaque modo ille numerus in factores primos 127×7853 resolutus habetur *).

Ceterum ex hac expositione abunde colligitur, praesertim utilia esse residua non nimis magna, aut saltem in factores primos non nimis magnos resolubilia, quum tabulae auxiliaris usus immediatus non ultra numeros in facie positos pateat, ususque mediatus tales tantum complectatur, qui in factores in tabula contentos resolvi possunt.

332.

Ad invenienda residua numeri dati M tres methodos diversas trademus, quarum expositioni duas observationes praemittimus, quarum adiumento e residuis minus idoneis simpliciora derivari possunt. *Primo*, si numerus akk per quadratum kk divisibilis (quod ad M primum esse supponitur) est residuum ipsius M, etiam a erit residuum; propter hanc rationem residua per magna

*) Auctor apparatum satis amplum tabulae hic descriptae, quem ad usum suum construendum curavit, publici iuris lubenter faceret, si paucitas eorum, quibus usui 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.

quadrata divisibilia aeque utilia sunt ac parva; omniaque residua per methodos sequentes suppeditata a fractoribus suis quadratis statim liberata supponemus. *Secundo* si duo pluresve numeri sunt residua, etiam productum ex ipsis residuum erit. Combinando hanc observationem 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, convenietque omnia statim in factores suos resolvere. Vis harum observationum melius per exempla usumque frequentem quam per praecepta percipietur.

I. Methodus simplicissima, iisque, qui per frequentem exercitationem iam aliquam dexteritatem sibi conciliaverunt, commodissima, consistit in eo, ut M aut generalius multiplum quodcunque ipsius M quomodocunque in duas partes decomponatur $kM = a + b$ (sive utraque sit positiva sive altera positiva altera negativa), quarum productum signo mutato erit residuum ipsius M; erit enim $-ab \equiv aa \equiv bb \pmod{M}$, adeoque $-ab \mathrel{R} M$. Numeri a, b ita accipiendi sunt, ut productum per quadratum magnum divisibile quotiensque vel parvus vel saltem in factores non nimis magnos resolubilis evadat, quod semper non difficile effici poterit. Imprimis commendandum est, ut pro a accipiatur vel quadratum, vel quadratum duplex, vel triplex etc. a numero M numero vel parvo vel in factores commodos resolubili discrepans. Ita *e. g.* invenitur $997331 = 999^2 - 2.5.67 = 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2 = 3.575^2 + 11.31.4^2 = 3.577^2 - 7.13.4^2 = 3.578^2 - 7.19.37 = 11.299^2 + 2.3.5.29.4^2 = 11.301^2 + 5.12^2$ 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 ultima 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 quivis characteristicus unius formae, puta m, etiam est numerus char. alterius, adeoque mA, mC,

mA', mC' omnes residua ipsius kM. Si itaque (a, b, a') est forma reducta determinantis positivi M aut generalius kM, atque (a', b', a''), (a'', b'', a''') etc. formae ex ipsius periodo, adeoque ipsi aequivalentes 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 evolvitur, iam supra erueramus.

III. Si C est classis quaecunque formarum det. neg. $-M$ sive generalius $-kM$, a principali diversa, ipsiusque periodus haec $2C$, $3C$ etc. (art. 307): classes $2C$, $4C$ etc. ad genus principale pertinebunt; hae vero $3C$, $5C$ etc. ad idem genus ut 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'). Evolutio periodi, *i. e.* formarum simplicissimarum in ipsius classibus, mira facilitate perficitur, quando a est valde parvus, praesertim quando est $= 3$, quod semper efficere licet, quando $kM \equiv 2 \pmod{3}$. Ecce initium periodi classis, in qua est forma $(3, 1, 332444)$

C	(3,	1, 332444)	$6C$ (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 sive (tollendo factores quadratos) 3.7.17, 13.79, 5.7.31, 17, e quorum combinatione apta cum octo residuis in II inventis facile eruuntur duodecim sequentia -2.3, 13, -2.7, 17, 37, -53, -5.11, 79, -83, -2.59, $-2.5.31$; 2.5.67; sex priora sunt eadem, quibus in art. 331 usi sumus. Adiici potuissent residua 19 et -29, si ea quoque in usum vocare voluissemus, quae in I reperta sunt; reliqua illic eruta ab iis quae hic evolvimus iam sunt dependentia.

333.

Methodus secunda, numerum datum M in factores resolvendi, petitur e consideratione valorum talis expr. $\sqrt{-D}\,(\mathrm{mod.}\,M)$, observationibusque 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 divisorum vel in forma non-divisorum ipsius $xx+D$ continetur, et in casu priori expressio $\sqrt{-D}\,(\mathrm{mod.}\,M)$ duos tantummodo valores diversos habebit, qui oppositi erunt.

II. Quando vero M est compositus, puta $= pp'p''$ etc., designantibus p, p', p'' etc. numeros primos (diversos 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 divisorum 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 $R \equiv -R$, unde divisor communis

maximus numeri M cum $R-R$ erit M, et 1 div. comm. max. ipsius M cum $R+R$; sed valores duo nec identici nec oppositi ut R et R' necessario unum pluresve numerorum p, p', p'' etc., neque vero secundum omnes, congrui erunt, et secundum reliquos $R \equiv -R'$; hinc illorum productum erit divisor communis maximus numerorum M et $R-R'$, productumque horum d. c. m. ipsorum M et $R+R'$. Hinc facile sequitur, si omnes divisores communes maximi ipsius M cum differentiis inter singulos valores expr. $\sqrt{-D}\,(\mathrm{mod.}\,M)$ 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 $\frac{m}{n}\,(\mathrm{mod.}\,M)$ reducat, ita ut denominator n ad M primus sit: ad institutum praesens ne necessarium quidem est, has ipsas computare. Nam div. comm. max. numeri M cum differentia inter R et R', qui cum $\frac{m}{n}$, $\frac{m'}{n'}$ conveniunt, manifesto etiam erit div. comm. max. ipsorum M et $nn'(R-R')$, sive ipsorum M et $mn'-m'n$, quippe cui $nn'(R-R')$ secundum modulum M est congruus.

334.

Applicatio observationum praecc. ad problema, de quo agimus, duplici modo institui potest; prior non solum decidet, utrum 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. Investigetur numerus negativus $-D$, 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 ut in methodo prace. opus est, ut D sit numerus parvus; sed calculus eo brevior erit, quo minor est multitudo classium formarum binariarum in singulis generibus pr. pr. det. $-D$ contentarum; quamobrem imprimis talia residua, quae inter 65 numeros art. 303 continentur, si quae se offerunt, opportuna erunt. Ita pro $M = 997331$ ex omnibus residuis negativis supra erutis hoc -102 maxime

idoneum esset. Eruantur omnes valores diversi expr. $\sqrt{-D}\,(\mathrm{mod.}\,M)$; quodsi duo tantum proveniunt (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, diversis, qui factores per methodum art. praec. erui poterunt. Utrum vero hi factores numeri primi sint an primorum potestates, tum per se facillimum erit dignoscere; tum etiam via ipsa, per quam valores expr. $\sqrt{-D}$ inveniuntur, omnes numeros primos, quorum potestas aliqua ipsum M metitur, sponte indicat; scilicet si M divisibilis est per quadratum numeri primi π, ille calculus certo etiam unam pluresve repraesentationes tales numeri M, $M = amm + 2bmn + cnn$, produxerit, in quibus divisor 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 divisorem communem habent, hoc certum indicium est, M per nullum quadratum divisibilem esse adeoque omnes p, p', p'' etc. numeros primos.

Ex. Per methodum supra traditam inveniuntur quatuor valores expr. $\sqrt{-408}\,(\mathrm{mod.}\,997331)$ cum valoribus harum $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$ convenientes; divisores communes maximi 997331 cum his $3.1664 - 113.2824$ et $3.1664 + 113.2824$ sive cum 314120 et 324104 eruuntur hi 7853 et 127, unde $997331 = 127.7853$, ut supra.

II. Accipiatur aliquis numerus negativus $-D$ talis, ut M contentus sit in forma divisorum ipsius $xx + D$; per se arbitrarium est, quis huiusmodi numerus eligatur, sed commoditatis caussa imprimis videndum est, ut multitudo classium in generibus det. $-D$ sit quam maxime parva. Ceterum inventio talis numeri nulli difficultati obnoxia est, si tentando adeatur; nam plerumque inter multitudinem considerabilem numerorum tentatorum pro totidem fere M in forma divisorum continetur, ac in forma non-divisorum. Quare maxime e re erit, tentamen a 65 numeris art. 303 inchoare (et quidem a maximis), et si eveniret, ut nullus idoneus esset (quod tamen generaliter loquendo inter 16384 casus semel tantum accidit), ad alios progredi, ubi classes binae in singulis generibus continentur. — Tunc investigentur valores expr. $\sqrt{-D}\,(\mathrm{mod.}\,M)$, et si qui inveniuntur, factores ipsius M prorsus eodem modo inde deducantur ut 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 invenitur in forma non-divisorum ipsorum $xx + 1848$, $xx + 1365$, $xx + 1320$, sed in forma divisorum ipsius $xx + 840$; pro valoribus expr. $\sqrt{-840}\,(\mathrm{mod.}\,997331)$ prodeunt expr. $\pm\frac{1272}{163}$, $\pm\frac{3285}{125}$, unde iidem factores deducuntur ut ante. — Si quis plura exempla desiderat, art. 328 consulat, ubi primum docet esse $5428681 = 307.17683$; secundum, 4272943 esse numerum primum; tertium, 997331 certe e pluribus primis compositum esse.

* * *

Ceterum limites huius operis praecipua tantum momenta utriusque methodi factores investigandi hic exsequi permiserunt; disquisitionem uberiorem una cum pluribus tabulis auxiliaribus aliisque subsidiis alii occasioni reservamus.

SECTIO SEPTIMA

DE

AEQUATIONIBUS CIRCULI SECTIONES DEFINIENTIBUS.

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 universae matheseos pars carere potest, summi geometrae recentiores industriam sagacitatemque suam tam assidue impenderunt, disciplinamque tam vastam inde efformaverunt, ut parum exspectari potuisset, ullam huius theoriae partem, nedum elementarem atque in limine quasi positam, gravium adhuc incrementorum capacem esse. Loquor de theoria functionum trigonometricarum, arcubus cum peripheria commensurabilibus respondentium, sive de theoria polygonorum regularium, cuius quam parva 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 abunde 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 brevitati consulentes, tum ut principia plane nova huius theoriae eo facilius intelligantur.

Disquisitio reducitur ad casum simplicissimum, ubi multitudo partium, in quas circulum secare oportet, est numerus primus.

336.

Designando circuli peripheriam sive 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 $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{etc.})P$, 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 primorum 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, ubi circulus in partes dividendus 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 derivari, et perinde ex illis per aequationem aeque altam functiones ad $\frac{mP}{p^3}$ pertinentes etc., ita ut, 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 evitare licet.

Aequationes pro functionibus trigonometricis arcuum, qui sunt pars aut partes totius peripheriae: reductio functionum trigonometricarum ad radices aequationis $x^n - 1 = 0$.

337.

Satis constat, functiones trigonometricas omnium angulorum $\frac{kP}{n}$, denotando per k indefinite omnes numeros 0, 1, 2 ... $n-1$, per radices aequationum n^{ti} gradus exprimi, puta *sinus* per radices huius (I)

$$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\tfrac{n.n-3}{1.2}x^{n-4} - \tfrac{1}{64}\tfrac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \pm \tfrac{1}{2^{n-1}}nx = 0$$

cosinus per radices huius (II)

$$x^n - \tfrac{1}{4}nx^{n-2} + \tfrac{1}{16}\tfrac{n.n-3}{1.2}x^{n-4} - \tfrac{1}{64}\tfrac{n.n-4.n-5}{1.2.3}x^{n-6} + \text{etc.} \pm \tfrac{1}{2^{n-1}}nx - \tfrac{1}{2^{n-1}} = 0$$

denique *tangentes* per radices huius (III)

$$x^n - \tfrac{n.n-1}{1.2}x^{n-2} + \tfrac{n.n-1.n-2.n-3}{1.2.3.4}x^{n-4} - \text{etc.} \pm nx = 0$$

Hae aequationes (quae generaliter pro quovis valore impari ipsius n valent, II vero pro pari quoque), ponendo $n = 2m+1$, facile ad gradum m^{tum} deprimuntur; scilicet I et III, dividendo partem a laeva 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 laeva per $x-1$ divisibilis, 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 $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{mP}{n}$. Ulteriores reductiones harum aequationum, pro eo quidem casu, ubi 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 brevitatis caussa i pro quantitate imaginaria $\sqrt{-1}$, radices aequationis $x^n - 1 = 0$ exhibentur per

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r,$$

ubi pro k accipiendi sunt omnes numeri 0, 1, 2 ... $n-1$. Quocirca quum sit $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, radices aequationis I exhibebuntur per $\frac{1}{2i}(r - \frac{1}{r})$ sive per $i\frac{1-rr}{2r}$; 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 investigationum ordinem interrumpere oporteat, sequens lemma hic praemittimus.

338.

Problema. *Data aequatione*

$$(W) \ldots z^m + Az^{m-1} + etc. = 0,$$

invenire aequationem (W'), cuius radices sint potestates λ^{tae} radicum aequationis (W), designante λ exponentem integrum positivum datum.

Sol. Designatis radicibus aequationis W per a, b, c etc., radices aequ. W' esse debebunt $a^\lambda, b^\lambda, c^\lambda$ etc. Per theorema notum Newtonianum e coëfficientibus aequ. W invenire licet aggregata quarumlibet potestatum radicum a, b, c etc. Quaerantur itaque summae

$$a^\lambda + b^\lambda + c^\lambda + \text{etc.},\ a^{2\lambda} + b^{2\lambda} + c^{2\lambda} \text{ etc. etc. usque ad } a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{etc.}$$

unde via inversa 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 evadere. 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) unicam radicem realem implicat, $x = 1$; $n-1$ reliquae, quas aequatio

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$$

complectitur, omnes sunt imaginariae; harum complexum per Ω, functionemque

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 \text{ per } X$$

denotabimus. Si itaque r est radix quaecunque ex Ω, erit $1 = r^n = r^{2n}$ etc., et generaliter $r^{en} = 1$ pro quovis valore integro ipsius e, positivo seu negativo; 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, ut fiat $(\lambda - \mu)\nu \equiv 1 \pmod n$, unde $r^{(\lambda-\mu)\nu} = r$, adeoque $r^{\lambda-\mu}$ certo non $= 1$. Porro patet, quamvis 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 diversae, 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 convenire cum $r^e, r^{2e}, r^{3e} \ldots r^{(n-1)e}$, si e sit integer quicunque per n non divisibilis, positivus seu negativus. Erit itaque

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$$

unde

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1, \text{ et } 1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

Duas radices tales ut 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 ut angulus ω vel angulo $\frac{P}{n}$ vel alicui multiplo eius sit aequalis.

340.

Quoniam itaque, una 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 ut λ sit vel 0, vel positivus et $< n$. Designando itaque per $\varphi(t, u, v \ldots)$ 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., $\varphi(a, b, c \ldots)$ sub formam

$$A + A'r + A''rr + A'''r^3 + \ldots + A^\nu r^{n-1}$$

reduci posse, ita ut coëfficientes A, A' etc. (e quibus etiam aliqui deesse adeoque $= 0$ fieri possunt) sint quantitates determinatae, insuperque omnes hos coëfficientes integros fieri, si omnes coëfficientes determinati in $\varphi(t, u, v \ldots)$, *i. e.* omnes

h sint integri. Quodsi vero postea pro $t, u, v \ldots$ substituuntur $aa, bb, cc \ldots$ resp., quaevis pars ut $ht^\alpha u^\beta v^\gamma \ldots$, quae antea reducebatur ad r^λ, nunc fiet $r^{2\lambda}$; unde facile concluditur, fieri

$$\varphi(aa, bb, cc \ldots) = A + A'rr + A''r^4 + A'''r^6 + \ldots + A^\nu r^{2n-2}$$

Perinde erit generaliter, pro valore quocunque integro ipsius λ,

$$\varphi(a^\lambda, b^\lambda, c^\lambda \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \ldots + A^\nu r^{(n-1)\lambda}$$

quae propositio maximi est momenti, fundamentumque disquisitionum sequentium constituit. — Hinc sequitur etiam

$$\varphi(1, 1, 1 \ldots) = \varphi(a^n, b^n, c^n \ldots) = A + A' + A'' + \ldots + A^\nu$$

nec non

$$\varphi(a, b, c \ldots) + \varphi(aa, bb, cc \ldots) + \varphi(a^3, b^3, c^3 \ldots) + \ldots + \varphi(a^n, b^n, c^n \ldots) = nA$$

quae itaque summa semper fit integra per n divisibilis, quando omnes coëfficientes determinati in $\varphi(t, u, v \ldots)$ sunt integri.

Theoria radicum aequationis $x^n - 1 = 0$ (ubi supponitur, n esse numerum primum).
Omittendo radicem 1, reliquae (Ω) continentur in aequatione $X = x^{n-1} + x^{n-2} + etc. + x + 1 = 0$.
Functio X resolvi nequit in factores inferiores, in quibus omnes coëfficientes sint rationales.

344.

THEOREMA. *Si functio X per functionem inferioris gradus*

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \ldots + Kx + L$$

est divisibilis, coëfficientes $A, B \ldots L$ omnes integri esse nequeunt.

Dem. Sit $X = PQ$, atque $\mathfrak{P}$ complexus radicum aequationis $P = 0$, $\mathfrak{Q}$ complexus radicum aequationis $Q = 0$, ita ut 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 $x^\lambda + \frac{K}{L}x^{\lambda-1} + \text{etc.} + \frac{A}{L}x + \frac{1}{L} = 0$ 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 $\mathfrak{P}$ convenit 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 positivum 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 $P, P', P'' \ldots P^\nu$, quos obtinent statuendo $x = 1$, resp. $p, p', p'' \ldots p^\nu$, tunc per ante dicta p erit quantitas positiva et prorsus simili ratione etiam p', p'' etc. positivae 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 divisibilis. Praeterea facile perspicietur, productum $PP'P'' \ldots$ 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 evaderent; 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 divisibilis. Quare suppositio consistere nequit.

II. Quando $\mathfrak{P}$ et $\mathfrak{R}$ non quidem coincidunt, attamen quasdam radices communes continent, sit $\mathfrak{T}$ harum complexus atque $T = 0$ aequatio, cuius radices sunt. Tunc T erit divisor communis maximus functionum P, R (ut e theoria aequationum constat). Manifesto autem binae semper radices in $\mathfrak{T}$ reciprocae erunt, unde per ante demonstrata omnes coëfficientes in T rationales esse nequeunt. Hoc vero certo eveniret, si omnes in P adeoque etiam omnes in R rationales essent, ut e natura operationis, divisiorem comm. max. investigandi 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 $\mathfrak{S}$ ullam radicem commu-

nem habet; omnes radices $\mathfrak{P}$ necessario reperientur in $\mathfrak{S}$, omnesque $\mathfrak{Q}$ in $\mathfrak{R}$, unde erit $P = S$ et $Q = R$. Quamobrem $X = PQ$ erit productum ex P in R *i. e.*

$$\text{ex } x^\lambda + Ax^{\lambda-1} \ldots + Kx + L \text{ in } x^\lambda + \tfrac{K}{L}x^{\lambda-1} \ldots + \tfrac{A}{L}x + \tfrac{1}{L},$$

unde 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 ultimum in X *i. e.* unitatem metiri deberet, necessario foret $= \pm 1$, unde $\pm n$ esset numerus quadratus. Quod quum hypothesi repugnet, suppositio consistere nequit.

Ex hoc itaque theoremate liquet, quomodocunque X in factores resolvatur, horum coëfficientes partim saltem irrationales fieri, adeoque aliter, quam per aequationem elevatam, determinari non posse.

Propositum disquisitionum sequentium declaratur.

342.

Propositum disquisitionum sequentium, quod paucis declaravisse haud inutile erit, eo tendit, ut X in factores continuo plures GRADATIM resolvatur, et quidem ita, ut horum coëfficientes per aequationes ordinis quam infimi determinentur, usque dum hoc modo ad factores simplices sive ad radices Ω ipsas perveniatur. Scilicet ostendemus, si numerus $n - 1$ quomodocunque in factores integros α, β, γ etc. resolvatur (pro quibus singulis numeros primos accipere licet), X in α factores $\frac{n-1}{\alpha}$ dimensionum resolvi posse, quorum coëfficientes per aequationem α^{ti} gradus determinentur; singulos hos factores iterum in β alios $\frac{n-1}{\alpha\beta}$ dimensionum adiumento aequationis β^{ti} gradus etc., ita ut designante ν multitudinem factorum α, β, γ etc. inventio radicum Ω ad resolutionem ν aequationum $\alpha^{\text{ti}}, \beta^{\text{ti}}, \gamma^{\text{ti}}$ etc. gradus reducatur. *E. g.* pro $n = 17$, ubi $n - 1 = 2.2.2.2$, quatuor aequationes quadraticas solvere 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 po-

sterum abbreviatione utemur. 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 sive $[1]$ 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 divisibilis est vel divisibilis.

Omnes radices Ω in certas classes (periodos) distribuuntur.

343.

Si, pro modulo n, g est numerus talis, qualem in Sect. III radicem primitivam 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 quivis numerus unius seriei congruum habebit in altera. Hinc sponte sequitur, radices $[1]$, $[g]$, $[gg]$ $\ldots$ $[g^{n-2}]$ cum Ω coincidere; et prorsus simili modo generalius

$$[\lambda],\ [\lambda g],\ [\lambda gg] \ldots [\lambda g^{n-2}] \text{ cum } \Omega$$

coincident, designante λ integrum quemcunque per n non divisibilem. Porro quum sit $g^{n-1} \equiv 1 \pmod n$, nullo negotio perspicietur, duas radices $[\lambda g^\mu]$, $[\lambda g^\nu]$ identicas vel diversas esse, prout μ, ν secundum $n-1$ congrui sint vel incongrui.

Si itaque G est alia radix primitiva, radices $[1]$, $[g] \ldots [g^{n-2}]$ etiam cum his $[1]$, $[G] \ldots [G^{n-2}]$ convenient, si ad ordinem non respicitur. Sed praeterea facile probatur, si e sit divisor ipsius $n-1$, atque ponatur $n-1 = ef$, $g^e = h$, $G^e = H$, etiam f numeros $1, h, hh \ldots h^{f-1}$ his $1, H, H^2 \ldots H^{f-1}$ secundum n congruos esse (sine respectu ordinis). Supponamus enim $G \equiv g^m \pmod n$ sitque μ numerus arbitrarius positivus et $< f$ atque ν residuum minimum ipsius $\mu\omega \pmod f$. Tunc erit $\nu e \equiv \mu\omega e \pmod{n-1}$, hinc $g^{\nu e} \equiv g^{\mu\omega e^*} \equiv G^{\omega e}$ $\pmod n$, sive $H^\omega \equiv h^\nu$, i. e. quivis 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 $[1]$, $[h]$, $[hh] \ldots [h^{f-1}]$ identicas esse cum his $[1]$, $[H]$, $[H^2] \ldots [H^{f-1}]$, generaliusque eodem modo facile perspicietur,

$$[\lambda],\ [\lambda h],\ [\lambda hh] \ldots [\lambda h^{f-1}] \text{ cum } [\lambda],\ [\lambda H],\ [\lambda H^2] \ldots [\lambda H^{f-1}]$$

convenire. *Aggregatum* talium f radicum $[\lambda]+[\lambda h]+$ etc. $+[\lambda h^{f-1}]$, quod, quum

non mutetur accipiendo pro g aliam radicem primitivam, tamquam independens a g considerandum est, per (f, λ) designabimus; earundem radicum *complexum* vocabimus *periodum* (f, λ), ubi 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 $n = 19$, ubi 2 est radix primitiva, periodus $(6, 1)$ constat e radicibus $[1]$, $[8]$, $[64]$, $[512]$, $[4096]$, $[32768]$, sive $[1]$, $[7]$, $[8]$, $[11]$, $[12]$, $[18]$. Similiter periodus $(6, 2)$ constat ex $[2]$, $[3]$, $[5]$, $[14]$, $[16]$, $[17]$. Periodus $(6, 3)$ cum praec. identica invenitur. Periodus $(6, 4)$ continet $[4]$, $[6]$, $[9]$, $[10]$, $[13]$, $[15]$.

Varia theoremata de periodis radicum Ω.

344.

Circa huiusmodi periodos statim se offerunt observationes sequentes:

I. Quum sit $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$ etc. $\pmod n$, 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) ullam radicem communem habent, manifesto identicae erunt. Quare fieri nequit, ut duae radices in aliqua periodo simul contineantur, in alia simili vero una earum tantum reperiatur; porro patet, si duae radices $[\lambda]$, $[\lambda']$ ad eandem periodum f terminorum pertineant, valorem expr. $\frac{\lambda'}{\lambda} \pmod n$ alicui potestati ipsius h congruum esse, sive supponi posse $\lambda' \equiv \lambda g^{\omega e} \pmod n$.

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 diversae erunt, patetque, quamvis aliam similem periodum (f, λ) cum harum aliqua coincidere, siquidem $[\lambda]$ ad Ω pertineat, i. e. si λ per n non divisibilis sit. Periodus $(f, 0)$ autem aut (f, kn) manifesto ex f unitatibus est composita. Aeque facile perspicitur,

*) Aggregatum in sequentibus etiam periodi valorem numericum vocare liceat, aut simpliciter periodum, ubi ambiguitas non metuenda.

si λ sit numerus quicunque per n non divisibilis, etiam complexum e periodorum (f, λ), $(f, \lambda g)$, $(f, \lambda gg) \ldots (f, \lambda g^{e-1})$ cum Ω convenire. — Ita *e.g.* pro $n = 19$, $f = 6$, Ω constat e tribus periodis $(6,1)$, $(6,2)$, $(6,4)$, ad quarum aliquam quaevis alia similis, praeter $(6,0)$ reducitur.

III. Si $n-1$ est productum e tribus numeris positivis a, b, c, manifestum est, quamvis periodum bc terminorum ex b periodis c terminorum compositam esse, puta (bc, λ) ex (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$, unde 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 diversae, 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 ut supra $n-1 = ef$; g radix primitiva pro modulo n, atque $h = g^e$, unde per praecedentia erit $(f, \lambda) = (f, \lambda h) = (f, \lambda hh)$ etc. Hinc productum quaesitum erit

$$= [\mu].(f, \lambda) + [\mu h].(f, \lambda h) + [\mu hh].(f, \lambda hh) + \text{etc.}$$

adeoque

$$\begin{array}{l} = [\lambda \quad +\mu] \quad +[\lambda h \ +\mu] \quad \ldots +[\lambda h^{f-1}+\mu] \\ +[\lambda h \ +\mu h] \ +[\lambda hh+\mu h] \quad \ldots +[\lambda h^f \ +\mu h] \\ +[\lambda hh+\mu hh]+[\lambda h^3 +\mu hh] \ldots +[\lambda h^{f+1}+\mu hh] \text{ etc.} \end{array}$$

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 convenire nullo negotio perspicitur, quum numeri $\lambda, \lambda', \lambda''$ 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), $(f, gg) \ldots (f, g^{e-1})$ conveniant, W ad formam sequentem reduci poterit

$$W = af+b(f, 1)+b'(f, g)+b''(f, gg)+\ldots+b^{\varepsilon}(f, g^{e-1})$$

ubi coëfficientes a, b, b' etc. erunt integri positivi (sive etiam quidam $= 0$): porro patet, productum ex $(f, k\lambda)$ in $(f, k\mu)$ tunc fieri

$$= af+b(f, k)+b'(f, kg)+\ldots+b^{\varepsilon}(f, kg^{e-1})$$

Ita *e.g.* pro $n = 19$ productum ex aggregato $(6,1)$ in se ipsum, sive 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 $cf+d(f, 1)\ldots+d^{\varepsilon}(f, g^{e-1})$ exhiberi posse, et coëfficientes c, d etc. integros ac positivos (sive $= 0$) evadere, insuperque pro valore quocunque integro ipsius k fieri

$$(f, k\lambda).(f, k\mu).(f, k\nu) = cf+d(f, k)+d'(f, kg)+\text{etc.}$$

Perinde hoc theorema ad producta e periodis similibus quotcunque extenditur nihilque interest, sive hae periodi omnes diversae sint, sive partim aut cunctae identicae.

IV. Hinc colligitur, si in functione quacunque algebraica rationali integra $F = \varphi(t, u, v \ldots)$ 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 $A + B(f, k) + B'(f, kg) + \text{etc.}$

346.

THEOREMA. *Supponendo, λ esse numerum per n non divisibilem, et scribendo brevitatis ergo p pro (f, λ), quaevis alia similis periodus (f, μ), ubi etiam μ per n non divisibilis supponitur, reduci poterit sub formam talem*

$$\alpha + \beta p + \gamma pp + \ldots + \vartheta p^{e-1}$$

ita ut coëfficientes α, β etc. sint quantitates determinatae rationales.

Dem. Designentur ad abbreviandum periodi $(f, \lambda g)$, $(f, \lambda gg)$, $(f, \lambda g^3)$ etc. usque ad $(f, \lambda g^{e-1})$, quarum multitudo est $= e-1$, et cum quarum aliqua (f, μ) necessario conveniet, per p', p'', p''' etc. Habetur itaque statim aequatio

$$0 = 1 + p + p' + p'' + p''' + \text{etc.} \quad \ldots\ldots (\text{I})$$

evolvendo autem secundum praecepta art. praec. valores potestatum ipsius p usque ad $e-1^{\text{tam}}$, $e-2$ aliae tales promanabunt.

$$0 = pp + A + ap + a'p' + a''p'' + a'''p''' + \text{etc.} \ldots (\text{II})$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{etc.} \ldots (\text{III})$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{etc.} \ldots (\text{IV}) \quad \text{etc.}$$

ubi 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 divisibilis accipiatur. — Supponamus $(f, \mu) = p'$; facillime enim perspicietur, si (f, μ) cum alia periodo ex p'', p''' etc. conveniat, 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 ut prodeat aequatio talis (Z) ab ipsis libera

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}pp + \text{etc.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

quod ita fieri poterit, ut 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, ut in

theoremate enuntiatum est, determinari. Superest itaque, ut 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 ultra gradum $e-1^{\text{tum}}$ certo non ascendat, plures quam $e-1$ valores diversi ipsius p satisfacere nequeunt. At quum aequationes, e quibus Z deducta fuit, a λ sint independentes, liquet, etiam Z a λ non pendere, sive locum habere, quicunque integer per n non divisibilis 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, unde sponte sequitur, haec aggregata omnia inaequalia esse non posse, sed ad minimum duo inter se aequalia esse debere. Contineat unum e duobus talibus aggregatis aequalibus radices $[\zeta]$, $[\zeta']$, $[\zeta'']$ etc., alterum has $[\eta]$, $[\eta']$, $[\eta'']$ etc., supponamusque (quod licet), omnes numeros ζ, ζ', ζ'' etc., η, η', η'' etc. esse positivos et $< n$; manifesto omnes etiam diversi erunt, nullusque $= 0$. Designetur functio

$$x^\zeta + x^{\zeta'} + x^{\zeta''} + \text{etc.} - x^\eta - x^{\eta'} - x^{\eta''} - \text{etc.}$$

cuius terminus summus non ultra 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 ullum factorem communem haberet, divisor communis *maximus* functionum X, Y (quem certo usque ad $n-1$ dimensiones ascendere non posse iam inde patet, quod Y per x est divisibilis), omnes coëfficientes suos rationales haberet, ut e natura operationum, divisorem communem maximum duarum talium functionum investigandi, 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 $pp = 6 + 2p + p' + 2p''$, unde et ex $0 = 1 + p + p' + p''$ deducitur $p' = 4 - pp$, $p'' = -5 - p + pp$. Quare

$$(6,2) = 4 - (6,1)^2, \quad (6,4) = -5 - (6,1) + (6,1)^2$$
$$(6,4) = 4 - (6,2)^2, \quad (6,1) = -5 - (6,2) + (6,2)^2$$
$$(6,1) = 4 - (6,4)^2, \quad (6,2) = -5 - (6,4) + (6,4)^2$$

347.

THEOREMA. *Si* $F = \varphi(t, u, v \ldots)$ *est functio invariabilis**) *algebraica rationalis integra* 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*

$$A + A'[1] + A''[2] + \text{etc.} = W$$

reducitur: radices quae in hac expressione ad eandem periodum quamcunque f *terminorum pertinent, coëfficientes aequales habebunt.*

Dem. Sint $[p]$, $[q]$ duae radices ad unam eandemque periodum pertinentes, supponanturque p, q positivi et minores quam n, ita ut demonstrare oporteat, $[p]$ et $[q]$ in W eundem coëfficientem habere. Sit $q \equiv pg^{\nu e} \pmod{n}$; sint porro radices in (f, λ) contentae $[\lambda]$, $[\lambda']$, $[\lambda'']$ etc., ubi numeros $\lambda, \lambda', \lambda''$ etc. positivos et minores quam n supponimus; denique sint residua minima positiva numerorum $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$ etc., secundum modulum n, haec μ, μ', μ'' etc., quae manifesto cum numeris $\lambda, \lambda', \lambda''$ etc. identica erunt, etsi ordine transposito. Iam ex art. 340 patet,

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}] \ldots) = (\mathrm{I})$$

reduci ad

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{etc. aut ad } A + A'[\mathfrak{y}] + A''[\mathfrak{y}'] + \text{etc.} = (W')$$

designando per $\mathfrak{y}, \mathfrak{y}'$ etc. residua minima numerorum $g^{\nu e}$, $2g^{\nu e}$ etc. secundum modulum n, unde manifestum est, $[q]$ habere eundem coëfficientem in (W'), quem $[p]$ habeat in (W). Sed nullo negotio perspicitur, ex evolutione expressionis (I) idem provenire atque ex evolutione huius $\varphi([\mu], [\mu'], [\mu''] \text{ etc.})$, quoniam $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$ etc. (mod. n); haec vero expressio idem producit ac haec $\varphi([\lambda], [\lambda'], [\lambda''] \text{ etc.})$, quoniam numeri μ, μ', μ'' etc. ordine tantum ab his $\lambda, \lambda', \lambda''$ etc. discrepant, cuius in functione invariabili nihil interest. Hinc colligitur, W' omnino identicam fore cum W; quamobrem radix $[q]$ eundem coëfficientem in W habebit ut $[p]$. *Q. E. D.*

Hinc manifestum est, W reduci posse sub formam

*) Functiones invariabiles eas vocari constat, quibus omnes indeterminatae eodem modo insunt, sive clarius, quae non mutantur, quomodocunque indeterminatae inter se permutentur; cuiusmodi sunt *e. g.* summa omnium, productum ex omnibus, summa productorum e binis etc.

$$A + a(f, 1) + a'(f, g) + a''(f, gg) \ldots + a^{\varepsilon}(f, g^{\varepsilon-1})$$

ita ut 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

$$A + a(f, k) + a'(f, kg) + a''(f, kgg) + \text{etc.}$$

348.

Quum in aequatione quacunque

$$x^f - \alpha x^{f-1} + \mathfrak{G} x^{f-2} - \gamma x^{f-3} \ldots = 0$$

coëfficientes $\alpha, \mathfrak{G}, \gamma$ etc. sint functiones invariabiles 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, ubi omnes A, a, a' etc. erunt integri; praetereaque patet, aequationem, cuius radices sint radices in quacunque alia periodo $(f, k\lambda)$ contentae, ex illa derivari, 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 ε aequationes $z = 0$, $z' = 0$, $z'' = 0$ etc., quarum radices sint radices contentae in $(f, 1)$, in (f, g), (f, gg) etc., quamprimum ε aggregata $(f, 1)$, (f, g), (f, gg) etc. innotuerunt, aut potius quamprimum *unum* quodcunque eorum inventum est, quoniam per art. 346 ex uno omnia reliqua rationaliter deducere licet. Quo pacto simul functio X in ε 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 invenitur $= 2+2(6,1)+(6,2) = \gamma$; summa productorum e quaternis $= 3+(6,1)+(6,4) = \delta$; summa productorum e quinis $= (6,1) = \varepsilon$; productum ex omnibus $= 1$; quare aequatio

$$z = x^6 - \alpha x^5 + \delta x^4 - \gamma x^3 + \delta x x - \varepsilon x + 1 = 0$$

omnes radices in $(6,1)$ contentas complectitur. Quodsi in coëfficientibus α, δ, 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 δ, γ 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 brevitatis caussa pro (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc. q, q', q'' etc. erit

$$\alpha = q, \quad 2\delta = \alpha q - q', \quad 3\gamma = \delta q - \alpha q' + q'' \text{ etc.}$$

ubi producta e duabus periodis per art. 345 statim in summas periodorum sunt convertenda. Ita in exemplo nostro, scribendo pro $(6,1)$, $(6,2)$, $(6,4)$ resp. p, p', p'' fiunt $q, q', q'', q''', q'''', q'''''$ resp. $= p, p', p', p'', p', p''$; hinc

$$\alpha = p, \quad 2\delta = pp - p' = 6 + 2p + 2p''$$
$$3\gamma = (3+p+p'')p - pp' + p' = 6 + 6p + 3p'$$
$$4\delta = (2+2p+p')p - (3+p+p'')p' + pp' - p'' = 12 + 4p + 4p'' \text{ etc.}$$

Ceterum sufficit semissem coëfficientium tantum hoc modo computare; etenim non difficile probatur, ultimos ordine inverso primis vel aequales esse, puta ultimum $= 1$, penultimum $= \alpha$, antepenultimum $= \delta$ etc., vel ex iisdem resp. deduci, si pro $(f, 1)$, (f, g) etc. substituantur $(f, -1)$, $(f, -g)$ etc. sive $(f, n-1)$, $(f, n-g)$ etc. Casus prior locum habet, quando f est par; posterior, quando f impar; coëfficiens ultimus autem semper fit $= 1$. Fundamentum huius rei innititur theoremati art. 79; sed brevitatis caussa huic argumento non immoramur.

350.

THEOREMA. *Sit $n-1$ productum e tribus integris positivis α, δ, γ; constet periodus $(\delta\gamma, \lambda)$, quae est $\delta\gamma$ terminorum, ex δ periodis minoribus γ terminorum his (γ, λ), (γ, λ'), (γ, λ'') etc., supponamusque, si in functione δ indeterminatarum, similiter affecta ut in art. 347, 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. 345. IV reduci ad*

$$A + a(\gamma, 1) + a'(\gamma, g) \ldots + a^\varepsilon(\gamma, g^{\alpha\delta-\alpha}) \ldots + a^\eta(\gamma, g^{\alpha\delta-1}) = W$$

Tum dico, si F sit functio invariabilis, eas periodos in W, quae sub eadem periodo $\delta\gamma$ terminorum contentae sint, i. e. generaliter tales $(\frac{\nu}{\gamma}, g^\mu)$ et $(\gamma, g^{\alpha\nu+\mu})$, designante ν integrum quemcunque, coëfficientes eosdem habituras esse.

Dem. Quum periodus $(\delta\gamma, \lambda g^\alpha)$ identica sit cum hac $(\delta\gamma, \lambda)$, minores hae $(\gamma, \lambda g^\alpha)$, $(\gamma, \lambda' g^\alpha)$, $(\gamma, \lambda'' g^\alpha)$ etc., e quibus manifesto prior constat, necessario cum iis convenient, 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

$$W' = A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \ldots + a^\varepsilon(\gamma, g^{\alpha\delta}) \ldots + a^\eta(\gamma, g^{\alpha\delta+\alpha-1})$$
$$= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \ldots + a^\varepsilon(\gamma, 1) \ldots + a^\eta(\gamma, g^{\alpha-1})$$

quare quum haec expressio cum W convenire debeat, coëfficiens primus, secundus, tertius etc. in W (incipiendo ab a) necessario conveniet cum $\alpha+1^{\text{to}}$, $\alpha+2^{\text{to}}$, $\alpha+3^{\text{to}}$ etc., unde 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 convenire debere. *Q. E. D.*

Hinc manifestum est, W reduci posse ad formam

$$A + a(\delta\gamma, 1) + a'(\delta\gamma, g) \ldots + a^\varepsilon(\delta\gamma, g^{\alpha-1})$$

ubi 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 δ periodi γ terminorum in alia periodo $\delta\gamma$ terminorum, puta in $(\delta\gamma, \lambda k)$ contentae, quae manifesto erunt $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$ etc., valorem inde prodeuntem fore $A + a(\delta\gamma, k) + a'(\delta\gamma, gk) \ldots + a^\varepsilon(\delta\gamma, g^{\alpha-1}k)$.

Ceterum patet, theorema ad eum quoque casum extendi posse, ubi $\alpha = 1$, sive $\vec{6}\gamma = n-1$; scilicet hic *omnes* coëfficientes in W aequales erunt, unde W reducetur sub formam $A + a(\vec{6}\gamma, 1)$.

351.

Retentis itaque omnibus signis art. praec., manifestum est, singulos coëfficientes aequationis, cuius radices sunt $\vec{6}$ aggregata (γ, λ), (γ, λ'), (γ, λ'') etc., sub formam talem

$$A + a(\vec{6}\gamma, 1) + a'(\vec{6}\gamma, g) \ldots + a^{\varepsilon}(\vec{6}\gamma, g^{\alpha-1})$$

reduci posse, atque numeros A, a etc. omnes fieri integros; aequationem autem, cuius radices sint $\vec{6}$ periodi γ terminorum in alia periodo $(\vec{6}\gamma, k\lambda)$ contentae, ex illa derivari, si ubique in coëfficientibus pro qualibet periodo $(\vec{6}\gamma, \mu)$ substituatur $(\vec{6}\gamma, k\mu)$. Si igitur $\alpha = 1$, omnes $\vec{6}$ periodi γ terminorum determinabuntur per aequationem $\vec{6}^{\text{ti}}$ gradus, cuius singuli coëfficientes sub formam $A + a(\vec{6}\gamma, 1)$ rediguntur, *adeoque sunt quantitates cognitae*, quoniam $(\vec{6}\gamma, 1) = (n-1, 1) = -1$. Si vero $\alpha > 1$, coëfficientes aequationis, cuius radices sunt omnes periodi γ terminorum in aliqua periodo data $\vec{6}\gamma$ terminorum contentae, quantitates cognitae erunt, simulac valores numerici omnium α periodorum $\vec{6}\gamma$ terminorum innotuerunt. — Ceterum calculus coëfficientium harum aequationum saepe commodius instituitur, praesertim quando $\vec{6}$ non est valde parvus, si primo summae potestatum radicum eruuntur, ac dein ex his per theorema Newtonianum coëfficientes deducuntur, simili modo ut 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

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p''$$

Hinc

$$A = (18, 1) = -1$$

porro habetur

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'', \quad p'p'' = 3p + p' + 2p''$$

unde

$$B = 6(p + p' + p'') = 6(18, 1) = -6$$

denique fit

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$$

quare aequatio quaesita

$$x^3 + xx - 6x - 7 = 0$$

Utendo methodo altera habemus

$$p + p' + p'' = -1$$

$$pp = 6 + 2p + p' + 2p'', \quad p'p' = 6 + 2p' + p'' + 2p, \quad p''p'' = 6 + 2p'' + p + 2p'$$

unde

$$pp + p'p' + p''p'' = 18 + 5(p + p' + p'') = 13$$

similiterque

$$p^3 + p'^3 + p''^3 = 36 + 31(p + p' + p'') = 2$$

hinc per theorema Newtonianum eadem aequatio derivatur ut ante.

II. Quaeritur pro $n = 19$ aequatio, cuius radices sint aggregata $(2, 1)$, $(2, 7)$, $(2, 8)$. Quibus resp. per q, q', q'' designatis, invenitur

$$q + q' + q'' = (6, 1), \quad qq' + qq'' + q'q'' = (6, 1) + (6, 4), \quad qq'q'' = 2 + (6, 2)$$

unde, 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.

Disquisitionibus praecc. superstruitur solutio aequationis $X = 0$.

352.

Theoremata praecedentia cum consectariis annexis praecipua totius theoriae momenta continent, modusque valores radicum Ω inveniendi paucis iam tradi poterit.

Ante omnia accipiendus est numerus g, qui pro modulo n sit radix primitiva, residuaque minima potestatum ipsius g usque ad g^{n-2} secundum modulum n eruenda. Resolvatur $n-1$ in factores, et quidem, si problema ad aequationes gradus quam infimi reducere lubet, in factores primos; sint hi (ordine prorsus arbitrario) $\alpha, \beta, \gamma, \ldots \zeta$, ponaturque

$$\frac{n-1}{\alpha} = \beta\gamma\ldots\zeta = a, \quad \frac{n-1}{\alpha\beta} = \gamma\ldots\zeta = b, \text{ etc.}$$

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. praec. 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) quodvis aggregatum aequale statuendum sit, puta quaenam 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 quaevis 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, unde 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, unicam tantummodo radicem per huius resolutionem ernere 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 ut per n non sit divisibilis; quo facto etiam $[2]$, $[3]$ etc. radices determinatas indicabunt, unde etiam aggregata $(a, 1)$, (a, g) etc. quantitates determinatas designabunt. Quibus e tabulis sinuum levi tantum calamo computatis, puta ea praecisione, ut quae maiora quaeve minora sint decidi possit, nullum dubium superesse poterit, quibusnam signis singulae radices aequ. (A) sint distinguendae.

Quando hoc modo omnia α aggregata a terminorum inventa sunt, investigetur per art. praec. aequatio (B) β^{ti} gradus, cuius radices sint β aggregata b terminorum sub $(a, 1)$ contenta; coëfficientes huius aequationis omnes erunt quantitates cognitae. Quum adhuc arbitrarium sit, quaenam ex a β 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. Investigetur itaque una radix quaecunque aequationis (B) per eius resolutionem, statuatur $= (b, 1)$, deriventurque 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 β^{ti} gradus eruere, quarum radices sint resp. singula β 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 investigare: tunc vero simili modo ut 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; unum tamen, pro eo casu ubi $\beta = 2$, quod imprimis utile est, ac per exempla brevius quam per praecepta declarari poterit, in exemplis sequentibus cognoscere licebit.

Postquam hoc modo valores omnium $\alpha\beta$ aggregatorum b terminorum inventi sunt, prorsus simili modo hinc per aequationes γ^{ti} gradus omnia $\alpha\beta\gamma$ aggregata c terminorum determinari poterunt. Scilicet *vel unam* aequationem γ^{ti} gradus, cuius radices sint γ aggregata c terminorum sub $(b, 1)$ contenta, per art. 350 eruere, per eius resolutionem unam radicem quamcunque elicere et $= (c, 1)$ statuere, tandemque hinc per art. 346 omnia reliqua similia aggregata deducere oportebit; *vel* simili modo omnino $\alpha\beta$ aequationes γ^{ti} gradus evolvere, 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 ut 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; evolvendo 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 una eius radix quaecunque elicitur, hanc $= [1]$ statuere licebit, omnesque reliquae radices Ω per huius potestates

habebuntur. Si magis placet, etiam *omnes* radices illius aequationis per resolutionem erui, praetereaque per solutionem $\frac{x-1}{\zeta}=1$ aliarum aequationum ζ^{ti} gradus, quae resp. omnes ζ radices in singulis reliquis periodis ζ terminorum contentas exhibent, omnes reliquae radices Ω inveniri poterunt.

Ceterum patet, simulac prima aequatio (A) soluta sit, sive 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), sive postquam valores omnium $\alpha\delta$ aggregatorum b terminorum inventi sint, singulos illos factores iterum in δ, sive X in $\alpha\delta$ factores b dimensionum resolvi etc.

353.

Exemplum primum pro $n=19$. Quum hic fiat $n-1=3.3.2$, inventio radicum Ω ad solutionem duarum aequationum cubicarum uniusque quadraticae est reducenda. Hoc exemplum eo facilius intelligetur, quod operationes necessariae ad maximam partem in praecedentibus iam sunt contentae. Accipiendo pro radice primitiva 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 $(6,1)$, $(6,2)$, $(6,4)$, invenitur $x^3+xx-6x-7=0$, cuius una 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

$$x^3-(6,1)xx+((6,1)+(6,4))x-2-(6,2)=0$$

sive

$$x^3+1,2218761623xx-3,5070186441x-4,5070186441=0$$

cuius una radix elicitur $=-1,3545631433$, quam per $(2,1)$ exprimemus. Per methodum art. 346 autem inveniuntur aequationes sequentes, ubi brevitatis 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 evolvi possunt. Supponendo

$$[1]=\cos\tfrac{kP}{19}+i\sin\tfrac{kP}{19}$$

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., unde per aequationes notas pro cosinubus angulorum multiplicium eaedem formulae ut supra derivantur. — 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, *utra* harum radicum fiat $(2,7)$ et utra $(2,8)$, vel per calculum approximatum secundum formulas praecc., vel per tabulas sinuum tolletur, quae obiter tantum consultae ostendunt, fieri $(2,1) = 2\cos\omega$ ponendo $\omega = \frac{1}{17}P$, unde fieri oportet

$$(2,7) = 2\cos\tfrac{8}{17}P = 2\cos\tfrac{8}{17}P, \quad \text{et} \quad (2,8) = 2\cos\tfrac{16}{17}P = 2\cos\tfrac{1}{17}P$$

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, invenire licet, incertitudoque, quaenam radices illis aggregatis *resp.* aequales statuendae sint, prorsus eodem modo removebitur, ut 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 $= -0{,}6772815716 \pm 0{,}7357239107\,i$. Sedecim radices reliquae vel ex evolutione potestatum utriusvis harum radicum, vel e solutione octo aliarum similium aequationum deduci possunt, ubi in methodo posteriori vel per tabulas sinuum vel per artificium in ex. sq. explicandum decidi debebit, pro utra radice parti imaginariae signum positivum et pro utra negativum praefigendum sit. Hoc modo inventi sunt valores sequentes, ubi signum superius radici priori, inferius posteriori respondere supponitur:

$$\begin{aligned}
[1] \text{ et } [18] &= -0{,}6772815716 \pm 0{,}7357239107\,i \\
[2] \text{ et } [17] &= -0{,}0825793455 \mp 0{,}9965844930\,i \\
[3] \text{ et } [16] &= \;\;0{,}7891405094 \pm 0{,}6142127127\,i \\
[4] \text{ et } [15] &= -0{,}9863613034 \pm 0{,}1645945903\,i \\
[5] \text{ et } [14] &= \;\;0{,}5469481581 \mp 0{,}8371664783\,i \\
[6] \text{ et } [13] &= \;\;0{,}2454854871 \pm 0{,}9694002659\,i \\
[7] \text{ et } [12] &= -0{,}8794737512 \mp 0{,}4759473930\,i \\
[8] \text{ et } [11] &= \;\;0{,}9458172417 \mp 0{,}3246994692\,i \\
[9] \text{ et } [10] &= -0{,}4016954247 \pm 0{,}9157733267\,i
\end{aligned}$$

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 primitiva hic accipiemus numerum 3, cuius potestates residua minima sequentia secundum modulum 17 suppeditant:

$$\begin{aligned}
&0.1.2.\;3.\;4.5.\;6.\;7.\;8.\;9.10.11.12.13.14.15 \\
&1.3.9.10.13.5.15.11.16.14.\;8.\;7.\;4.12.\;2.\;6
\end{aligned}$$

Hinc emergunt distributiones sequentes complexus Ω in periodos duas octonorum, quatuor quaternorum, octo binorum terminorum:

$$\Omega = (16,1)\begin{cases}(8,1)\begin{cases}(4,\;1)\begin{cases}(2,\;1)\ldots[1],\,[16]\\(2,13)\ldots[4],\,[13]\end{cases}\\(4,\;9)\begin{cases}(2,\;9)\ldots[5],\,[\;9]\\(2,15)\ldots[2],\,[15]\end{cases}\end{cases}\\(8,3)\begin{cases}(4,\;3)\begin{cases}(2,\;3)\ldots[3],\,[14]\\(2,\;5)\ldots[8],\,[12]\end{cases}\\(4,10)\begin{cases}(2,10)\ldots[7],\,[10]\\(2,11)\ldots[6],\,[11]\end{cases}\end{cases}\end{cases}$$

Aequatio (A), cuius radices sunt aggregata $(8,1)$, $(8,3)$, per praecepta art. 351 invenitur haec $xx + x - 4 = 0$; huius radices computantur $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}5615528128$, et $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}5615528128$; priorem statuemus $= (8,1)$, unde 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 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 positivum tribuitur, et cuius valor numericus est $2{,}0494811777$, statuemus $= (4,1)$, unde sponte altera, ubi quantitas radicalis negative sumitur et cuius valor est $-0{,}4879283649$, 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, ubi ad abbreviandum pro $(4,1)$ scribitur p:

$$\begin{aligned}
(4,\;3) &= -\tfrac{1}{2} + 3p - \tfrac{1}{2}p^3 = 0{,}3441507314 \\
(4,10) &= \tfrac{3}{2} + 2p - pp - \tfrac{1}{2}p^3 = -2{,}9057035442
\end{aligned}$$

Eadem methodus etiam hanc formulam largitur $(4,9) = -1 - 6p + pp + p^3$, unde 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 $xx - (8,3)x - 1 = 0$, unde eius radices sunt $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{(4 + (8,3)^2)}$, sive $\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{(12 + 4(8,1) + 3(8,3))}$ et $\frac{1}{2}(8,3) - \frac{1}{2}\sqrt{(12 + 4(8,1) + 3(8,3))}$; dubium vero, *utram* radicem per $(4,3)$ et utram per $(4,10)$ exprimere oporteat, per artificium sequens, cuius mentionem in art. 352 iniecimus, tolletur. Evolvatur productum ex $(4,1) - (4,9)$ in $(4,3) - (4,10)$, unde emergere invenietur $2(8,1) - 2(8,3)$*); iam huius expressionis valor manifesto est positivus puta $= +2\sqrt{17}$, praetereaque etiam producti factor primus $(4,1) - (4,9)$ positivus est puta $= +\sqrt{(12 + 3(8,1) + 4(8,3))}$, quare necessario etiam alter factor $(4,3) - (4,10)$ positivus esse debebit, et proin $(4,3)$ radici *priori*, in qua signum positivum radicali praefigitur, et $(4,10)$ posteriori aequale statui. Ceterum hinc iidem valores numerici derivantur ut supra.

Cunctis aggregatis quatuor terminorum inventis, progredimur ad aggregata duorum terminorum. Aequatio (C), cuius radices sunt hae $(2,1)$, $(2,13)$, sub $(4,1)$ contentae, eruitur haec $xx - (4,1)x + (4,3) = 0$; huius radices sunt $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(-4(4,3) + (4,1)^2)}$ sive $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(4 + (4,9) - 2(4,3))}$: eam, ubi quantitas radicalis positive sumitur et cuius valor reperitur $= 1,8649144588$, statuimus $= (2,1)$, unde $(2,13)$ aequale fiet alteri, cuius valor $= 0,1845367189$. Si aggregata reliqua duorum terminorum per methodum art. 346 investigare 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 designatis tradidimus; puta $(2,2)$, (sive $(2,15)$), $= (2,1)^2 - 2$ etc. Si vero magis arridet, binas per resolutionem aequationis quadraticae computare, pro his $(2,9)$, $(2,15)$ invenitur aequatio $xx - (4,9)x + (4,10) = 0$, cuius radices evolvuntur $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{(4 + (4,1) - 2(4,10))}$; quo pacto vero signum ambiguum hic definire oporteat, simili modo decidetur ut supra. Scilicet per evolutionem producti $(2,1) - (2,13)$ in $(2,9) - (2,15)$ producitur $-(4,1) + (4,9) - (4,3) + (4,10)$, quod quum manifesto sit negativum, factor $(2,1) - (2,13)$ vero positivus, necessario $(2,9) - (2,15)$ negativus esse debebit, quocirca in expressione ante data signum superius positivum pro $(2,15)$, pro $(2,9)$ inferius negativum adoptandum erit. Hinc computatur $(2,9) = -1,9659461994$, $(2,15) = 1,4780178344$. — Perinde quum ex evolutione producti ex $(2,1) - (2,13)$ in $(2,3) - (2,5)$ prodeat $(4,9) - (4,10)$, adeoque quantitas positiva, factorem $(2,3) - (2,5)$ positivum esse concludimus; hinc simili calculo ut ante instituto invenitur

$$(2,3) = \tfrac{1}{2}(4,3) + \tfrac{1}{2}\sqrt{(4 + (4,10) - 2(4,9))} = 0,8914767116$$
$$(2,5) = \tfrac{1}{2}(4,3) - \tfrac{1}{2}\sqrt{(4 + (4,10) - 2(4,9))} = -0,5473259801$$

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 ut ad radices Ω ipsas descendamus. Aequatio (D), cuius radices sunt $[1]$ et $[16]$, prodit $xx - (2,1)x + 1 = 0$, unde radices $\frac{1}{2}(2,1) \pm \frac{1}{2}\sqrt{((2,1)^2 - 4)}$ aut potius $\frac{1}{2}(2,1) \pm i\sqrt{(4 - (2,1)^2)}$ sive $\frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{(2 - (2,15))}$; 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, ubi incertitudo de signis quantitatum radicalium per idem artificium tolli poterit ut in praecedentibus. Ita $[4]$ et $[13]$ sunt radices aequationis $xx - (2,13)x + 1 = 0$, adeoque $\frac{1}{2}(2,13) \pm \frac{1}{2}i\sqrt{(2 - (2,9))}$; per evolutionem producti ex $[1] - [16]$ in $[4] - [13]$ autem prodit $(2,5) - (2,3)$, adeoque quantitas realis negativa, quare quum $[1] - [16]$ sit $+i\sqrt{(2 - (2,15))}$, *i. e.* productum ex imaginaria i in realem *positivam*, etiam $[4] - [13]$ esse debet productum ex i in realem *positivam* propter $ii = -1$; hinc colligitur, pro $[4]$ signum superius, pro $[13]$ inferius accipiendum esse. Simili modo pro radicibus $[8]$ et $[9]$ invenitur $\frac{1}{2}(2,9) \pm \frac{1}{2}i\sqrt{(2 - (2,1))}$, ubi, quoniam productum ex $[1] - [16]$ in $[8] - [9]$ fit $(2,9) - (2,10)$ adeoque negativum, pro $[8]$ signum superius, pro $[9]$ inferius accipere oportet. Computando perinde radices reliquas, sequentes valores numericos obtinemus, ubi radicibus prioribus signa superiora, posterioribus inferiora respondere subintelligendum est:

*) Vera indoles huius artificii in eo consistit, quod a priori praevideri poterat, hocce productum evolutum aggregata quatuor terminorum non continere sed per sola aggregata octo terminorum exhiberi posse, cuius rei rationem hic brevitatis causa praetereundam periti facillime deprehendent.

$$
\begin{array}{ll}
[1], [16] \ldots & 0{,}9324722294 \pm 0{,}3612416662\,i \\
[2], [15] \ldots & 0{,}7390089172 \pm 0{,}6736956436\,i \\
[3], [14] \ldots & 0{,}4457383558 \pm 0{,}8951632914\,i \\
[4], [13] \ldots & 0{,}0922683595 \pm 0{,}9957341763\,i \\
[5], [12] \ldots & -0{,}2736629901 \pm 0{,}9618256432\,i \\
[6], [11] \ldots & -0{,}6026346364 \pm 0{,}7980172273\,i \\
[7], [10] \ldots & -0{,}8502171357 \pm 0{,}5264321629\,i \\
[8], [9] \ldots & -0{,}9829730997 \pm 0{,}1837495178\,i
\end{array}
$$

* * *

Possent quidem ea, quae in praecc. sunt tradita, ad solutionem aequationis $x^n - 1 = 0$ adeoque etiam ad inventionem functionum trigonometricarum arcubus cum peripheria commensurabilibus respondentium sufficere: attamen, propter rei gravitatem, finem huic disquisitioni imponere non possumus, quin antea ex magna copia quum observationum hoc argumentum illustrantium tum positionum ei affinium vel inde pendentium quaedam hic annectamus. Inter quae talia potissimum eligemus, quae sine magno aliarum disquisitionum apparatu absolvere licet, aliterque ea considerari nolimus quam ut *specimina* huius amplissimae doctrinae, in posterum copiose pertractandae.

Disquisitiones ulteriores de radicum periodis, Aggregata, in quibus terminorum multitudo par, sunt quantitates reales.

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 ut $(2, \lambda)$, e radicibus $[\lambda]$ et $[\lambda g^{\frac{1}{2}(n-1)}]$ constabit, denotante g ut supra radicem primitivam 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), unde $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$. 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 $(2, \lambda) = 2\cos\frac{kP}{n}$. Unde hoc loco hanc tantummodo conclusionem deducimus, valorem cuiusvis aggregati duorum terminorum esse quantitatem realem. Quum quaevis periodus, cuius terminorum multitudo par $= 2a$, in a periodos binorum terminorum discerpi possit, patet generalius, valorem cuiusvis aggregati,

cuius terminorum multitudo par, semper esse quantitatem realem. Quodsi itaque in art. 352 inter factores α, δ, γ etc. binarius ad ultimum locum reservatur, omnes operationes, usquedum ad aggregata duorum terminorum perveniatur, per quantitates reales absolventur, imaginariaeque tunc demum introducentur, quando ab his aggregatis ad radices ipsas progredieris.

De aequatione, per quam distributio radicum Ω in duas periodos definitur.

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, ubi $n-1$ factorem 3 implicat, de cubica, cuius radices sunt aggregata $\frac{1}{3}(n-1)$ terminorum, agemus.

Scribendo brevitatis caussa m pro $\frac{1}{2}(n-1)$ et designando per g radicem primitivam 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 positiva 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 convenient 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 diversi ipsoque n minores sint ipsorumque multitudo $= \frac{1}{2}(n-1)$ adeoque multitudini cunctorum residuorum positivorum ipsius n infra n aequalis, haec residua cum illis numeris omnino convenient. Hinc sponte sequitur, omnes numeros N, N', N'' etc., qui tum inter se tum ab ipsis $1, R, R'$ etc. diversi sunt, et cum his simul sumti omnes numeros $1, 2, 3 \ldots n-1$ exhauriunt, cum omnibus *non-residuis quadraticis* positivis ipsius n infra n convenire debere. Quodsi iam supponitur, aequationem, cuius radices sunt aggregata $(m, 1)$, (m, g), esse

$$xx - Ax + B = 0$$

fit

$$A = (m, 1) + (m, g) = -1, \quad B = (m, 1) \times (m, g)$$

Productum ex $(m, 1)$ in (m, g) per art. 345 fit

$$= (m, N+1)+(m, N'+1)+(m, N''+1)+\text{etc.} = W$$

atque hinc reducetur sub formam talem $\alpha(m, 0)+\vec{o}(m, 1)+\gamma(m, g)$. Ad determinationem coëfficientium $\alpha, \vec{o}, \gamma$ observamus, *primo*, fieri $\alpha+\vec{o}+\gamma = m$ (scilicet quoniam multitudo aggregatorum in W est $= m$); *secundo*, esse $\vec{o} = \gamma$ (hoc sequitur ex art. 350, quum productum $(m, 1) \times (m, g)$ sit functio invariabilis 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 $(m, 0)$ reduci adeoque esse $\alpha = 0$, quando inter numeros N, N', N'' etc. non occurrat $n-1$, *vel* unum puta (m, n), et proin haberi $\alpha = 1$, quando $n-1$ inter numeros N, N', N'' etc. reperiatur. Hinc colligitur, in casu priori fieri $\alpha = 0$, $\vec{o} = \gamma = \frac{1}{2}m$, in posteriori $\alpha = 1$, $\vec{o} = \gamma = \frac{1}{2}(m-1)$, simul hinc sequitur, quum numeri $\vec{o}$ et γ necessario fiant integri, casum priorem locum habere, sive $n-1$ (aut quod idem est -1) inter non-residua ipsius n non reperiri, quando m sit par sive n formae $4k+1$; casum posteriorem vero adesse, sive $n-1$ aut -1 inter non-residua ipsius n reperiri, quoties m sit impar sive n formae $4k+3$ *). Hinc productum 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 $\Sigma[\mathfrak{N}]$, ubi pro $\mathfrak{R}$ omnia residua, pro $\mathfrak{N}$ omnia non-residua quadratica positiva 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 divisibilem, fieri

$$\Sigma\cos\frac{k\mathfrak{R}P}{n} - \Sigma\cos\frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{et} \quad \Sigma\sin\frac{k\mathfrak{R}P}{n} - \Sigma\sin\frac{k\mathfrak{N}P}{n} = 0$$

pro $n \equiv 1 \pmod 4$; contra pro $n \equiv 3 \pmod 4$ differentiam illam $= 0$, hanc

*) Hoc modo macti sumus demonstrationem novam theorematis, -1 esse residuum omnium numerorum primorum formae $4k+1$, non-residuum omnium formae $4k+3$, quod supra (art. 108, 109, 262) iam pluribus modis diversis comprobatum fuit. Si magis arridet, hoc theorema supponere, non necessarium erit ad distinctionem duorum casuum diversorum eius conditionis rationem habere, quod $\vec{o}, \gamma$ iam per se fiunt integri.

$= \pm\sqrt{n}$, quae theoremata propter elegantiam suam valde sunt memorabilia. Ceterum observamus, signa superiora semper valere, quando pro k accipiatur unitas aut generalius residuum quadraticum ipsius n, inferiora, quando pro k non-residuum assumatur, nec non haecce theoremata salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

Demonstratio theorematis in Sect. IV commemorati.

357.

Sit aequatio m^{ti} gradus, cuius radices sunt m radices in periodo $(m, 1)$ contentae, haec

$$x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$$

sive $z = 0$, eritque $a = (m, 1)$, singulique reliqui coëfficientes b etc. sub forma tali $\mathfrak{A}+\mathfrak{B}(m, 1)+\mathfrak{C}(m, g)$ comprehensi, ita ut $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ sint integri (art. 348); denotandoque per z' functionem, in quam z transit, si pro $(m, 1)$ ubique substituitur (m, g), pro (m, g) vero (m, gg) sive 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, ubi 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 brevitatis 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

$$2z' = 2R-S-T+(T-S)(p-q)$$

unde ponendo

$$2R-S-T = Y, \quad T-S = Z$$

fit $4X = YY-(p-q)^2ZZ$, 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 diversa indole numeri n, nec formulae analyticae generali subiici possunt.

Ex. Pro $n = 17$ aequatio, cuius radices sunt octo radices in (8, 1) contentae, per praecepta art. 348 eruitur

$$x^8 - px^7 + (4+p+2q)x^6 - (4p+3q)x^5 + (6+3p+5q)x^4 - (4p+3q)x^3 + (4+p+2q)xx - px + 1 = 0$$

unde

$$R = x^8 + 4x^6 + 6x^4 + 4xx + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$$

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	$2x^{11}+x^{10}-5x^9-8x^8-7x^7-4x^6+4x^5+7x^4+8x^3+5xx-x-2$	$x^{10}+x^9-x^7-2x^6-2x^5-x^4+xx+x$

De aequatione pro distributione radicum Ω in tres periodos.

358.

Progredimur ad considerationem aequationum cubicarum, per quas in eo casu, ubi n est formae $3k+1$, tria aggregata $\frac{1}{3}(n-1)$ terminorum complexum Ω componentia determinantur. Sit g radix primitiva 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'', patetque primum continere radices $[1], [g^3], [g^6] \dots [g^{n-4}]$, secundum has $[g], [g^4] \dots [g^{n-3}]$, tertium has $[gg], [g^5] \dots [g^{n-2}]$. Supponendo, aequationem quaesitam esse

$$x^3 - Axx + Bx - C = 0$$

fit

$$A = p+p'+p'', \quad B = pp'+p'p''+pp'', \quad C = pp'p''$$

unde protinus habetur $A = -1$. Sint residua minima positiva numerorum g^3, $g^6 \dots g^{n-4}$ 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 $g, g^4, g^7 \dots g^{n-3}$, atque $\mathfrak{K}'$ illorum complexus; denique $\mathfrak{A}'', \mathfrak{B}'', \mathfrak{C}''$ etc. residua minima ipsorum $gg, g^5, g^8 \dots g^{n-2}$ et $\mathfrak{K}''$ eorum complexus, unde omnes numeri in $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ diversi erunt et cum his 1, 2, 3 . . . $n-1$ convenient. Ante omnia hic observandum est, numerum $n-1$ necessario in $\mathfrak{K}$ reperiri, quippe quem esse residuum ipsius $g^{\frac{3m}{2}}$ 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 $g^{\lambda+\frac{3m}{2}}$, aut huius $g^{\lambda-\frac{3m}{2}}$ si $\lambda > \frac{3m}{2}$. Denotemus hocce signo $(\mathfrak{K}\mathfrak{K})$ multitudinem numerorum in serie 1, 2, 3 . . . $n-1$, qui tum ipsi tum simul numeri proximi unitate 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, unde 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 $n-h$, $n-h'$ etc.

in $\mathfrak{R}$; quare quum tales numeri omnino dentur $(\mathfrak{R}'\mathfrak{R})$, certo nequit esse $(\mathfrak{R}'\mathfrak{R}) < (\mathfrak{R}\mathfrak{R}')$, et perinde demonstratur, esse non posse $(\mathfrak{R}\mathfrak{R}') < (\mathfrak{R}'\mathfrak{R})$, quocirca hi numeri necessario aequales erunt. Prorsus eodem modo probatur $(\mathfrak{R}\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R})$, $(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}')$. Secundo, quum necessario quemvis numerum ex $\mathfrak{R}$, maximo $n-1$ excepto, sequi debeat proxime maior vel in $\mathfrak{R}$, vel in $\mathfrak{R}'$ vel in $\mathfrak{R}''$ contentus, summa $(\mathfrak{R}\mathfrak{R})+(\mathfrak{R}\mathfrak{R}')+(\mathfrak{R}\mathfrak{R}'')$ fiet aequalis multitudini omnium numerorum in $\mathfrak{R}$ unitate deminutae puta $= m-1$, et simili ratione erit

$$(\mathfrak{R}'\mathfrak{R})+(\mathfrak{R}'\mathfrak{R}')+(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R})+(\mathfrak{R}''\mathfrak{R}')+(\mathfrak{R}''\mathfrak{R}'') = m$$

His ita praeparatis evolvimus 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 $(\mathfrak{R}'\mathfrak{R})p+(\mathfrak{R}'\mathfrak{R}')p'+(\mathfrak{R}'\mathfrak{R}'')p''$, 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, ut antea pp' evolutum 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

$$(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a, \quad (\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}') = b, \quad (\mathfrak{R}'\mathfrak{R}') = (\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}'') = c$$

fieri $m-1 = (\mathfrak{R}\mathfrak{R})+(\mathfrak{R}\mathfrak{R}')+(\mathfrak{R}\mathfrak{R}'') = (\mathfrak{R}\mathfrak{R})+b+c$, atque $a+b+c = m$, unde $(\mathfrak{R}\mathfrak{R}) = a-1$, ita ut illae novem quantitates incognitae ad tres, a, b, c, sive potius propter aequationem $a+b+c = m$ ad duas reductae sint. Denique patet, quadratum pp evolvi 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 $(m, 0)$ sive ad m, reliquas vero facile perspicietur reduci ad $(\mathfrak{R}\mathfrak{R})p+(\mathfrak{R}\mathfrak{R}')p'+(\mathfrak{R}\mathfrak{R}'')p''$, unde habetur $pp = m+(a-1)p+bp'+cp''$.

Hoc itaque modo per disquisitiones praecedentes quatuor hasce reductiones nacti sumus.

$$\begin{aligned} pp &= m+(a-1)p+bp'+cp'' \\ pp' &= \quad bp+cp'+ap'' \\ pp'' &= \quad cp+ap'+bp'' \\ p'p'' &= \quad ap+bp'+cp'' \end{aligned}$$

ubi inter tres incognitas a, b, c aequatio conditionalis

$$a+b+c = m \quad \ldots\ldots\ldots\ldots (\mathrm{I})$$

intercedit, insuperque certum est, ipsas esse numeros integros. Hinc colligitur

$$\begin{aligned} C = p \times p'p'' &= app+bpp'+cpp'' \\ &= am+(aa+bb+cc-a)p+(ab+bc+ac)p'+(ab+bc+ac)p'' \end{aligned}$$

At quum $pp'p''$ sit functio invariabilis aggregatorum p, p', p'', coëfficientes, per quos haec in expr. praec. multiplicata sunt, necessario aequales erunt (art. 350), unde habetur aequatio nova

$$aa+bb+cc-a = ab+bc+ac \ldots (\mathrm{II})$$

atque hinc $C = am+(ab+bc+ac)(p+p'+p'')$, sive (propter I. et $p+p'+p'' = -1$)

$$C = aa-bc \ldots\ldots (\mathrm{III})$$

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 ut ostendamus, aequationem II ita exhibemus

$$\begin{aligned} 12a+12b+12c+4 = 36aa+36bb+36cc-36ab-36ac-36bc \\ -24a+12b+12c+4 \end{aligned}$$

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 $3m+1$) 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 unico 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, utrumque hunc numerum esse minorem quam n; quare is, quem n metitur, necessario esse debet $= 0$, adeoque etiam $u'u' - uu = 0$, unde $u'u' = uu$ 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 $k = 2a-b-c = 3a-m$, erit $a = \frac{1}{3}(m+k)$, $b+c = m-a = \frac{1}{3}(2m-k)$, unde

$$C = aa - bc = aa - \tfrac{1}{4}(b+c)^2 + \tfrac{1}{4}(b-c)^2$$
$$= \tfrac{1}{9}(m+k)^2 - \tfrac{3}{36}(2m-k)^2 + \tfrac{1}{4}NN = \tfrac{1}{12}kk + \tfrac{1}{3}km + \tfrac{1}{4}NN$$

atque sic omnes coëfficientes aequ. quaesitae inventi. *Q. E. F.* — Haec formula

*) Magis directe haecce proposito e principiis Sect. V probari posset.

†) Manifesto M nequit esse formae $3z$, alioquin enim $4n$ per 3 divisibilis evaderet. — Ad ambiguitatem, utrum $b-c$ statui debeat $= N$, an $= -N$, hic non opus est respicere, neque etiam per rei naturam ullo modo auferri potest, quum ab electione radicis primitivae g pendeat, ita ut pro aliis radicibus primitivis differentia $b-c$ positiva evadat, pro aliis negativa.

adhuc simplicior evadit, si pro NN eius valor ex aequ. $(3k-2)^2 + 27NN = 4n = 12m+4$ substituitur, unde elicitur calculo facto

$$C = \tfrac{1}{9}(m + k + 3km) \Rightarrow \tfrac{1}{9}(m + kn)$$

Idem valor etiam ad $(3k-2)NN + k^3 - 2kk + k - km + m$ reduci potest, quae expressio, ad usum quidem minus idonea, protinus monstrat, C ut par est, certo evadere integrum.

Ex. Pro $n = 19$, fit $4n = 49 + 27$, unde $3k-2 = +7$, $k = 3$, $C = \frac{1}{9}(6+57) = 7$ et aequatio quaesita $x^3 + xx - 6x - 7 = 0$ ut supra (art. 351). — Simili modo pro $n = 7, 13, 31, 37, 43, 61, 67$ valor ipsius k eruitur resp. $1, -1, 2, -3, -2, 1, -1$, unde $C = 1, -1, 8, -11, -8, 9, -5$.

Ceterum etsi problema in hoc art. solutum satis intricatum sit, tamen id supprimere noluimus, tum propter solutionis elegantiam, tum quod variis artificiis in usum vocandis occasionem dedit, quae in aliis quoque quaestionibus insigni cum fructu adhiberi poterunt*).

Aequationum per quas radices Ω inveniuntur reductio ad puras.

359.

Disquisitiones praecc. circa *inventionem* aequationum auxiliarium versabantur: iam de earum *solutione* proprietatem magnopere insignem explicabimus. Constat, omnes summorum geometrarum labores, aequationum ordinem quartum superantium resolutionem generalem, sive (ut accuratius quid desideretur definiam) AFFECTARUM REDUCTIONEM AD PURAS, inveniendi 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 annotavimus in *Demonstr. nova etc. art.* 9). 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,

*) Corollar. Sit ε radix aequationis $x^3 - 1 = 0$ et habebis $(p + \varepsilon p' + \varepsilon\varepsilon p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$.

Fiat $\frac{M}{\sqrt{4n}} = \cos\varphi$, $\frac{N\sqrt{27}}{\sqrt{4n}} = \sin\varphi$ critque

$$p = -\tfrac{1}{3} + \tfrac{2}{3}\cos\tfrac{1}{3}\varphi\sqrt{n}, \quad M \equiv +1 \pmod 3; \quad 1 \equiv M(1, 2, 3 \ldots m)^3 \pmod n$$

Setzt man $3x + 1 = y$ so wird die Gleichung $y^3 - 3ny - Mn = 0$.

praecipua tantum momenta, quae ad possibilitatem ostendendam necessaria sunt, hoc loco tradimus, uberioremque tractationem, qua hoc argumentum perdignum est, ad aliud tempus differimus. Praemittendae sunt quaedam observationes generales circa radices aequ. $x^e - 1 = 0$, quae eum quoque casum complectantur, ubi e est numerus compositus.

I. Exhibentur hae radices (ut ex libris elementaribus notum est) per $\cos\frac{kP}{e} + i\sin\frac{kP}{e}$, ubi pro k accipiendi sunt e numeri $0, 1, 2, 3 \ldots e-1$, aut quicunque alii his secundum modulum e congrui. Una radix, pro $k = 0$ aut generaliter pro k per e divisibili fit $= 1$; cuivis alii valori ipsius k radix ab 1 diversa 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 diversos. 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

$$1 + R^\lambda + R^{2\lambda} \ldots + R^{\lambda(e-1)} \text{ fit } = 0$$

pro quovis valore integro ipsius λ per e non divisibili; etenim est $= \frac{1-R^{\lambda e}}{1-R^\lambda}$, cuius fractionis numerator fit $= 0$, denominator vero non $= 0$. Quando vero λ per e divisibilis est, illud aggregatum manifesto fit $= e$.

360.

Sit, ut semper in praecc., n numerus primus, g radix primitiva pro modulo n, atque $n-1$ productum e tribus integris positivis α, δ, γ; brevitatis caussa disquisitionem ita statim instituemus, ut etiam ad casus ubi 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 $\delta\gamma$ terminorum cognitis $(\delta\gamma, 1)$, $(\delta\gamma, g)$, $(\delta\gamma, gg) \ldots (\delta\gamma, g^{\alpha-1})$ deducenda esse aggregata γ terminorum, quod negotium supra ad aequationem affectam δ^{ti} gradus reduximus, nunc vero per puram aeque altam absolvere docebimus. Ad abbreviandum pro aggregatis

$$(\gamma, 1),\ (\gamma, g^\delta),\ (\gamma, g^{2\delta}) \ldots (\gamma, g^{\alpha\delta-\delta})$$

quae sub $(\delta\gamma, 1)$ contenta sunt, scribemus $a, b, c \ldots m$ resp.; pro his

$$(\gamma, g),\ (\gamma, g^{\alpha+1}) \ldots (\gamma, g^{\alpha\delta-\alpha+1})$$

sub $(\delta\gamma, g)$ contentis resp. $a', b' \ldots m'$; pro his

$$(\gamma, gg),\ (\gamma, g^{\alpha+2}) \ldots (\gamma, g^{\alpha\delta-\alpha+2})$$

resp. $a'', b'' \ldots m''$ etc. usque ad ea, quae sub $(\delta\gamma, g^{\alpha-1})$ continentur.

I. Iam designet R indefinite radicem aequationis $x^\delta - 1 = 0$, supponamusque ex evolutione potestatis δ^{tae} functionis

$$t = a + Rb + RRc \ldots + R^{\delta-1}m$$

oriri per praecepta art. 345

$$\begin{aligned} N = {} & Aa + Bb + Cc \ldots + Mm \\ & + A'a' + B'b' + C'c' \ldots + M'm' \\ & + A''a'' + B''b'' + C''c'' \ldots + M''m'' \\ & + \text{etc.} \end{aligned}$$

ubi omnes coëfficientes N, A, B, A' etc. erunt functiones rationales integrae ipsius R. Supponantur etiam potestates δ^{tae} duarum aliarum functionum

$$u = R^\delta a + Rb + RRc \ldots + R^{\delta-1}m,\ u' = b + Rc + RRd \ldots + R^{\delta-2}m + R^{\delta-1}a$$

resp. evolvi 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

$$\begin{aligned} U' = {} & N + Ab + Bc + Cd \ldots + Ma \\ & + A'b' + B'c' + C'd' \ldots + M'a' \\ & + A''b'' + B''c'' + C''d'' \ldots + M''a'' \\ & + \text{etc.} \end{aligned}$$

Porro patet, quum sit $u = Ru'$, fore $U = R^\delta U'$, quare propter $R^\delta = 1$ coëfficientes correspondentes in U et U' aequales erunt; denique, quum t et u in eo tantum differant, quod a in t per unitatem, in u per R^δ 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., unde T reducitur ad formam talem

$$N + A(\vec{\sigma}\gamma, 1) + A'(\vec{\sigma}\gamma, g) + A''(\vec{\sigma}\gamma, gg) \text{ etc.}$$

ubi singuli coëfficientes N, A, A' etc. sub formam talem reducere licet

$$pR^{\vec{\sigma}-1} + p'R^{\vec{\sigma}-2} + p''R^{\vec{\sigma}-3} + \text{etc.}$$

ita ut p, p', p'' etc. sint numeri integri dati.

II. Si pro R accipitur radix determinata aequationis $x^{\vec{\sigma}} - 1 = 0$ (cuius solutionem iam haberi supponimus), et quidem talis, cuius nulla inferior potestas quam $\vec{\sigma}^{\text{ta}}$ unitati aequalis est, etiam T quantitas determinata erit, ex qua t per aequationem puram $t^{\vec{\sigma}} - T = 0$ derivare licet. At quum haec aequatio $\vec{\sigma}$ radices habeat, quae erunt t, Rt, $RRt \ldots R^{\vec{\sigma}-1}t$, dubium videri potest, quamnam radicem adoptare oporteat. Hoc vero prorsus arbitrarium esse, ita facile apparebit. Meminisse oportet, postquam omnia aggregata $\vec{\sigma}\gamma$ terminorum determinata sint, radicem [1] eatenus tantum definitam esse, ut aliqua ex $\vec{\sigma}\gamma$ radicibus in $(\vec{\sigma}\gamma, 1)$ contentis hoc signo denotari debeat; et perin omnino arbitrarium esse, quidnam ex $\vec{\sigma}$ aggregatis ipsum $(\vec{\sigma}\gamma, 1)$ 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 $= \frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\vec{\sigma}-1}$. Simili modo si per a id aggregatum exprimere placet, quod ab initio erat c, valor ipsius t fiet $\mathfrak{T}R^{\vec{\sigma}-2}$, et ita porro t cuicunque quantitatum $\mathfrak{T}$, $\mathfrak{T}R^{\vec{\sigma}-1}$, $\mathfrak{T}R^{\vec{\sigma}-2}$ etc. aequalis censeri potest, *i. e.* cuilibet radici aequ. $x^{\vec{\sigma}} - T = 0$, prout aliud aliudve aggregatum sub $(\vec{\sigma}\gamma, 1)$ contentum per $(\gamma, 1)$ expressum supponatur. *Q. E. D.*

III. Postquam quantitas t hoc modo determinata est, $\vec{\sigma} - 1$ alias investigare oportet, quae ex t prodeunt, si in eius expressione pro R successive RR, R^3, $R^4 \ldots R^{\vec{\sigma}}$ substituuntur, puta

$$t' = a + RRb + R^4c \ldots + R^{2\vec{\sigma}-2}m, \quad t'' = a + R^3b + R^6c \ldots + R^{3\vec{\sigma}-3}m \text{ etc.}$$

Ultima quidem iam habetur, quum manifesto fiat $= a + b + c \ldots + m = (\vec{\sigma}\gamma, 1)$; reliquae vero sequenti modo erui possunt. Si per praecepta art. 345, simili modo ut $t^{\vec{\sigma}}$ antea in I. productum $t^{\vec{\sigma}-2}t'$ evolvitur, probabitur per methodum praecedenti prorsus analogam, quod inde prodeat ad formam talem

$$\mathfrak{N} + \mathfrak{A}(\vec{\sigma}\gamma, 1) + \mathfrak{A}'(\vec{\sigma}\gamma, g) + \mathfrak{A}''(\vec{\sigma}\gamma, gg) \text{ etc.} = T''$$

reduci posse, ita ut $\mathfrak{N}$, $\mathfrak{A}$, $\mathfrak{A}'$ etc. sint functiones rationales integrae ipsius R, adeoque T' quantitas nota, unde habebitur $t' = \frac{T'tt}{T}$. Prorsus eodem modo, si ex evolutione producti $t^{\vec{\sigma}-3}t''$ prodire supponitur T'', haec expressio similem formam habebit et proin ex eius valore noto derivabitur t'' per aequationem $t'' = \frac{T''t^3}{T}$; perinde t''' per aequationem talem invenietur $t''' = \frac{T'''t^4}{T^2}$, ita ut T''' sit quantitas nota etc.

Haec methodus non foret applicabilis, si fieri posset, $t = 0$, unde 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 convertere licet; nec non methodi breviores pro eo casu ubi $\alpha = 1$ valores ipsarum t', t'' etc. eruendi, quae omnia hic silentio praeterire debemus.

IV. Denique simulac t, t', t'' etc. inventae sunt, habebitur statim per obs. III art. praec. $t + t' + t'' + \text{etc.} = \vec{\sigma}a$, unde valor ipsius a notus erit, ex quo per art. 346 valores omnium reliquorum aggregatorum γ terminorum derivari poterunt. — Valores ipsorum b, c, d etc. etiam per aequationes sequentes elici possunt, quarum ratio cuivis attendenti facile patebit:

$$\vec{\sigma}b = R^{\vec{\sigma}-1}t + R^{\vec{\sigma}-2}t' + R^{\vec{\sigma}-3}t'' + \text{etc.}$$
$$\vec{\sigma}c = R^{2\vec{\sigma}-2}t + R^{2\vec{\sigma}-4}t' + R^{2\vec{\sigma}-6}t'' + \text{etc.}$$
$$\vec{\sigma}d = R^{3\vec{\sigma}-3}t + R^{3\vec{\sigma}-6}t' + R^{3\vec{\sigma}-9}t'' + \text{etc. etc.}$$

Ex magno numero observationum ad disquisitionem praec. pertinentium hic unam tantum attingimus. Quod attinet ad solutionem aequationis purae $x^{\vec{\sigma}} - T = 0$, facile patet, T in plerisque casibus valorem imaginarium $P + iQ$ habere, unde illa solutio partim a sectione anguli (cuius tangens $= \frac{Q}{P}$) partim a sectione rationis (unitatis ad $\sqrt{(PP+QQ)}$) in $\vec{\sigma}$ partes, ut constat, pendebit. Ubi valde mirabile est (quod tamen fusius hic non exsequimur), valorem ipsius $\sqrt[\vec{\sigma}]{(PP+QQ)}$ semper *rationaliter* per quantitates iam notas exprimi posse, ita ut, praeter extractionem radicis quadraticae, ad solutionem *sola* sectio anguli requiratur, *e. g.* pro $\vec{\sigma} = 3$ sola trisectio anguli.

Tandem quum nihil obstet, quo minus statuamus $\alpha = 1$, $\gamma = 1$ adeoque

$6 = n-1$: manifestum est, solutionem aequationis $x^n - 1 = 0$ statim reduci posse ad solutionem aequationis puras $n-1^{\text{ti}}$ gradus $x^{n-1} - T = 0$, ubi T per radices aequationis $x^{n-1} - 1 = 0$ determinabitur. Unde adiumento observationis 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 unius radicis quadraticae, et quidem ostendi potest, hanc semper esse $\sqrt{n}$.

Applicatio disquisitionum praecedentium ad functiones trigonometricas. Methodus, angulos quibus singulae radices Ω respondeant dignoscendi.

361.

Superest, ut nexum inter radices Ω atque functiones trigonometricas angulorum $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{n}$ adhuc propius contemplemur. Methodus, quam pro inveniendis radicibus Ω exposuimus, ita comparata est, ut adhuc incertum relinquat (nisi tabulae sinuum inter laborem ita ut 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 $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n} \ldots \frac{(n-1)P}{2n}$ continuo decrescere (siquidem etiam signorum ratio habeatur), sinus omnes positivos esse; angulos $\frac{(n-1)P}{n}, \frac{(n-2)P}{n}, \frac{(n-3)P}{n} \ldots \frac{(n+1)P}{2n}$ vero eosdem resp. cosinus habere ut illos, sinus autem negativos 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, ubi quantitas imaginaria i per quantitatem positivam, posteriori ea, ubi i per quantitatem negativam 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 agnita est, eae quae angulis reliquis respondent etiam inde distingui poterunt, quod, si illa supponatur esse $= [\lambda]$, angulis $\frac{2P}{n}, \frac{3P}{n}, \frac{4P}{n}$ etc. manifesto respondebunt radices $[2\lambda]$, $[3\lambda]$, $[4\lambda]$ etc. Ita in exemplo art. 353 illico videtur, angulo $\frac{1}{19}P$ aliam radicem respondere non posse quam hanc [11] anguloque $\frac{4}{19}P$ radicem [8]; similiter angulis $\frac{2}{19}P$, $\frac{4}{19}P$, $\frac{8}{19}P$, $\frac{9}{19}P$, $\frac{7}{19}P$ 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.

Tangentes, cotangentes, secantes et cosecantes e sinubus et cosinubus absque divisione derivantur.

362.

Quod vero attinet ad reliquas functiones trigonometricas horum angulorum, possent eae quidem e cosinubus et sinubus respondentibus per methodos vulgo notas facile derivari, puta secantes et tangentes, dividendo unitatem et sinus per cosinus; nec non cosecantes et cotangentes, dividendo unitatem et cosinus per sinus. Sed commodius plerumque idem obtinetur adiumento formularum sequentium absque divisionibus per meras additiones. Sit ω angulus quicunque ex his $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$ atque $\cos\omega + i\sin\omega = R$, unde R erit aliqua e radicibus Ω,

$$\cos\omega = \tfrac{1}{2}(R + \tfrac{1}{R}) = \frac{1+RR}{2R}, \quad \sin\omega = \frac{1}{2i}(R - \frac{1}{R}) = \frac{i(1-RR)}{2R}$$

Hinc fit

$$\sec\omega = \frac{2R}{1+RR}, \quad \operatorname{tang}\omega = \frac{i(1-RR)}{1+RR}, \quad \operatorname{cosec}\omega = \frac{2Ri}{RR-1}, \quad \operatorname{cotang}\omega = \frac{i(RR+1)}{RR-1}$$

Iam numeratores harum quatuor fractionum ita transformare ostendemus, ut per denominatores divisibiles evadant.

I. Propter $R = R^{n+1} = R^{2n+1}$, fit $2R = R + R^{2n+1}$, quam expressionem per $1+RR$ divisibilem 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 $\sin\omega - \sin 3\omega + \sin 5\omega \ldots + \sin(2n-1)\omega = 0$)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \ldots + \cos(2n-1)\omega$$

sive tandem, (quoniam $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$ etc.),

$$= 2\big(\cos\omega - \cos 3\omega + \cos 5\omega \ldots \mp \cos(n-2)\omega\big) \pm \cos n\omega$$

signo superiori vel inferiori valente prout n est formae $4k+1$ vel $4k+3$. Manifesto haec formula etiam ita exhiberi potest

$$\sec\omega = \pm\big(1 - 2\cos 2\omega + 2\cos 4\omega \ldots \pm 2\cos(n-1)\omega\big)$$

II. Simili modo substituendo $1 - R^{2n+2}$ pro $1 - RR$, prodit

$$\text{tang}\,\omega = i(1 - RR + R^4 - R^6 \ldots - R^{2n})$$

sive (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 divisibiles. Hinc

$$\begin{aligned}\frac{n}{1-RR} &= 1 + (1+RR) + (1+RR+R^4) \ldots + (1+RR+R^4 \ldots + R^{2n-4}) \\ &= (n-1) + (n-2)\,RR + (n-3)\,R^4 \ldots + R^{2n-4}\end{aligned}$$

quocirca multiplicando per 2, subtrahendo

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

rursusque per R multiplicando fit

$$\frac{2nR}{1-RR} = (n-1)R + (n-3)R^3 + (n-5)R^5 \ldots - (n-3)R^{2n-3} - (n-1)R^{2n-1}$$

unde protinus deducitur

$$\begin{aligned}\text{cosec}\,\omega &= \tfrac{1}{n}((n-1)\sin\omega + (n-3)\sin 3\omega \ldots - (n-1)\sin(2n-1)\omega) \\ &= \tfrac{2}{n}((n-1)\sin\omega + (n-3)\sin 3\omega + \text{etc.} + 2\sin(n-2)\omega)\end{aligned}$$

quae formula etiam ita exhiberi potest

$$\text{cosec}\,\omega = -\tfrac{2}{n}(2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega \ldots + (n-1)\sin(n-1)\omega)$$

IV. Multiplicando valorem ipsius $\frac{n}{1-RR}$ supra traditum per $1 + RR$ et subtrahendo

$$0 = (n-1)(1 + RR + R^4 \ldots + R^{2n-2})$$

prodit

$$\frac{n(1+RR)}{1-RR} = (n-2)\,RR + (n-4)\,R^4 + (n-6)\,R^6 \ldots - (n-2)\,R^{2n-2}$$

unde statim sequitur

$$\begin{aligned}\text{cotang}\,\omega &= \tfrac{1}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega + (n-6)\sin 6\omega \ldots - (n-2)\sin(n-2)\omega \\ &= \tfrac{2}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega \ldots + 3\sin(n-3)\omega + \sin(n-1)\omega)\end{aligned}$$

quam formulam etiam hocce modo exhibere licet

$$\text{cotang}\,\omega = -\tfrac{2}{n}(\sin\omega + 3\sin 3\omega \ldots + (n-2)\sin(n-2)\omega)$$

Methodus, aequationes pro functionibus trigonometricis successive deprimendi.

363.

Quemadmodum, supponendo $n - 1 = ef$, functio X in e factores f dimensionum resolvi 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 angulorum $\frac{P}{n}, \frac{2P}{n} \ldots \frac{(n-1)P}{n}$, functio Z in e factores f dimensionum resolvi 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 *) convenire. Quodsi itaque functio, de qua agitur, per characterem φ angulo praefixum denotetur; productum ex e factoribus

$$x - \varphi\omega,\ x - \varphi a\omega,\ x - \varphi b\omega \text{ etc.}$$

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, ut demonstremus, omnes coëfficientes in functionibus Y, Y', Y'' etc. ad formam talem

*) Hoc respectu duo anguli conveniunt, quorum differentia vel peripheriae integrae vel alicui eius multiplo aequalis est, quales *secundum peripheriam congruos* vocare possemus, si congruentiam sensu aliquantum latiori intelligere luberet.

$$A+B(f,1)+C(f,g)+D(f,gg)\ldots+L(f,g^{e-1})$$

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 invariabiles 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 invariabiles 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 observationes 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 derivari posse, si modo ubique 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 derivabitur substituendo ubique 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 evoluta est, reliquae Y', Y'' etc. nullo negotio inde sequuntur.

II. Supponendo

$$Y = x^f - \alpha x^{f-1} + \delta x^{f-2} - \text{etc.}$$

coëfficientes α, δ etc. erunt resp. summa radicum aequ. $Y=0$ *i. e.* quantitatum $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc., summa productorum e binis etc. At plerumque hi coëfficientes multo commodius eruuntur per methodum ei, quae art. 349 tradita est, similem, computando summam radicum $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ 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, ubi f est numerus par, adeoque quaevis periodus P, P', P'' etc. ex $\frac{1}{2}f$ periodis binorum terminorum composita. Constet P ex his $(2,1)$, $(2,\mathfrak{a})$, $(2,\mathfrak{b})$, $(2,\mathfrak{c})$ etc., convenientque numeri 1, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ etc. atque $n-1$, $n-\mathfrak{a}$, $n-\mathfrak{b}$, $n-\mathfrak{c}$ etc. simul sumti, cum his 1, a, b, c etc. aut saltem (quod hic eodem redit) his secundum modulum n congrui erunt. Sed est $\varphi(n-1)\omega = \pm\varphi\omega$, $\varphi(n-\mathfrak{a})\omega = \pm\varphi\mathfrak{a}\omega$ 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 Y, binos semper aequales, adeoque Y quadratum esse, et quidem $Y=yy$, si y ponatur aequalis producto ex

$$x-\varphi\omega,\quad x-\varphi\mathfrak{a}\omega,\quad x-\varphi\mathfrak{b}\omega \text{ etc.}$$

Similiter in iisdem casibus functiones reliquae Y', Y'' etc. quadrata erunt, et quidem supponendo P' constare ex $(2,a')$, $(2,\mathfrak{b}')$, $(2,\mathfrak{c}')$ etc.; P'' ex $(2,a'')$, $(2,\mathfrak{b}'')$, $(2,\mathfrak{c}'')$ etc. etc., productum ex $x-\varphi a'\omega$, $x-\varphi\mathfrak{b}'\omega$, $x-\varphi\mathfrak{c}'\omega$ etc. esse $=y'$, productum ex $x-\varphi a''\omega$, $x-\varphi\mathfrak{b}''\omega$ etc. $=y''$ etc., erit $Y'=y'y'$, $Y''=y''y''$ 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 derivari, ut Y', Y'' etc. ex Y sequi ante in I diximus; nec non singulos coëfficientes in y quoque ad formam

$$A+B(f,1)+C(f,g)+\text{etc.}$$

reduci posse, quum summae singularum potestatum rad. aequ. $y=0$ manifesto sint semisses potestatum aequ. $Y=0$, adeoque ad talem formam reducibiles. In quatuor casibus posterioribus autem Y erit productum e factoribus

$$xx-(\varphi\omega)^2,\quad xx-(\varphi\mathfrak{a}\omega)^2,\quad xx-(\varphi\mathfrak{b}\omega)^2 \text{ etc.}$$

adeoque formae

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{etc.}$$

patetque coëfficientes λ, μ etc. e summis quadratorum, biquadratorum etc. ra-

dicum $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$ etc. deduci posse; et similiter se habebunt functiones Y', Y'' etc.

Ex. I. Sit $n = 17$, $f = 8$ atque designet φ cosinum. Hinc fit

$$Z = (x^8 + \tfrac{1}{2}x^7 - \tfrac{7}{4}x^6 - \tfrac{3}{8}x^5 + \tfrac{13}{16}x^4 + \tfrac{5}{16}x^3 - \tfrac{5}{32}xx - \tfrac{1}{32}x + \tfrac{1}{256})^2$$

oportetque adeo $\sqrt{Z}$ in duos factores quaternarum dimensionum y, y' resolvere. Periodus $P = (8,1)$ constat ex $(2,1)$, $(2,9)$, $(2,13)$, $(2,15)$, unde 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 $\varphi k\omega$, invenitur

$$\varphi\omega + \varphi 9\omega + \varphi 13\omega + \varphi 15\omega = \tfrac{1}{2}(8,1),\ (\varphi\omega)^2 + (\varphi 9\omega)^2 + (\varphi 13\omega)^2 + (\varphi 15\omega)^2 = 2 + \tfrac{1}{4}(8,1)$$

perinde summa cuborum $= \frac{3}{8}(8,1) + \frac{1}{4}(8,3)$, summa biquadratorum $= 1\frac{1}{2} + \frac{3}{16}(8,1)$; hinc per theorema Newtonianum coëfficientibus in y determinatis prodit

$$y = x^4 - \tfrac{1}{4}(8,1)x^3 + \tfrac{1}{4}((8,1) + 2(8,3))xx - \tfrac{1}{8}((8,1) + 3(8,3))x + \tfrac{1}{16}((8,1) + (8,3))$$

y' vero ex y derivatur 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

$$y = x^4 + (\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} + \tfrac{1}{8}\sqrt{17})xx + (\tfrac{1}{8} + \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$
$$y' = x^4 + (\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17})x^3 - (\tfrac{3}{8} - \tfrac{1}{8}\sqrt{17})xx + (\tfrac{1}{8} - \tfrac{1}{8}\sqrt{17})x - \tfrac{1}{16}$$

Simili modo $\sqrt{Z}$ in quatuor factores binarum dimensionum resolvi potest, quorum primus erit $(x - \varphi\omega)(x - \varphi 13\omega)$, secundus $(x - \varphi 9\omega)(x - \varphi 15\omega)$, tertius $(x - \varphi 3\omega)(x - \varphi 5\omega)$, 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 ut

$$Z = x^{16} - \tfrac{7}{4}x^{14} + \tfrac{11}{16}x^{12} - \tfrac{7}{32}x^{10} + \tfrac{9}{256}x^8 - \tfrac{5}{512}x^6 + \tfrac{1}{2048}x^4 - \tfrac{5}{8192}xx + \tfrac{1}{32768}$$

in duos factores 8 dimensionum y, y' resolvere 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

$$(\varphi k\omega)^2 = -\tfrac{1}{2}[2k] + \tfrac{1}{2}[n] - \tfrac{1}{4}[2n-2k] = \tfrac{1}{4} - \tfrac{1}{4}[2k] - \tfrac{1}{4}[2n-2k]$$

hinc deducitur summa quadratorum radicum $\varphi\omega$, $\varphi 9\omega$, $\varphi 13\omega$, $\varphi 15\omega$ 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 octavarum $\frac{35}{32} - \frac{25}{256}(8,1) - \frac{1}{32}(8,3)$. Hinc fit

$$y = x^8 - (2 - \tfrac{1}{4}(8,1))x^6 + (\tfrac{3}{2} - \tfrac{3}{16}(8,1) + \tfrac{1}{8}(8,3))x^4$$
$$- (\tfrac{1}{2} - \tfrac{9}{64}(8,1) + \tfrac{5}{64}(8,3))xx + \tfrac{1}{256} - \tfrac{5}{2048}(8,1) + \tfrac{3}{2048}(8,3)$$

y' derivatur ex y commutando $(8,1)$, $(8,3)$, ita ut per substitutionem valorum horum aggregatorum habeatur

$$y = x^8 - (\tfrac{7}{8} - \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{31}{32} - \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{7}{32} - \tfrac{1}{32}\sqrt{17})xx + \tfrac{1}{256} - \tfrac{1}{256}\sqrt{17}$$
$$y' = x^8 - (\tfrac{7}{8} + \tfrac{1}{8}\sqrt{17})x^6 + (\tfrac{31}{32} + \tfrac{7}{32}\sqrt{17})x^4 - (\tfrac{7}{32} + \tfrac{1}{32}\sqrt{17})xx + \tfrac{1}{256} + \tfrac{1}{256}\sqrt{17}$$

Perinde Z in quatuor factores resolvi potest, quorum coëfficientes per aggregata quatuor terminorum exprimi possunt, et quidem productum e duobus erit y, productum e duobus reliquis y'.

Sectiones circuli, quas per aequationes quadraticas sive per constructiones geometricas perficere licet.

365.

Reduximus itaque, per disquisitiones praecedentes, sectionem circuli in n partes, si n est numerus primus, ad solutionem tot aequationum, in quot factores resolvere licet numerum $n-1$, quarum aequationum gradus per magnitudinem factorum determinantur. Quoties itaque $n-1$ est potestas numeri 2, quod evenit 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 minusve complicatas (pro magnitudine ipsius n) exhiberi poterunt; quocirca in his casibus sectio circuli in n partes, sive descriptio polygoni regularis n laterum manifesto per constructiones geome-

tricas absolvi poterit. Ita *e. g.* pro $n = 17$ ex artt. 354, 361 facile pro cosinu anguli ${}_{17}^{1}P$ expressio haec derivatur:

$$-{}_{16}^{1}+{}_{16}^{1}\sqrt{17}+{}_{16}^{1}\sqrt{(34-2\sqrt{17})}+{}_{8}^{1}\sqrt{(17+3\sqrt{17}-\sqrt{(34-2\sqrt{17})}-2\sqrt{(34+2\sqrt{17})})}$$

cosinus multiplorum illius anguli formam similem, sinus autem uno signo radicali plus habent. Magnopere sane est mirandum, quod, quum iam Euclidis temporibus circuli divisibilitas geometrica in tres et quinque partes nota fuerit, nihil his inventis intervallo 2000 annorum adiectum sit, omnesque geometrae tamquam certum pronuntiaverint, praeter illas sectiones easque, quae sponte inde demanant, puta sectiones in 15, 3.2^{α}, 5.2^{β}, 15.2^{α} nec non in 2^{α} partes, nullas alias per constructiones geometricas absolvi 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 ullum numerum imparem ζ (unitate maiorem) divisibilis esset atque $m = \zeta\eta$, foret $2^m + 1$ divisibilis 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 $\nu = 0, 1, 2, 3, 4$ sive $m = 1, 2, 4, 8, 16$. 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 affirmaverat, omnes numeros sub illa forma contentos necessario primos esse; at ill. Euler hanc regulam iam pro $\nu = 5$ sive $m = 32$ erroneam esse, numero $2^{32} + 1 = 4294967297$ factorem 641 involvente, primus animadvertit.

Quoties autem $n - 1$ alios factores primos praeter 2 implicat, semper ad aequationes altiores deferimur; puta ad unam pluresve cubicas, quando 3 semel aut pluries inter factores primos ipsius $n - 1$ reperitur, ad aequationes quinti gradus, quando $n - 1$ divisibilis est per 5 etc., OMNIQUE RIGORE DEMONSTRARE POSSUMUS, HAS AEQUATIONES ELEVATAS NULLO MODO NEC EVITARI NEC AD INFERIORES REDUCI 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 ullo 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 solvere oportet; etiam has nullo modo nec evitare nec deprimere licet. Gradus itaque aequationum necessariarum e factoribus primis numeri $(a-1)a^{\alpha-1}$ generaliter (scilicet pro eo quoque casu ubi $\alpha = 1$) 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 $a^{\alpha}, b^{\beta}, c^{\gamma}$ etc. partes perfecisse (art. 336); quare ut gradus aequationum ad hunc finem necessarium cognoscantur, factores primos numerorum

$$(a-1)a^{\alpha-1},\ (b-1)b^{\beta-1},\ (c-1)c^{\gamma-1} \text{ etc.}$$

sive quod hic eodem redit producti ex his numeris considerare oportet. Observetur, hoc productum exprimere multitudinem numerorum ad N primorum ipsoque minorum (art. 38). Geometrice itaque sectio tunc tantummodo absolvitur, quando hic numerus est potestas binarii; quando vero factores primos alios quam 2 puta p, p' etc. implicat, aequationes gradus $p^{\text{ti}}, p'^{\text{ti}}$ etc. nullo modo evitari possunt. Hinc colligitur generaliter, ut circulus geometrice in N partes dividi 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 uno tali primo aut pluribus in 2 aut potestatem altiorem ipsius 2; sive brevius, requiritur, ut N neque ullum factorem primum imparem qui non est formae $2^m + 1$, implicet, neque etiam ullum 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 (ut 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 vindicavit (*Add. à l'Algèbre d'Euler p.* 525, ubi simul methodi indoles indicata est), Bachet inventum suum in editione secunda libri *Problémes plaisans et délectables qui se font par les nombres*, 1624, tradidit; in editione prima (à Lyon 1612), quam solam mihi videre licuit, nondum exstat, verumtamen iam annuntiatur.

Ad artt. 151, 296, 297. Ill. Le Gendre demonstrationem suam denuo exposuit in opere praeclaro *Essai d'une théorie des nombres* p. 214 sqq., attamen ita, ut nihil essentiale mutatum sit: quamobrem haec methodus etiamnum omnibus obiectionibus in art. 297 prolatis obnoxia manet. Theorema quidem (cui una suppositio innititur), in quavis progressione arithmetica $l, l+k, l+2k$ etc., numeros primos reperiri, si k et l divisorem 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 $4n+1$ positive sumtus), quae an *rigorose* demonstrari possit, nisi theorema fundamentale ipsum iam *supponatur*, nescio. Ceterum observare oportet, ill. Le Gendre hanc posteriorem suppositionem non tacite assumsisse, sed ipsum quoque eam non dissimulavisse, 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, ut nihil amplius desiderari possit, ill. Le Gendre in parte III operis sui p. 321—400 disquisitionem multo ampliorem instituit*). Principiis et methodis usus est a nostris prorsus diversis: attamen hac via compluribus difficultatibus implicatus est, quae effecerunt, ut theoremata palmaria demonstratione rigorosa munire non licuerit. Has difficultates ipse candide indicavit: sed ni fallimur hae quidem facilius forsan auferri poterunt, quam ea, quod in hac quoque disquisitione theorema modo memoratum (In quavis progressione arithmetica etc.) suppositum est, p. 371 annot. in fine.

Ad art. 306 VIII. In chiliade tertia determinantium negativorum reperti sunt 37 irregulares, inter quos 18 habent indicem irregularitatis 2, et 19 reliqui indicem 3.

Ad eundem X. Quaestionem hic propositam plene solvere 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, esse $= \gamma\pi = 2{,}3458847616$, designante γ eandem quantitatem ut in art. 302, et π ut ibidem semicircumferentiam circuli, cuius radius 1.

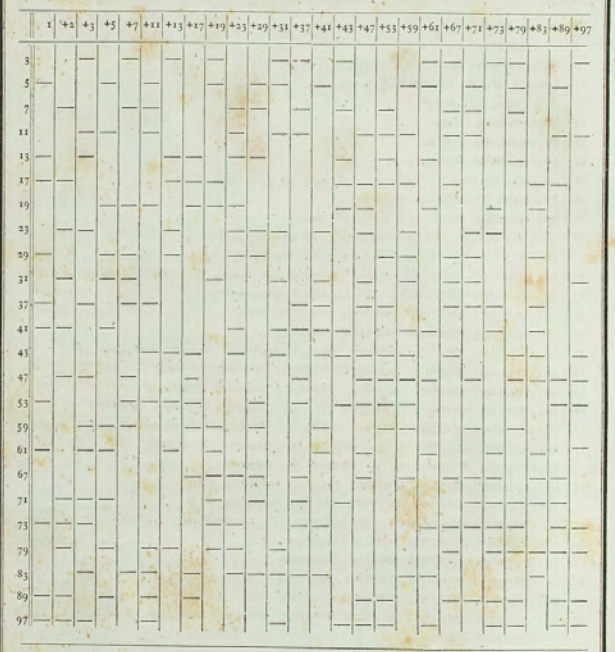
*) Vel nobis non monentibus lectores cavebunt, ne nostras formas ternarias cum eo, quod ill. Le Gendre *forme trinaire d'un nombre* dixit, confundant. Scilicet per hanc expressionem indicavit decompositionem numeri in tria quadrata.

TABULAE.

Tabula I. (artt. 58, 91).

		2. 3. 5. 7. 11	13. 17. 19. 23. 29	31. 37. 41. 43. 47	53. 59. 61. 67. 71	73. 79. 83. 89
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		
59	10	25. 32. 34. 44. 45	23. 14. 22. 27. 4	7. 41. 2. 13. 53	28	
61	10	47. 42. 14. 23. 45	30. 49. 22. 39. 25	13. 33. 18. 41. 40	51. 17	
64	5	*. 3. 1. 10. 5	15. 12. 7. 14. 11	8. 9. 14. 13. 12	5. 1. 3	
67	12	29. 9. 39. 7. 61	23. 8. 26. 20. 22	43. 44. 19. 63. 64	3. 54. 5	
71	62	58. 18. 14. 33. 43	27. 7. 38. 5. 4	13. 30. 55. 44. 17	59. 29. 37. 11	
73	5	8. 6. 1. 33. 55	59. 21. 62. 46. 35	11. 64. 4. 51. 31	53. 5. 58. 50. 44	
79	29	50. 71. 34. 19. 70	74. 9. 10. 52. 1	76. 25. 21. 47. 55	7. 17. 75. 54. 33	4
81	11	25. *. 35. 22. 1	38. 15. 12. 5. 7	14. 24. 29. 10. 13	45. 53. 4. 20. 33	48. 52
83	50	3. 52. 81. 24. 72	67. 4. 59. 16. 36	32. 60. 38. 49. 69	13. 20. 34. 53. 17	43. 47
89	30	72. 87. 18. 7. 4	65. 82. 53. 31. 29	57. 77. 67. 59. 34	10. 45. 19. 32. 26	68. 46. 27
97	10	86. 2. 11. 53. 82	83. 19. 27. 79. 47	26. 41. 71. 44. 60	14. 65. 32. 51. 25	20. 42. 91. 18

Tabula II. (art. 99).



Tabula 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)..05882352941 17647
19	(0)..05263157894 73684211
23	(0)..04347826086 95652173913
27	(0)..037; (1)..074; (2)..148; (3)..296; (4)..592; (5)..185
29	(0)..03448275862 06896551724 13793103
31	(0)..03225806451 61290; (1)..54838709677 41935
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)..02325581395 34883720930 23; (1)..65116279069 76744186046 4
47	(0)..02127659574 46808510638 29787234042 55319148936 17;
49	(0)..02040816326 53061224489 79591836734 69387755102 51
53	(0)..01886792452 83; (1)..49056603773 584; (2)..75471698113 320; (3)..62264150943 396
59	(0)..01694915254 23728813559 32203389830 50847457627 11864406779661
61	(0)..01639344262 29508196721 31147540983 60655737704 91803278688524590
67	(0)..01492537313 43283582089 55223880597; (1)..17910447761 19402985074 62686567164
71	(0)..01408450704 22535211267 60563380281 69; (1)..87323943661 97183098591 54929577464 78;
73	(0)..01369863; (1)..06849315; (2)..34246575; (3)..71232876; (4)..56164383 (5)..80821917; (6)..04109589; (7)..20547945; (8)..02739726
79	(0)..01265822784 81; (1)..36708860759 49; (2)..64556962025 31;
	(3)..72151898734 177; (4)..92405063291 139; (5)..79746835443 303
81	(0)..01234567901 23456790123 45679012345 67901234567 90123456790 12345679; (1)..13580246913 58024691358 02469135802 46913580246 91358024691 35802469; (2)..49382716049 38271604938 27160493827 16049382716 04938271604 93827160; (3)..43209876543 20987654320 98765432098 76543209876 54320987654 32098765; (4)..75308641975 30864197530 86419753086 41975308641 97530864197 53086419; (5)..28395061728 39506172839 50617283950 61728395061 72839506172 83950617
83	(0)..01204819277 10843373493 97590361445 78313253; 3
	(1)..60240963855 42168674698 79518072289 15662650; 0
89	(0)..01123595505 61797752808 98876404494 38202247191
	(1)..33707865168 53932584269 66292134831 46067415730
97	(0)..01030927835 05154639175 32577319587 62886597938 14432989690 72164948453 60824742268041 23711340206 185567

CONTENTA.

GOSLARIAE EX OFFICINA E. W. G. KIRCHER.

ANHANG.

HANDSCHRIFTLICHE AUFZEICHNUNGEN VON GAUSS.

Zu Art. 40. *Accedente numero tertio C, sit λ' maximus divisor communis numerorum λ, C, determinenturque numeri k, γ ita ut sit $k\lambda + \gamma C = \lambda'$, unde erit $k\alpha A + k\beta B + \gamma C = \lambda'$. Manifesto autem λ' est divisor communis numerorum A, B, C, et quidem maximus, si enim exstaret major $= \theta$, foret*

$$k\alpha \cdot \frac{A}{\theta} + k\beta \cdot \frac{B}{\theta} + \gamma \cdot \frac{C}{\theta} = \frac{\lambda'}{\theta} \quad \textit{integer, Q. E. A.}$$

Factum est itaque quod propositum fuerat, dum statuimus $k\alpha = a$, $k\beta = b$, $\gamma = c$, $\lambda' = \mu$.

Zu Art. 114. *Concinnius demonstratio ita adornatur* $(a^{3n} - a^n)^2 = 2 + (a^{4n} + 1)(a^{2n} - 2)$, $(a^{3n} + a^n)^2 = -2 + (a^{4n} + 1)(a^{2n} + 2)$ *adeoque* $\sqrt{2} \equiv \pm (a^{3n} - a^n)$, $\sqrt{-2} \equiv \pm (a^{3n} + a^n) \pmod{nn + 1}$

Zu den in Art. 256 VI angegebenen 16 positiven Determinanten von der Form $8n + 5$, für welche die Anzahl der eigentlich primitiven Classen drei mal grösser ist als die der uneigentlich primitiven '37, .. 573' sind hinzugefügt: *677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997 adeoque inter 125 exstant 31.*

Zu den Worten des Art. 361: Hoc modo summa mult. gen. pro dett. -1 usque ad -100 invenitur $= 234{,}4$ quum revera sit $233. - -$ *a -1 usque ad -3000, tabula 11166, formula 11167,9.*

Zu Art. 336. *Wären alle Zahlen der Form $2^{2^n} + 1$ Primzahlen, so würde ein hinlänglich genäherter Ausdruck für die Menge der in Rede stehenden Zahlen (N) kleiner als die gegebene Zahl M, folgender sein* $\frac{1}{2}\left(\frac{\log M}{\log 2}\right)^2$.

Zu dem Lehrsatze in Art. 42 über die Theiler einer algebraischen ganzen rationalen Function mit ganzzahligen Coëfficienten $- -$ *1797 Jul. 22.*

Zu den Worten des Art. 130: Postquam rigorose demonstravimus, quemvis numerum primum formae $4n + 1$, et positive et negative acceptum, alicuivis numeri primi ipso minoris non-residuum esse; $- -$ *Hanc demonstrationem deteximus 1796 Apr. 8.*

Zu Art. 131. *Theorema fundamentale per inductionem detectum 1795 Martio.*
Demonstratio prima, quae in hac sectione traditur, inventa 1796 Apr.

Zu den Worten des Art. 133: Investigationem (theor. fund.) adhuc generalius instituamus. Contemplemur duos numeros quoscunque impares inter se primos, signis quibuscunque affectos, P et Q. — — *1796 Apr. 29.*

Zu den Worten des Art. 145: Praeterea theoremata ad residua $+2$ et -2 pertinentia tunc supponi debuissent; quum vero nostra demonstratio absque his theorematibus sit perfecta, novam hinc methodum nanciscimur, illa demonstrandi. — — *1797 Febr. 4.*

Zu der Ueberschrift der Sectio quinta: De formis aequationibusque indeterminatis secundi gradus. — — *Inde a Jun. 22. 1796.*

Zu den Worten des Art. 234: . . ad aliud argumentum gravissimum transimus a nemine hucusque attactum, de formarum compositione. — — *Haec disquiss. inchoatae autumno 1798.*

Zu den Worten des Art. 262: Ex hoc principio methodum novam haurire possumus, non modo theorema fundamentale, sed etiam reliqua theoremata Sect. praec. ad residua -1, $+2$, -2 pertinentia demonstrandi, — — *Principia huius methodi primum se obtulerant 1796 Jul. 27, at exculta et ad formam praesentem reducta Vere a. 1800.*

Zu den Worten des Art. 266: . . sed quoniam complures veritates ad has spectantes, eaeque pulcherrimae, adhuc supersunt, quarum fons proprius in theoria formarum ternariarum secundi gradus est quaerendus, brevem ad hanc theoriam digressionem hic intercalamus. — — *Febr. 14. 1799.*

Zu den Worten des Art. 272: scilicet ostendendo, primo, quo pacto quaevis forma ternaria ad formam simpliciorem reduci possit, dein, formarum simplicissimarum (ad quas per tales reductiones perveniatur), multitudinem pro quovis determinante dato esse finitam. — — *1800 Febr. 13.*

Zu den Worten des Art. 287 III: Prorsus simili ratione probatur, in ordine improprie primitivo eos characteres, qui per praecepta art. 264 II, III soli possibiles inveniuntur, omnes possibiles esse, sive sint P sive Q. — Haecce theoremata, etc. — — *Demonstratione primum munita sunt Mense Aprili 1798.*

Zu den Worten des Art. 302: Multitudo classium mediocris autem (quae definitione opus non habebit) valde regulariter crescit, — — *Idea prima initio a. 1799.*

Zu den Worten des Art. 306 X: Denique observamus, 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, ut inter ipsum atque determinantem, ad quem pertinet, nexus generalis detegatur. — — *Ex voto nobis ac sic successit ut nihil amplius desiderandum supersit Nov. 30—Dec. 3. 1800.*

Zu Art. 306. *Circulum in 17 partes divisibilem esse geometrice, deteximus 1796 Mart. 30.*

SCHLUSSBEMERKUNG ZUR NEUEN AUSGABE.

Dieser erste Band von Gauss Werken ist ein Wiederabdruck der im Jahre 1801 in Octav erschienenen sieben Sectionen der Disquis. Arithm. Die achte Section, auf die an mehren Stellen verwiesen wird und die Gauss wol anfangs mit den übrigen zu veröffentlichen beabsichtigte, findet sich unter seinen Handschriften. Da er die Ausarbeitung derselben aber nicht in gleicher Weise abgeschlossen hat wie die der sieben ersten Sectionen, so wird sie in dieser Ausgabe den arithmetischen Abhandlungen des Nachlasses sich anschliessen.

Textänderungen sind in den Disqu. Ar. nur an folgenden Stellen vorgenommen:

In Art. 125 sind die beiden Einschaltungen ($si > 6$) und (> 17; sed $-13 N 3$, $-17 N 5$) eingefügt worden.

In Art. 126. *Demonstr.* ist 'in serie (I) a terminos esse per p divisibiles, b terminos per p^2 divisibiles, c terminos per p^3 divisibiles etc.' statt 'in serie (I) a terminos esse per p divisibiles neque vero per p^2, b terminos per p^2 non autem per p^3 divisibiles, c terminos per p^3 non autem per p^4 etc.' gesetzt worden.

In Art. 128 III sind die nach 'Si enim $+b$ vel $-b \equiv r \pmod p$, erit $bb \equiv rr \pmod{2p}$, adeoque terminus $\frac{1}{2}(a-bb)$ per p divisibilis.' in der Ausgabe von 1801 noch folgenden Worte 'multoque magis $2(a-bb)$.' ausgelassen.

In Art. 129 ist überall $2\sqrt{a+1}$ statt $2\sqrt{a}$ und demnach 9 statt 1 als diejenige Zahl, bis zu welcher a jedenfalls nicht herabgeht, gesetzt worden.

In Art. 130 lautete der Schluss der Untersuchung über den Fall (4) 'Facile vero perspicitur, ex ista aequatione deduci posse haec $a'pRh$, $\pm ahpRa'$, $\pm aa'hRp$; quae cum iis quae in (2) invenimus conveniunt. In reliquis autem demonstratio est eadem.' Dieses ist gemäss der Note geändert, die Gauss dem Art. 2 der Abhandlung *Theorematis arithmetici demonstratio nova* beigefügt hat: 'Haud abs re erit, levem aliquem errorem, qui nescio qua negligentia in illius demonstrationis expositionem irrepsit, hic indicare atque corrigere. Pag. (108) inde a l. (14) ratiocinia sequentia sunt substituenda: Facile vero perspicitur, ex ista aequatione deduci posse haec $a'pRh \ldots (\alpha)$; $\pm ahRa' \ldots (\beta)$; $\pm ahRp \ldots (\gamma)$. Ex (α) quod convenit cum (α) in (2) sequitur perinde ut illic, esse vel simul hRp, hRa', vel hNp, hNa'. Sed in casu priori foret per (β), aRa' contra hyp.; quare erit hNp, adeoque per (γ) etiam aNp.

In Art. 171 ist zufolge einer handschriftlichen Bemerkung 'in qua A nec maior quam $\sqrt{\frac{4}{3}}D$, C, nec minor quam $2B$' statt 'in qua A non $>\sqrt{\frac{4}{3}}D$, B non $>\frac{1}{2}A$, C non $<A$' gesetzt worden.

In Art. 174. *Methodus secunda.* ist 'Quum a non erit $>\sqrt{\frac{4}{3}}D$, omnes formae quae hoc modo prodeunt, manifesto erunt reductae.' gesetzt statt 'Si quae formae hoc modo prodeunt, in quibus $a>\sqrt{\frac{4}{3}}D$, erunt reiiciendae, reliquae vero omnes manifesto erunt reductae.'

In Art. 256 VI enthält die frühere Ausgabe unter den positiven Determinanten von der Form $8n+5$, für welche die Anzahl der Classen in der eigentlich primitiven Ordnung dreimal grösser ist als die in der uneigentlich primitiven, auch den Determinant 397, dem aber von beiden Arten gleich viel Classen zugehören.

In Art. 302 ist zufolge einer handschriftlichen Bemerkung die Anzahl der Classen für das zweite Tausend der negativen Determinanten zu 28595 angegeben und nicht zu 28603, wie in der frühern Ausgabe steht.

In Art. 303 sind für die Classificationen II. 4; II. 5; IV. 2 die Mengen der Determinanten nach den im Nachlass vorgefundenen Tafeln zu 31, 44, 69 angegeben und nicht wie in der früheren Ausgabe zu 32, 42, 68.

In Art. 325 ist '23ℓ, $23\ell\pm1$, $23\ell\pm5$, $23\ell\pm7$, $23\ell\pm9$, $23\ell\pm10$. His deletis superstites inveniuntur 119, 127, qui duo soli ipsi V valorem quadratum conciliant', gesetzt statt '23ℓ, $23\ell\pm5$, $23\ell\pm7$, $23\ell\pm9$, $23\ell\pm10$. His deletis superstites inveniuntur 119, 127, 137, e quibus duo priores soli ipsi V valorem quadratum conciliant.'

In Art. 360 IV sind die Worte 'quum pro plerisque aliis aequationibus cubicis, quarum radices omnes reales sunt, simul anguli et rationis trisectio evitari nequeat.' die auf: '*e. g.* pro $6=3$ sola trisectio anguli', folgten, und deren Unrichtigkeit Gauss in seinem Handexemplare notirt hat, ausgelassen.

Die Noten auf Seite 80, 102, 133, 211, 263, 265, 419, sind dem handschriftlichen Nachlasse entlehnt.

Die äussere Form ist bei der neuen Ausgabe zur Erleichterung der Uebersicht einigen Abänderungen gegen den Druck dieses Werkes im Jahre 1801 unterworfen, man glaubte sich dazu um so mehr berechtigt, als Gauss ausgesprochener Weise auch in anderen Punkten auf Raumersparniss Rücksicht genommen. Viele Formeln, die der Textzeile eingeschlossen waren, sind abgesondert herausgesetzt. Die Inhaltsangaben, die zusammengestellt dem Werke vorangingen, sind auch den einzelnen Abtheilungen und nicht nur den Sectionen wie in der ersten Ausgabe beigefügt, die allgemeineren darunter sind den Seiten als Überschrift gegeben.

GÖTTINGEN,
GEDRUCKT IN DER DIETERICHSCHEN UNIVERSITÄTS-DRUCKEREI
W. FR. KAESTNER.

C. F. GAUSS WERKE

erscheinen in der nachstehenden Reihenfolge der Bände:

I. DISQUISITIONES ARITHMETICAE.
II. HÖHERE ARITHMETIK.
III. ANALYSIS.
IV. GEOMETRIE UND METHODE DER KLEINSTEN QUADRATE.
V. MATHEMATISCHE PHYSIK.
VI. ASTRONOMIE.

Die THEORIA MOTUS CORPORUM COELESTIUM wird als VII. Band, sobald es möglich ist, nachfolgen.

GÖTTINGEN
GEDRUCKT IN DER DIETERICHSCHEN UNIVERSITÄTS-BUCHDRUCKEREI.
W. FR. KAESTNER.