THEOREMATIS ARITHMETICI

DEMONSTRATIO NOVA

A U C T O R E

CAROLO FRIDERICO GAUSS

SOCIETATI REGIAE SCIENTIARUM TRADITA IAN. 15. 1808.

Commentationes societatis regiae scientiarum Gottingensis. Vol. XVI.

Gottingae MDCCCVIII.

THEOREMATIS ARITHMETICI

DEMONSTRATIO NOVA.

1.

Quaestiones ex arithmetica sublimiori saepenumero phaenomenon singulare offerunt, quod in analysi longe rarius occurrit, atque ad illarum illecebras augendas multum confert. Dum scilicet in disquisitionibus analyticis plerumque ad veritates novas pertingere non licet, nisi prius principiis, quibus innituntur quaeque ad eas viam quasi patefacere debent, penitus potiti simus: contra in arithmetica frequentissime per inductionem fortuna quadam inopinata veritates elegantissimae novae prosiliunt, quarum demonstrationes tam profunde latent tantisque tenebris obvolutae sunt, ut omnes conatus eludant, acerrimisque perscrutationibus aditum denegent. Tantus porro adest tamque mirus inter veritates arithmeticas, primo aspectu maxime heterogeneas, nexus, ut haud raro, dum longe alia quaerimus, tandem ad demonstrationem tantopere exoptatam longisque antea meditationibus frustra quaesitam longe alia via quam qua exspectata fuerat felicissime perveniamus. Plerumque autem huiusmodi veritates eius sunt indolis, ut pluribus viis valde diversis adiri queant, nec semper viae brevissimae sint, quae primo se offerunt. In magno itaque certe pretio habendum erit, si, tali veritate longe incassum ventilata, dein demonstrata quidem sed per ambages abstrusiores, tandem viam simplicissimam atque genuinam detegere contigerit.

2.

Inter quaestiones, de quibus in art. praec. diximus, locum insignem tenet theorema omnem fere theoriam residuorum quadraticorum continens, quod in *Disquisitionibus arithmeticis* (Sect. IV) *theorematis fundamentalis* nomine distinctum est.

Pro *primo* huius elegantissimi theorematis inventore ill. LEGENDRE absque dubio habendus est, postquam longe antea summi geometrae EULER et LAGRANGE plures eius casus speciales iam per inductionem detexerant. Conatibus horum virorum circa demonstrationem enumerandis hic non immoror; adeant quibus volupe est opus modo commemoratum. Adiicere liceat tantummodo, in confirmationem eorum, quae in art. praec. prolata sunt, quae ad meos conatus pertinent. In ipsum theorema proprio marte incideram anno 1795, dum omnium, quae in arithmetica sublimiori iam elaborata fuerant, penitus ignarus et a subsidiis literariis omnino praeclusus essem: sed per integrum annum me torsit, operamque enixissimam effugit, donec tandem demonstrationem in Sectione quarta operis illius traditam nactus essem. Postea tres aliae principiis prorsus diversis innixae se mihi obtulerunt, quarum unam in Sectione quinta tradidi, reliquas elegantia illa haud inferiores alia occasione publici iuris faciam. Sed omnes hae demonstrationes, etiamsi respectu rigoris nihil desiderandum relinquere videantur, e principiis nimis heterogeneis derivatae sunt, prima forsan excepta, quae tamen per ratiocinia magis laboriosa procedit, operationibusque prolixioribus premitur. Demonstrationem itaque *genuinam* hactenus haud affuisse non dubito pronunciare: esto iam penes peritos iudicium, an ea, quam nuper detegere successit, quamque pagellae sequentes exhibent, hoc nomine decorari mereatur.

3.

THEOREMA. *Sit p numerus primus positivus; k integer quicunque per p non divisibilis;*

$$A \text{ complexus numerorum } 1, 2, 3 \ldots \tfrac{1}{2}(p-1)$$

$$B \text{ complexus horum } \tfrac{1}{2}(p+1), \tfrac{1}{2}(p+3), \tfrac{1}{2}(p+5) \ldots p-1$$

Capiantur residua minima positiva productorum ex k in singulos numeros A secundum modulum p, quae manifesto omnia diversa erunt, atque partim ad A partim ad B pertinebunt. Iam si ad B omnino μ residua pertinere supponantur, erit k vel residuum vel non-residuum quadraticum ipsius p, prout μ par est vel impar.

Dem. Sint residua ad A pertinentia haec a, a', $a'' \ldots$, reliqua ad B pertinentia b, b', $b'' \ldots$, patetque posteriorum complementa $p-b$, $p-b'$, $p-b'' \ldots$ cuncta a numeris a, a', $a'' \ldots$ diversa esse, cum his vero simul sumta complexum A explere. Habemus

itaque

$$1.2.3\ldots\tfrac{1}{2}(p-1) = aa'a''\ldots(p-b)(p-b')(p-b'')\ldots$$

Productum posterius autem manifesto fit

$$\equiv (-1)^{\mu} aa'a''\ldots bb'b''\ldots \equiv (-1)^{\mu} k.2k.3k\ldots\tfrac{1}{2}(p-1)k$$
$$\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)} 1.2.3\ldots\tfrac{1}{2}(p-1) \pmod{p}$$

Hinc erit

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

sive $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, prout μ par est vel impar, unde theorema nostrum protinus demanat.

4.

Ratiocinia sequentia magnopere abbreviare licebit per introductionem quarundam designationum idonearum. Exprimet igitur nobis character (k,p) multitudinem productorum ex his

$$k, 2k, 3k\ldots\tfrac{1}{2}(p-1)k,$$

quorum residua minima positiva secundum modulum p huius semissem superant. Porro existente x quantitate quacunque non integra, per signum $[x]$ exprimemus integrum ipsa x proxime minorem, ita ut $x-[x]$ semper fiat quantitas positiva intra limites 0 et 1 sita. Levi iam negotio relationes sequentes evolventur:

I. $[x]+[-x] = -1$.

II. $[x]+h = [x+h]$, quoties h est integer.

III. $[x]+[h-x] = h-1$

IV. Si $x-[x]$ est fractio minor quam $\frac{1}{2}$, erit $[2x]-2[x] = 0$; si vero $x-[x]$ est maior quam $\frac{1}{2}$, erit $[2x]-2[x] = 1$.

V. Iacente itaque residuo minimo positivo integri h secundum modulum p infra $\frac{1}{2}p$, erit $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 0$; iacente autem residuo illo ultra $\frac{1}{2}p$, erit $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 1$.

VI. Hinc statim sequitur $(k,p) =$

$$\left[\tfrac{2k}{p}\right] + \left[\tfrac{4k}{p}\right] + \left[\tfrac{6k}{p}\right] \ldots + \left[\tfrac{(p-1)k}{p}\right]$$
$$-2\left[\tfrac{k}{p}\right] - 2\left[\tfrac{2k}{p}\right] - 2\left[\tfrac{3k}{p}\right] \ldots - 2\left[\tfrac{\frac{1}{2}(p-1)k}{p}\right].$$

VII. Ex VI. et I. nullo negotio derivatur

$$(k,p) + (-k,p) = \tfrac{1}{2}(p-1)$$

Unde sequitur, $-k$ vel eandem vel oppositam relationem ad p habere (quatenus huius residuum aut non-residuum quadraticum est) ut $+k$, prout p vel formae $4n+1$ fuerit, vel formae $4n+3$. In casu priori manifesto -1 residuum, in posteriori non-residuum ipsius p erit.

VIII. Formulam in VI. traditam sequenti modo transformabimus. Per III. fit

$$\left[\tfrac{(p-1)k}{p}\right] \equiv k-1-\left[\tfrac{k}{p}\right], \left[\tfrac{(p-3)k}{p}\right] = k-1-\left[\tfrac{3k}{p}\right], \left[\tfrac{(p-5)k}{p}\right] = k-1-\left[\tfrac{5k}{p}\right] \ldots$$

Applicando hasce substitutiones ad $\frac{p\mp 1}{4}$ membra ultima seriei superioris in illa expressione, habebimus

primo, quoties p est formae $4n+1$

$$(k,p) = \tfrac{1}{4}(k-1)(p-1)$$
$$-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-3)k}{p}\right]\right\}$$
$$-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{3k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

secundo, quoties p est formae $4n+3$

$$(k,p) = \tfrac{1}{4}(k-1)(p+1)$$
$$-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$
$$-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{3k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

IX. Pro casu speciali $k = +2$ e formulis modo traditis sequitur $(2,p) = \frac{1}{4}(p\mp 1)$, sumendo signum superius vel inferius, prout p est formae $4n+1$ vel $4n+3$. Erit itaque $(2,p)$ par, adeoque $2Rp$, quoties p est formae $8n+1$ vel $8n+7$; contra erit $(2,p)$ impar atque $2Np$, quoties p est formae $8n+3$ vel $8n+5$.

5.

THEOREMA. *Sit x quantitas positiva non integra, inter cuius multipla x, $2x$, $3x\ldots$ usque ad nx nullum fiat integer; ponatur $[nx]=h$, unde facile concluditur, etiam inter multipla quantitatis reciprocae $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x}\ldots$ usque ad $\frac{h}{x}$ integrum non reperiri. Tum dico fore*

$$\left.\begin{array}{r}[x]+[2x]+[3x]\cdots+[nx]\\ +\left[\frac{1}{x}\right]+\left[\frac{2}{x}\right]+\left[\frac{3}{x}\right]\ldots+\left[\frac{h}{x}\right]\end{array}\right\}=nh$$

Dem. Seriei $[x]+[2x]+[3x]\ldots+[nx]$, quam ponemus $=\Omega$, membra prima usque ad $\left[\frac{1}{x}\right]^{\text{tum}}$ inclus. manifesto omnia erunt $=0$; sequentia usque ad $\left[\frac{2}{x}\right]^{\text{tum}}$ cuncta $=1$; sequentia usque ad $\left[\frac{3}{x}\right]^{\text{tum}}$ cuncta $=2$ et sic porro. Hinc fit

$$\left.\begin{array}{l}\Omega=0\times\left[\frac{1}{x}\right]\\ \quad+1\times\left\{\left[\frac{2}{x}\right]-\left[\frac{1}{x}\right]\right\}\\ \quad+2\times\left\{\left[\frac{3}{x}\right]-\left[\frac{2}{x}\right]\right\}\\ \quad+3\times\left\{\left[\frac{4}{x}\right]-\left[\frac{3}{x}\right]\right\}\\ \qquad\text{etc.}\\ \quad+(h-1)\left\{\left[\frac{h}{x}\right]-\left[\frac{h-1}{x}\right]\right\}\\ \quad+h\left\{n-\left[\frac{h}{x}\right]\right\}\end{array}\right\}=hn-\left[\frac{1}{x}\right]-\left[\frac{2}{x}\right]-\left[\frac{3}{x}\right]\ldots-\left[\frac{h}{x}\right]$$

Q. E. D.

6.

THEOREMA. *Designantibus k, p numeros positivos impares inter se primos quoscunque, erit*

$$\left.\begin{array}{r}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{array}\right\}=\tfrac{1}{4}(k-1)(p-1).$$

Demonstr. Supponendo, quod licet, $k<p$, erit $\frac{\frac{1}{2}(p-1)k}{p}$ minor quam $\frac{1}{2}k$, sed maior quam $\frac{1}{2}(k-1)$, adeoque $\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=\frac{1}{2}(k-1)$. Hinc patet, theorema praesens ex praec. protinus sequi, statuendo illic $\frac{k}{p}=x$, $\frac{1}{2}(p-1)=n$, adeoque $\frac{1}{2}(k-1)=h$.

Ceterum simili modo demonstrari potest, si k fuerit numerus *par* ad p primus, fore

$$\left.\begin{array}{r}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}kp}{k}\right]\end{array}\right\}=\tfrac{1}{4}k(p-1)$$

At huic propositioni ad institutum nostrum non necessariae non immoramur.

7.

Iam ex combinatione theorematis praec. cum propos. VIII. art. 4. theorema fundamentale protinus demanat. Nimirum denotantibus k, p numeros primos positivos inaequales quoscunque, et ponendo

$$(k,p)+\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=L$$

$$(p,k)+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]=M$$

per VIII. art. 4. patet, L et M semper fieri numeros pares. At per theorema art. 6. erit

$$L+M=(k,p)+(p,k)+\tfrac{1}{4}(k-1)(p-1)$$

Quoties igitur $\frac{1}{4}(k-1)(p-1)$ par evadit, quod fit, si vel uterque k, p vel saltem alteruter est formae $4n+1$, necessario (k,p) et (p,k) vel ambo pares vel ambo impares esse debent. Quoties autem $\frac{1}{4}(k-1)(p-1)$ impar est, quod evenit, si uterque k, p est formae $4n+3$, necessario alter numerorum (k,p), (p,k) par, alter impar esse debebit. In casu priori itaque relatio ipsius k ad p et relatio ipsius p ad k (quatenus alter alterius residuum vel non-residuum est) identicae erunt, in casu posteriori oppositae.

Q. E. D.

SUMMATIO

QUARUMDAM SERIERUM

SINGULARIUM

A U C T O R E

CAROLO FRIDERICO GAUSS

EXHIBITA SOCIETATI D. XXIV. AUGUST. MDCCCVIII.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. I.
Gottingae MDCCCXI.

SUMMATIO

QUARUMDAM SERIERUM SINGULARIUM.

1.

Inter veritates insigniores, ad quas theoria divisionis circuli aditum aperuit, locum haud ultimum sibi vindicat summatio in Disquiss. Arithmet. art. 356 proposita, non modo propter elegantiam suam peculiarem, miramque foecunditatem, quam fusius exponendi occasionem posthac dabit alia disquisitio, sed ideo quoque, quod eius demonstratio rigorosa atque completa difficultatibus haud vulgaribus premitur. Quae sane eo minus exspectari debuissent, quum non tam in ipsum theorema cadant, quam potius in aliquam theorematis limitationem, qua neglecta demonstratio statim in promtu est, facillimeque e theoria in opere isto explicata derivatur. Theorema illic exhibitum est in forma sequente. Supponendo n esse numerum primum, denotandoque indefinite omnia residua quadratica ipsius n inter limites 1 et $n-1$ incl. sita per a, omniaque non-residua inter eosdem limites iacentia per b, denique per ω arcum $\frac{360^\circ}{n}$, et per k integrum determinatum quemcunque per n non divisibilem, erit

I. pro valore ipsius n, qui est formae $4m+1$,

$$\Sigma \cos akw = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}$$

$$\Sigma \cos bkw = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ adeoque}$$

$$\Sigma \cos akw - \Sigma \cos bkw = \pm\sqrt{n}$$

$$\Sigma \sin akw = 0$$

$$\Sigma \sin bkw = 0$$

II. pro valore ipsius n, qui est formae $4m+3$,

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$
$$\Sigma \sin ak\omega = \pm\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin bk\omega = \mp\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = \pm\sqrt{n}$$

Hae summationes l.c. omni rigore demonstratae sunt, neque alia difficultas hic remanet nisi in determinatione *signi* quantitati radicali praefigendi. Nullo quidem negotio ostendi potest, hoc signum eatenus a numero k pendere, quod semper pro cunctis valoribus ipsius k, qui sint residua quadratica ipsius n, signum *idem* valere debeat, et contra signum huic oppositum pro omnibus valoribus ipsius k, qui sint non-residua quadratica ipsius n. Hinc totum negotium in valore $k = 1$ versabitur, patetque, quam primum signum pro hoc valore valens innotuerit, pro omnibus quoque reliquis valoribus ipsius k signa statim in promtu fore. Verum enim vero in hac ipsa quaestione, quae primo aspectu inter faciliores referenda videtur, in difficultates improvisas incidimus, methodusque, qua ducente sine impedimentis hucusque progressi eramus, auxilium ulterius prorsus denegat.

2.

Haud abs re erit, antequam ulterius progrediamur, quaedam exempla summationis nostrae per calculum numericum evolvisse: huic vero quasdam observationes generales praemittere conveniet.

I. Si in casu eo, ubi n est numerus primus formae $4m+1$, omnia residua quadratica ipsius n inter 1 et $\frac{1}{2}(n-1)$ incl. iacentia indefinite per a' exhibentur, omniaque non-residua inter eosdem limites per b', constat, omnes $n-a'$ inter ipsos a, omnesque $n-b'$ inter b comprehensos fore: quamobrem quum omnes a', b', $n-a'$, $n-b'$ manifesto totum complexum numerorum 1, 2, $3 \ldots n-1$ expleant, omnes a' cum omnibus $n-a'$ iuncti omnes a complectentur, et perinde omnes b' cum omnibus $n-b'$ iuncti omnes b comprehendent. Hinc erit

$$\Sigma \cos ak\omega = \Sigma \cos a'k\omega + \Sigma \cos(n-a')k\omega$$
$$\Sigma \cos bk\omega = \Sigma \cos b'k\omega + \Sigma \cos(n-b')k\omega$$
$$\Sigma \sin ak\omega = \Sigma \sin a'k\omega + \Sigma \sin(n-a')k\omega$$
$$\Sigma \sin bk\omega = \Sigma \sin b'k\omega + \Sigma \sin(n-b')k\omega$$

Iam quum habeatur $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, $\sin(n-b')k\omega = -\sin b'k\omega$, patet sponte fieri

$$\Sigma \sin ak\omega = \Sigma \sin a'k\omega - \Sigma \sin a'k\omega = 0$$
$$\Sigma \sin bk\omega = \Sigma \sin b'k\omega - \Sigma \sin b'k\omega = 0$$

Summatio cosinuum vero hanc formam assumit

$$\Sigma \cos ak\omega = 2\Sigma \cos a'k\omega$$
$$\Sigma \cos bk\omega = 2\Sigma \cos b'k\omega$$

unde fieri debebit

$$1 + 4\Sigma \cos a'k\omega = \pm\sqrt{n}$$
$$1 + 4\Sigma \cos b'k\omega = \mp\sqrt{n}$$
$$2\Sigma \cos a'k\omega - 2\Sigma \cos b'k\omega = \pm\sqrt{n}$$

II. In casu eo, ubi n est formae $4m+3$, complementum cuiusvis residui a ad n erit non-residuum, complementumque cuiusvis b erit residuum; quocirca omnes $n-a$ convenient cum omnibus b, omnesque $n-b$ cum omnibus a. Hinc colligitur

$$\Sigma \cos ak\omega = \Sigma \cos(n-b)k\omega = \Sigma \cos bk\omega$$

quare quum omnes a et b iuncti omnes numeros 1, 2, $3 \ldots n-1$ expleant, adeoque fiat $\Sigma \cos ak\omega + \Sigma \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \text{etc.} + \cos(n-1)k\omega = -1$, summationes

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$

sponte sunt obviae. Perinde erit

$$\Sigma \sin ak\omega = \Sigma \sin(n-b)k\omega = -\Sigma \sin bk\omega$$

unde patet, quomodo summationum

$$2\Sigma \sin ak\omega = \pm\sqrt{n}$$
$$2\Sigma \sin bk\omega = \mp\sqrt{n}$$

altera ab altera pendeat.

3.

Ecce iam computum numericum pro aliquot exemplis:

I. Pro $n = 5$ adest valor unus ipsius a', puta $a' = 1$, valorque unus ipsius b', puta $b' = 2$; est autem

$$\cos\omega = +0{,}3090169944 \qquad \cos 2\omega = -0{,}8090169944$$

adeoque $1 + 4\cos\omega = +\sqrt{5},\ 1 + 4\cos 2\omega = -\sqrt{5}$.

II. Pro $n = 13$ adsunt tres valores ipsius a', puta 1, 3, 4, totidemque valores ipsius b', puta 2, 5, 6, unde computamus

$\cos\omega = +0{,}8854560257$	$\cos 2\omega = +0{,}5680647467$
$\cos 3\omega = +0{,}1205366803$	$\cos 5\omega = -0{,}7485107482$
$\cos 4\omega = -0{,}3546048870$	$\cos 6\omega = -0{,}9709418174$
$\text{Summa} = +0{,}6513878190$	$\text{Summa} = -1{,}1513878189$

Hinc $1 + 4\sum \cos a'\omega = +\sqrt{13},\ 1 + 4\Sigma \cos b'\omega = -\sqrt{13}$.

III. Pro $n = 17$ habemus quatuor valores ipsius a', puta 1, 2, 4, 8, totidemque valores ipsius b', puta 3, 5, 6, 7. Hinc computantur cosinus

$\cos\omega = +0{,}9324722294$	$\cos 3\omega = +0{,}4457383558$
$\cos 2\omega = +0{,}7390089172$	$\cos 5\omega = -0{,}2736629901$
$\cos 4\omega = +0{,}0922683595$	$\cos 6\omega = -0{,}6026346364$
$\cos 8\omega = -0{,}9829730997$	$\cos 7\omega = -0{,}8502171357$
$\text{Summa} = +0{,}7807764064$	$\text{Summa} = -1{,}2807764065$

Hinc $1 + 4\Sigma \cos a'\omega = +\sqrt{17}, 1 + 4\Sigma \cos b'\omega = -\sqrt{17}$.

IV. Pro $n = 3$ adest valor unicus ipsius a, puta $a = 1$, cui respondet

$$\sin\omega = +0{,}8660254038$$

Hinc $2\sin\omega = +\sqrt{3}$.

V. Pro $n = 7$ adsunt valores tres ipsius a, puta 1, 2, 4: hinc habentur sinus

$$\begin{aligned}\sin\omega &= +0{,}7818314825\\ \sin 2\omega &= +0{,}9749279122\\ \sin 4\omega &= -0{,}4338837391\end{aligned}$$

$$\text{Summa} = +1{,}3228756556, \text{ adeoque } 2\Sigma\sin a\omega = +\sqrt{7}.$$

VI. Pro $n = 11$ valores ipsius a sunt 1, 3, 4, 5, 9, quibus respondent sinus

$$\begin{aligned}\sin\omega &= +0{,}5406408175\\ \sin 3\omega &= +0{,}9898214419\\ \sin 4\omega &= +0{,}7557495744\\ \sin 5\omega &= +0{,}2817325568\\ \sin 9\omega &= -0{,}9096319954\end{aligned}$$

$$\text{Summa} = +1{,}6583123952, \text{ et proin } 2\Sigma\sin a\omega = +\sqrt{11}.$$

VII. Pro $n = 19$ valores ipsius a sunt 1, 4, 5, 6, 7, 9, 11, 16, 17, quibus respondent sinus

$$\begin{aligned}\sin\omega &= +0{,}3246994692\\ \sin 4\omega &= +0{,}9694002659\\ \sin 5\omega &= +0{,}9965844930\\ \sin 6\omega &= +0{,}9157733267\\ \sin 7\omega &= +0{,}7357239107\\ \sin 9\omega &= +0{,}1645945903\\ \sin 11\omega &= -0{,}4759473930\\ \sin 16\omega &= -0{,}8371664783\\ \sin 17\omega &= -0{,}6142127127\end{aligned}$$

$$\text{Summa} = +2{,}1794494718, \text{ adeoque } 2\Sigma\sin a\omega = +\sqrt{19}.$$

4.

In omnibus hisce exemplis quantitas radicalis signum positivum obtinet, idemque facile pro valoribus maioribus $n = 23$, $n = 29$ etc. confirmatur, unde fartis iam probabilitas oritur, hoc generaliter perinde se habere. Sed demonstratio huius phaenomeni e principiis l.c. expositis peti nequit, plenissimoque iure altioris indaginis aestimanda est. Propositum itaque huius commentationis eo tendit, ut demonstrationem rigorosam huius elegantissimi theorematis, per plures annos olim variis modis incassum tentatam, tandemque per considerationes singulares satisque subtiles feliciter perfectam in medium proferamus, simulque theorema ipsum salva seu potius aucta elegantia sua ad longe maiorem generalitatem evehamus. Coronidis denique loco nexum mirabilem arctissimum inter hanc summationem aliudque theorema arithmeticum gravissimum docebimus. Speramus, hasce disquisitiones non modo per se geometris gratas fore, sed methodos quoque, per quas haec omnia efficere licuit, quaeque in aliis quoque occasionibus utiles esse poterunt, ipsorum attentione dignas visum iri.

5.

Petita est demonstratio nostra e consideratione generis singularis progressionum, quarum termini pendent ab expressionibus talibus

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})...(1-x^{m-\mu+1})}{(1-x)(1-xx)(1-x^3)...(1-x^\mu)}$$

Brevitatis caussa talem fractionem per (m, μ) denotabimus, et primo quasdam observationes generales circa huiusmodi functiones praemittemus.

I. Quoties m est integer positivus minor quam μ, functio (m, μ) manifesto evanescit, numeratore factorem $1 - x^0$ implicante. Pro $m = \mu$, factores in numeratore identici erunt ordine inverso cum factoribus in denominatore, unde erit $(\mu, \mu) = 1$: denique pro casu eo, ubi m est integer positivus maior quam μ, habentur formulae

$$(\mu+1, \mu) = \frac{1-x^{\mu+1}}{1-x} = (\mu+1, 1)$$
$$(\mu+2, \mu) = \frac{(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)} = (\mu+2, 2)$$
$$(\mu+3, \mu) = \frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)(1-x^3)} = (\mu+3, 3) \text{ etc.}$$

sive generaliter

$$(m,\mu) = (m, m-\mu)$$

II. Porro facile confirmatur, haberi generaliter

$$(m,\mu+1) = (m-1,\mu+1) + x^{m-\mu-1}(m-1,\mu)$$

quamobrem, quum perinde sit

$$(m-1,\mu+1) = (m-2,\mu+1) + x^{m-\mu-2}(m-2,\mu)$$
$$(m-2,\mu+1) = (m-3,\mu+1) + x^{m-\mu-3}(m-3,\mu)$$
$$(m-3,\mu+1) = (m-4,\mu+1) + x^{m-\mu-4}(m-4,\mu) \text{ etc.},$$

quae series continuari poterit usque ad

$$\begin{aligned}(\mu+2,\mu+1) &= (\mu+1,\mu+1) + x(\mu+1,\mu)\\ &= (\mu,\mu) + x(\mu+1,\mu)\end{aligned}$$

siquidem m est integer positivus maior quam $\mu+1$, erit

$$(m,\mu+1) = (\mu,\mu) + x(\mu+1,\mu) + xx(\mu+2,\mu) + x^3(\mu+3,\mu) + \text{etc.} + x^{m-\mu-1}(m-1,\mu)$$

Hinc patet, si pro aliquo valore determinato ipsius μ quaevis functio (m,μ) integra sit, existente m integro positivo, etiam quamvis functionem $(m,\mu+1)$ integram evadere debere. Quare quum suppositio illa pro $\mu = 1$ locum habeat, eadem etiam pro $\mu = 2$ valebit, atque hinc etiam pro $\mu = 3$ etc., *i.e.* generaliter pro valore quocunque integro positivo ipsius m erit (m,μ) functio integra, sive productum

$$(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})$$

divisibile per

$$(1-x)(1-x^2)(1-x^3)\ldots(1-x^\mu)$$

6.

Duas iam progressiones considerabimus, quae ambae ad scopum nostrum ducere possunt. Progressio prima haec est

$$1 - \tfrac{1-x^m}{1-x} + \tfrac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)} - \tfrac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)} + \text{etc.}$$

sive

$$1 - (m,1) + (m,2) - (m,3) + (m,4) - \text{etc.}$$

quam brevitatis caussa per $f(x,m)$ denotabimus. Primo statim obvium est, quoties m sit numerus integer positivus, hanc seriem post terminum suum $m+1^{\text{tum}}$ (qui fit $= \pm 1$) *abrumpi*, adeoque in hoc casu summam fieri debere functionem finitam integram ipsius x. Porro per art. 5. II. patet, generaliter pro valore quocunque ipsius m haberi

$$\begin{aligned} 1 &= 1 \\ -(m,1) &= -(m-1,1) - x^{m-1} \\ +(m,2) &= +(m-1,2) + x^{m-2}(m-1,1) \\ -(m,3) &= -(m-1,3) - x^{m-3}(m-1,2) \text{ etc.} \end{aligned}$$

adeoque

$$\begin{aligned} f(x,m) = 1 - x^{m-1} - (1-x^{m-2})(m-1,1) + (1-x^{m-3})(m-1,2) \\ - (1-x^{m-4})(m-1.3) + \text{etc.} \end{aligned}$$

Sed manifesto fit

$$\begin{aligned} (1-x^{m-2})(m-1,1) &= (1-x^{m-1})(m-2,1) \\ (1-x^{m-3})(m-1,2) &= (1-x^{m-1})(m-2,2) \\ (1-x^{m-4})(m-1,3) &= (1-x^{m-1})(m-2,3) \text{ etc.} \end{aligned}$$

unde deducimus aequationem

$$f(x,m) = (1-x^{m-1}) f(x,m-2) \qquad [1]$$

7.

Quum pro $m = 0$ fiat $f(x,m) = 1$, per formulam modo inventam erit

$$\begin{aligned} f(x,2) &= 1-x \\ f(x,4) &= (1-x)(1-x^3) \\ f(x,6) &= (1-x)(1-x^3)(1-x^5) \\ f(x,8) &= (1-x)(1-x^3)(1-x^5)(1-x^7) \text{ etc.} \end{aligned}$$

sive generaliter pro valore quocunque pari ipsius m

$$f(x,m) = (1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1}) \qquad [2]$$

Contra quum pro $m = 1$ fiat $f(x,m) = 0$, erit etiam

$$f(x,3) = 0$$
$$f(x,5) = 0$$
$$f(x,7) = 0 \text{ etc.}$$

sive generaliter pro valore quocunque impari ipsius m

$$f(x,m) = 0$$

Ceterum summatio posterior iam inde derivari potuisset, quod in progressione

$$1 - (m,1) + (m,2) - (m,3) + \text{etc.} + (m,m-1) - (m,m)$$

terminus ultimus primum destruit, penultimus secundum etc.

8.

Ad scopum quidem nostrum sufficit casus is, ubi m est integer positivus impar: sed propter rei singularitatem etiam de casibus iis, ubi m vel fractus vel negativus est, pauca adiecisse haud poenitebit. Manifesto tunc series nostra haud amplius abrumpetur, sed in infinitum excurret, facileque insuper perspicitur, divergentem eam fieri, quoties ipsi x valor minor quam 1 tribuatur, quapropter ipsius summatio ad valores ipsius x qui sint maiores quam 1 restringi debebit.

Per formulam [1] art. 6. habemus

$$f(x,-2) = \frac{1}{1-\frac{1}{x}}$$
$$f(x,-4) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}}$$
$$f(x,-6) = \frac{1}{1-\frac{1}{x}} \cdot \frac{1}{1-\frac{1}{x^3}} \cdot \frac{1}{1-\frac{1}{x^5}} \text{ etc.}$$

ita ut valor functionis $f(x,m)$ etiam pro valore negativo integro pari ipsius m in terminis finitis assignabilis sit. Pro reliquis vero valoribus ipsius m functionem $f(x,m)$ in *productum infinitum* sequenti modo convertemus.

Crescente m in valorem negativum infinitum, functio $f(x,m)$ transit in

$$1+\tfrac{1}{x-1}+\tfrac{1}{x-1}\cdot\tfrac{1}{xx-1}+\tfrac{1}{x-1}\cdot\tfrac{1}{xx-1}\cdot\tfrac{1}{x^3-1}+\text{etc.}$$

Haec itaque series aequalis est producto infinito

$$\tfrac{1}{1-\frac{1}{x}}\cdot\tfrac{1}{1-\frac{1}{x^3}}\cdot\tfrac{1}{1-\frac{1}{x^5}}\cdot\tfrac{1}{1-\frac{1}{x^7}}\text{etc. in infin.}$$

Porro quum generaliter sit

$$f(x,m)=f(x,m-2\lambda).(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\ldots(1-x^{m-2\lambda+1})$$

erit

$$\begin{aligned}f(x,m)&=f(x,-\infty)\cdot(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\text{ etc. in infin.}\\&=\tfrac{1-x^{m-1}}{1-x^{-1}}\cdot\tfrac{1-x^{m-3}}{1-x^{-3}}\cdot\tfrac{1-x^{m-5}}{1-x^{-5}}\cdot\tfrac{1-x^{m-7}}{1-x^{-7}}\text{ etc. in infin.}\end{aligned}$$

quos factores tandem continuo magis ad unitatem convergere palam est.

Attentionem peculiarem meretur casus $m=-1$, ubi fit

$$f(x,-1)=1+x^{-1}+x^{-3}+x^{-6}+x^{-10}+\text{etc.}$$

Haec itaque series aequatur producto infinito

$$\tfrac{1-x^{-2}}{1-x^{-1}}\cdot\tfrac{1-x^{-2}}{1-x^{-3}}\cdot\tfrac{1-x^{-6}}{1-x^{-5}}\text{ etc.}$$

sive scribendo x pro x^{-1}, erit

$$1+x+x^3+x^6+\text{etc.}=\tfrac{1-xx}{1-x}\cdot\tfrac{1-x^4}{1-x^3}\cdot\tfrac{1-x^6}{1-x^5}\cdot\tfrac{1-x^8}{1-x^7}\text{ etc.}$$

Haec aequalitas inter duas expressiones abstrusiores, ad quas alia occasione reveniemus, valde sane est memorabilis.

9.

Secundo loco considerabimus progressionem hancce

$$1+x^{\frac{1}{2}}\tfrac{1-x^m}{1-x}+x\tfrac{(1-x^m)}{(1-x)}\tfrac{(1-x^{m-1})}{(1-xx)}+x^{\frac{3}{2}}\tfrac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)}+\text{etc.}$$

sive

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+xx(m,4)+\text{etc.}$$

quam per $F(x,m)$ denotabimus. Restringemus hanc disquisitionem ad casum eum, ubi m est integer positivus, ita ut haec quoque series semper abrumpaturcum termino

$m+1^{\text{to}}$, qui est $= x^{\frac{1}{2}m}(m,m)$. Quum sit

$$(m,m) = 1, \quad (m,m-1) = (m,1), \quad (m,m-2) = (m,2) \text{ etc.}$$

progressio ita quoque exhiberi poterit:

$$F(x,m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m,1) + x^{\frac{1}{2}(m-2)}(m,2) + x^{\frac{1}{2}(m-3)}(m,3) + \text{etc.}$$

Hinc fit

$$\begin{aligned}(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = 1 + x^{\frac{1}{2}}(m,1) + x(m,2) + x^{\frac{3}{2}}(m,3) + \text{etc.} \\ + x^{\frac{1}{2}}.x^m + x.x^{m-1}(m,1) + x^{\frac{3}{2}}.x^{m-2}(m,2) + \text{etc.}\end{aligned}$$

Quare quum habeatur (art. 5. II)

$$\begin{aligned}(m,1) + x^m &= (m+1,1) \\ (m,2) + x^{m-1}(m,1) &= (m+1,2) \\ (m,3) + x^{m-2}(m,2) &= (m+1,3) \text{ etc.},\end{aligned}$$

provenit

$$(1+x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = F(x,m+1) \qquad [3]$$

Sed fit $F(x,0) = 1$: quamobrem erit

$$\begin{aligned}F(x,1) &= 1 + x^{\frac{1}{2}} \\ F(x,2) &= (1+x^{\frac{1}{2}})(1+x) \\ F(x,3) &= (1+x^{\frac{1}{2}})(1+x)(1+x^3) \text{ etc.},\end{aligned}$$

sive generaliter

$$F(x,m) = (1+x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}}) \ldots (1+x^{\frac{1}{2}m}) \qquad [4]$$

10.

Praemissis hisce disquisitionibus praeliminaribus iam propius ad propositum nostrum accedamus. Quum pro valore primo ipsius n quadrata $1,\ 4,\ 9 \ldots (\frac{1}{2}(n-1))^2$ omnia inter se incongrua sint secundum modulum n, patet, illorum residua minima secundum hunc modulum cum numeris a identica esse debere, adeoque

$$\begin{aligned}\Sigma \cos akw &= \cos kw + \cos 4kw + \cos 9kw + \text{etc.} + \cos(\tfrac{1}{2}(n-1))^2 kw \\ \Sigma \sin akw &= \sin kw + \sin 4kw + \sin 9kw + \text{etc.} + \sin(\tfrac{1}{2}(n-1))^2 kw\end{aligned}$$

Perinde quum eadem quadrata $1, 4, 9 \ldots (\frac{1}{2}(n-1))^2$ ordine inverso congrua sint his $(\frac{1}{2}(n+1))^2, (\frac{1}{2}(n+3))^2, (\frac{1}{2}(n+5))^2 \ldots (n-1)^2$, etiam erit

$$\Sigma \cos akw = \cos(\tfrac{1}{2}(n+1))^2 kw + \cos(\tfrac{1}{2}(n+3))^2 kw + \text{etc.} + \cos(n-1)^2 kw$$
$$\Sigma \sin akw = \sin(\tfrac{1}{2}(n+1))^2 kw + \sin(\tfrac{1}{2}(n+3))^2 kw + \text{etc.} + \sin(n-1)^2 kw$$

Statuendo itaque

$$T = 1 + \cos kw + \cos 4kw + \cos 9kw + \text{etc.} + \cos(n-1)^2 kw$$
$$U = \quad \sin kw + \sin 4kw + \sin 9kw + \text{etc.} + \sin(n-1)^2 kw$$

erit

$$1 + 2\Sigma \cos akw = T$$
$$2\Sigma \sin akw = U$$

Hinc patet, summationes, quales in art. 1. propositae sunt, pendere a summatione serierum T et U, quocirca, missis illis, disquisitionem nostram his adaptabimus, eaque generalitate absolvemus, ut non modo valores primos ipsius n, sed quoscunque compositos complectatur. Numerum k autem supponemus ad n primum esse: nullo enim negotio casus is, ubi k et n divisorem communem haberent, ad hunc reduci poterit.

11.

Designemus quantitatem imaginariam $\sqrt{-1}$ per i, statuamusque

$$\cos kw + i \sin kw = r$$

unde erit $r^n = 1$, sive r radix aequationis $r^n - 1 = 0$. Facile perspicietur, omnes numeros k, $2k$, $3k \ldots (n-1)k$ per n non divisibiles atque inter se secundum modulum n incongruos esse: hinc potestates ipsius r

$$1, r, rr, r^3 \ldots r^{n-1}$$

omnes erunt inaequales, singulae vero quoque aequationi $x^n - 1 = 0$ satisfacient. Hanc ob caussam hae potestates omnes radices aequationis $x^n - 1 = 0$ repraesentabunt.

Hae conclusiones non valerent, si k divisorem communem haberet cum n. Si enim ν esset talis divisor communis, foret $k.\frac{n}{\nu}$ per n divisibilis, adeoque potestas inferior quam r^n, puta $r^{\frac{n}{\nu}}$, unitati aequalis. In hoc itaque casu potestates ipsius r ad summum $\frac{n}{\nu}$ radices aequationis $x^n - 1 = 0$ exhibebunt, et quidem revera tot radices diversas sistent, si ν est divisor communis *maximus* numerorum k, n. In

casu nostro, ubi k et n supponuntur inter se primi, r commode dici potest *radix propria* aequationis $x^n - 1 = 0$: contra in casu altero, ubi k et n haberent divisorem communem (maximum) ν, r vocaretur *radix impropria* illius aequationis, manifesto autem tunc eadem r foret radix propria aequationis $x^{\frac{n}{\nu}} - 1 = 0$. Radix impropria simplicissima est unitas, in eoque casu, ubi n est numerus primus, impropriae aliae omnino non dabuntur.

12.

Quodsi iam statuimus

$$W = 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

patet fieri $W = T + iU$, adeoque T esse partem realem ipsius W, atque U prodire ex parte imaginaria ipsius W factore i suppresso. Totum itaque negotium reducitur ad inventionem summae W: ad hunc finem vel series in art. 6 considerata, vel ea quam in art. 9 summare docuimus, adhiberi potest, prior tamen minus idonea est in casu eo, ubi n est numerus par. Nihilominus lectoribus gratum fore speramus, si casum eum, ubi n impar est, secundum methodum duplicem tractemus.

Supponamus itaque primo, n esse numerum imparem, r designare radicem propriam aequationis $x^n - 1 = 0$ quamcunque, et in functione $f(x, m)$ statui $x = r$, atque $m = n - 1$. Hinc patet fieri

$$\begin{aligned} \tfrac{1-x^m}{1-x} &= \tfrac{1-r^{-1}}{1-r} = -r^{-1} \\ \tfrac{1-x^{m-1}}{1-xx} &= \tfrac{1-r^{-2}}{1-rr} = -r^{-2} \\ \tfrac{1-x^{m-2}}{1-x^3} &= \tfrac{1-r^{-3}}{1-r^3} = -r^{-3} \text{ etc.} \end{aligned}$$

usque ad

$$\tfrac{1-x}{1-x^m} = \tfrac{1-r^{-m}}{1-r^m} = -r^{-m}$$

(Haud superfluum erit monere, has aequationes eatenus tantum valere, quatenus r supponitur radix propria: si enim esset r radix impropria, in quibusdam illarum fractionum numerator et denominator simul evanescerent, adeoque fractiones indeterminatae fierent).

Hinc deducimus aequationem sequentem

$$f(r,n-1) = 1 + r^{-1} + r^{-3} + r^{-6} + \text{etc.} + r^{-\frac{1}{2}(n-1)n}$$
$$= (1-r)(1-r^3)(1-r^5)\dots(1-r^{n-2})$$

Eadem aequatio etiamnum valebit, si pro r substituitur r^λ, designante λ integrum quemcunque ad n primum: tunc enim etiam r^λ erit radix propria aequationis $x^n - 1 = 0$. Scribamus itaque pro r, r^{n-2} sive quod idem est r^{-2}, eritque

$$1 + r^2 + r^6 + r^{12} + \text{etc.} + r^{(n-1)n} = (1-r^{-2})(1-r^{-6})(1-r^{-10})\dots(1-r^{-2(n-2)})$$

Multiplicemus utramque partem huius aequationis per

$$r \cdot r^3 \cdot r^5 \dots \cdot r^{(n-2)} = r^{\frac{1}{4}(n-1)^2}$$

prodibitque, propter

$$r^{2+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-3)^2}, \qquad r^{(n-1)n+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+1)^2}$$
$$r^{6+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-5)^2}, \quad r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+3)^2}$$
$$r^{12+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-7)^2}, \quad r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+5)^2} \text{ etc.}$$

aequatio sequens

$$r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \text{etc.} + r + 1$$
$$+ r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} + \text{etc.} + r^{\frac{1}{4}(2n-2)^2}$$
$$= (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5})\dots(r^{n-2} - r^{-n+2})$$

aut, partibus membri primi aliter dispositis,

$$1 + r + r^4 + \text{etc.} + r^{(n-1)^2} = (r - r^{-1})(r^3 - r^{-3})\dots(r^{n-2} - r^{-n+2}) \qquad [5]$$

13.

Factores membri secundi aequationis [5] ita quoque exhiberi possunt

$$r - r^{-1} = -(r^{n-1} - r^{-n+1})$$
$$r^3 - r^{-3} = -(r^{n-3} - r^{-n+3})$$
$$r^5 - r^{-5} = -(r^{n-5} - r^{-n+5}) \text{ etc.}$$

usque ad

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2})$$

quo pacto aequatio ista hanc formam assumit:

$$W = (-1)^{\frac{1}{2}(n-1)}(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \dots (r^{n-1} - r^{-n+1})$$

Multiplicando hanc aequationem per [5] in forma primitiva, prodit

$$W^2 = (-1)^{\frac{1}{2}(n-1)}(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \dots (r^{n-1} - r^{-n+1})$$

ubi $(-1)^{\frac{1}{2}(n-1)}$ est vel $= +1$ vel $= -1$, prout n est formae $4\mu + 1$, vel formae $4\mu + 3$. Hinc

$$W^2 = \pm r^{\frac{1}{2}n(n-1)}(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \dots (1 - r^{-2(n-1)})$$

Sed nullo negotio perspicitur, r^{-2}, r^{-4}, $r^{-6} \dots r^{-2n+2}$ exhibere omnes radices aequationis $x^n - 1 = 0$, radice $x = 1$ excepta, unde locum habere debebit aequatio identica indefinita

$$(x - r^{-2})(x - r^{-4})(x - r^{-6}) \dots (x - r^{-2n+2}) = x^{n-1} + x^{n-2} + x^{n-3} + \text{etc.} + x + 1$$

Quamobrem statuendo $x = 1$, fiet

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \dots (1 - r^{-2n+2}) = n$$

et quum manifesto sit $r^{\frac{1}{2}n(n-1)} = 1$, aequatio nostra transit in hanc

$$W^2 = \pm n \qquad [6]$$

In casu itaque eo, ubi n est formae $4\mu + 1$, fiet

$$W = \pm\sqrt{n}, \text{ et proin } T = \pm\sqrt{n}, \quad U = 0$$

Contra in casu altero, ubi n est formae $4\mu + 3$, fiet

$$W = \pm i\sqrt{n}, \text{ adeoque } T = 0, \quad U = \pm\sqrt{n}$$

14.

Methodus art. praec. valorem tantummodo absolutum aggregatorum T, U assignat, ambiguumque linquit, utrum statuere oporteat T in casu priori atque U in casu posteriori $= +\sqrt{n}$, an $= -\sqrt{n}$. Hoc autem, saltem pro casu eo ubi $k = 1$, ex aequatione [5] sequenti modo decidere licebit. Quum sit, pro $k = 1$,

$$r - r^{-1} = 2i \sin \omega$$
$$r^3 - r^{-3} = 2i \sin 3\omega$$
$$r^5 - r^{-5} = 2i \sin 5\omega \text{ etc.},$$

aequatio ista transmutatur in

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega$$

Iam in casu eo, ubi n est formae $4\mu+1$, in serie numerorum imparium

$$1, 3, 5, 7 \ldots \tfrac{1}{2}(n-3), \tfrac{1}{2}(n+1) \ldots (n-2)$$

reperiuntur $\frac{1}{4}(n-1)$, qui sunt minores quam $\frac{1}{2}n$, hisque manifesto respondent sinus positivi; contra reliqui $\frac{1}{4}(n-1)$ erunt maiores quam $\frac{1}{2}n$, hisque sinus negativi respondebunt: quapropter productum omnium sinuum statuendum est aequale producto e quantitate positiva in multiplicatorem $(-1)^{\frac{1}{4}(n-1)}$, adeoque W aequalis erit producto e quantitate reali positiva in i^{n-1} sive in 1, quoniam $i^4 = 1$, atque $n-1$ per 4 divisibilis: i.e. quantitas W erit realis positiva, unde necessario esse debebit

$$W = +\sqrt{n}, \quad T = +\sqrt{n}$$

In casu altero, ubi n est formae $4\mu+3$ in serie numerorum imparium

$$1, 3, 5, 7 \ldots \tfrac{1}{2}(n-1), \tfrac{1}{2}(n+3) \ldots (n-2)$$

priores $\frac{1}{4}(n+1)$ erunt minores quam $\frac{1}{2}n$, reliqui $\frac{1}{4}(n-3)$ autem maiores. Hinc inter sinus arcuum $\omega, 3\omega, 5\omega \ldots (n-2)\omega$ negativi erunt $\frac{1}{4}(n-3)$, adeoque W erit productum ex $i^{\frac{1}{2}(n-1)}$ in quantitatem realem positivam in $(-1)^{\frac{1}{4}(n-3)}$; factor tertius est $= i^{\frac{1}{2}(n-3)}$, qui cum primo iunctus producit $i^{n-2} = i$, quoniam $i^{n-3} = 1$. Quamobrem necessario erit

$$W = +i\sqrt{n}, \text{ atque } U = +\sqrt{n}$$

15.

Iam ostendemus, quo pacto eaedem conclusiones e progressione in art. 9 considerata deduci possint. Scribamus in aequ. [4] pro $x^{\frac{1}{2}}$, $-y^{-1}$, eritque

$$1 - y^{-1}\tfrac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\tfrac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} - y^{-3}\tfrac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \text{etc.}$$

usque ad terminum $m+1^{\text{tum}}$

$$= (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4})\dots(1\pm y^{-m}) \qquad [7]$$

Quodsi hic pro y accipitur radix propria aequationis $y^n - 1 = 0$, puta r, atque simul statuitur $m = n-1$, erit

$$\tfrac{1-y^{-2m}}{1-y^{-2}} = \tfrac{1-r^2}{1-r^{-2}} = -r^2$$
$$\tfrac{1-y^{-2m+2}}{1-y^{-4}} = \tfrac{1-r^4}{1-r^{-4}} = -r^4$$
$$\tfrac{1-y^{-2m+4}}{1-y^{-6}} = \tfrac{1-r^6}{1-r^{-6}} = -r^6 \text{ etc.}$$

usque ad

$$\tfrac{1-y^{-2}}{1-y^{-2m}} = \tfrac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2}$$

ubi notandum, nullum denominatorum $1-r^{-2}$, $1-r^{-4}$ etc. fieri $= 0$. Hinc aequatio [7] hancce formam assumit

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = (1-r^{-1})(1+r^{-2})(1-r^{-3})\dots(1+r^{-n+1})$$

Multiplicando in membro secundo huius aequationis terminum primum per ultimum, secundum per penultimum etc., habemus

$$(1-r^{-1})(1+r^{-n+1}) = r - r^{-1}$$
$$(1+r^{-2})(1-r^{-n+2}) = r^{n-2} - r^{-n+2}$$
$$(1-r^{-3})(1+r^{-n+3}) = r^3 - r^{-3}$$
$$(1+r^{-4})(1-r^{-n+4}) = r^{n-4} - r^{-n+4} \text{ etc.}$$

Ex his productis partialibus facile perspicietur conflari productum

$$(r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\dots(r^{n-4}-r^{-n+4})(r^{n-2}-r^{-n+2})$$

quod itaque erit

$$= 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = W$$

Haec aequatio identica est cum aequ. [5] in art. 12 e progressione prima derivata, ratiociniaque dein reliqua eodem modo adstruentur, ut in artt. 13 et 14.

16.

Transimus ad casum alterum, ubi n est numerus par. Sit primo n formae $4\mu+2$ sive impariter par, patetque, numeros $\frac{1}{4}nn$, $(\frac{1}{2}n+1)^2-1$, $(\frac{1}{2}n+2)^2-4$ etc. sive generaliter $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$ per $\frac{1}{2}n$ divisos producere quotientes impares, adeoque secundum modulum n congruos fieri ipsi $\frac{1}{2}n$. Hinc colligitur, si r sit radix propria aequationis $x^n-1=0$, adeoque $r^{\frac{1}{2}n}=-1$, fieri

$$r^{(\frac{1}{2}n)^2}=-1$$
$$r^{(\frac{1}{2}n+1)^2}=-r$$
$$r^{(\frac{1}{2}n+2)^2}=-r^4$$
$$r^{(\frac{1}{2}n+3)^2}=-r^9 \text{ etc.}$$

Hinc in progressione

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

terminus $r^{(\frac{1}{2}n)^2}$ destruet primum, sequens secundum etc., adeoque erit

$$W=0, \quad T=0, \quad U=0$$

17.

Superest casus, ubi n est formae 4μ sive pariter par. Hic generaliter $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$ divisibilis erit per n, adeoque

$$r^{(\frac{1}{2}n+\lambda)^2}=r^{\lambda\lambda}$$

Hinc in serie

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

terminus $r^{(\frac{1}{2}n)^2}$ aequalis erit primo, sequens secundo etc., ita ut fiat

$$W=2(1+r+r^4+r^9+\text{etc.}+r^{(\frac{1}{2}n-1)^2})$$

Iam supponamus, in aequ. [7] art. 15 statui $m=\frac{1}{2}n-1$, et pro y accipi radicem propriam aequationis $y^n-1=0$, puta r. Tunc perinde ut in art. 15 aequatio sequentem formam obtinet:

$$1+r+r^4+\text{etc.}+r^{(\frac{1}{2}n-1)^2}=(1-r^{-1})(1+r^{-2})(1-r^{-3})\ldots(1-r^{-\frac{1}{2}n+1})$$

sive

$$W = 2(1-r^{-1})(1+r^{-2})(1-r^{-3})(1+r^{-4})\dots(1-r^{-\frac{1}{2}n+1}) \qquad [8]$$

Porro quum sit $r^{\frac{1}{2}n} = -1$, adeoque

$$1+r^{-2} = -r^{\frac{1}{2}n-2}(1-r^{-\frac{1}{2}n+2})$$
$$1+r^{-4} = -r^{\frac{1}{2}n-4}(1-r^{-\frac{1}{2}n+4})$$
$$1+r^{-6} = -r^{\frac{1}{2}n-6}(1-r^{-\frac{1}{2}n+6}) \text{ etc.}$$

productumque e factoribus $-r^{\frac{1}{2}n-2}$,$-r^{\frac{1}{2}n-4}$,$-r^{\frac{1}{2}n-6}$ etc. usque ad $-r^2$ fiat $= (-1)^{\frac{1}{4}n-1}r^{\frac{1}{16}nn-\frac{1}{4}n}$, aequatio praecedens ita quoque exhiberi potest

$$W = 2(-1)^{\frac{1}{4}n-1}r^{\frac{1}{16}nn-\frac{1}{4}n}(1-r^{-1})(1-r^{-2})(1-r^{-3})(1-r^{-4})\dots(1-r^{-\frac{1}{2}n+1})$$

Quum habeatur

$$1-r^{-1} = -r^{-1}(1-r^{-n+1})$$
$$1-r^{-2} = -r^{-2}(1-r^{-n+2})$$
$$1-r^{-3} = -r^{-3}(1-r^{-n+3}) \text{ etc.}$$

erit

$$(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-\frac{1}{2}n+1})$$
$$=(-1)^{\frac{1}{2}n-1}r^{-\frac{1}{8}nn+\frac{1}{4}n}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\dots(1-r^{-n+1})$$

adeoque

$$W = 2(-1)^{\frac{3}{4}n-2}r^{-\frac{1}{16}nn}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\dots(1-r^{-n+1})$$

Multiplicando hunc valorem ipsius W per prius inventum, adiungendoque utrimque factorem $1-r^{-\frac{1}{2}n}$, prodit

$$(1-r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3}r^{-\frac{1}{4}n}(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-n+1})$$

Sed fit

$$1-r^{-\frac{1}{2}n} = 2$$
$$(-1)^{n-3} = -1$$
$$r^{-\frac{1}{4}n} = -r^{\frac{1}{4}n}$$
$$(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-n+1}) = n$$

Unde tandem concluditur

$$W^2 = 2r^{\frac{1}{4}n}n \qquad [9]$$

Iam facile perspicietur, $r^{\frac{1}{4}n}$ esse vel $= +i$ vel $= -i$, prout scilicet k vel formae $4\mu+1$ sit, vel formae $4\mu+3$. Et quum sit

$$2i = (1+i)^2, \quad -2i = (1-i)^2$$

erit in casu eo, ubi k est formae $4\mu+1$,

$$W = \pm(1+i)\sqrt{n}, \text{ adeoque } \quad T = U = \pm\sqrt{n}$$

in casu altero autem, ubi k est formae $4\mu+3$,

$$W = \pm(1-i)\sqrt{n}, \text{ adeoque } T = -U = \pm\sqrt{n}$$

18.

Methodus art. praec. valores absolutos functionum T, U suppeditavit, conditionesque assignavit, sub quibus signa aequalia vel opposita illis tribuenda sint: sed signa ipsa hinc nondum determinantur. Hoc pro eo casu, ubi statuitur $k = 1$, sequenti modo supplebimus.

Statuamus $\rho = \cos\frac{1}{2}\omega + i\sin\frac{1}{2}\omega$, ita ut fiat $r = \rho\rho$, patetque, propter $\rho^n = -1$ aequationem [8] ita exhiberi posse

$$W = 2(1+\rho^{n-2})(1+\rho^{-4})(1+\rho^{n-6})(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^2)$$

sive factoribus alio ordine dispositis

$$W = 2(1+\rho^2)(1+\rho^{-4})(1+\rho^6)(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^{n-2})$$

Iam fit

$$\begin{aligned} 1+\rho^2 &= 2\rho\cos\tfrac{1}{2}\omega \\ 1+\rho^{-4} &= 2\rho^{-2}\cos\omega \\ 1+\rho^{+6} &= 2\rho^3\cos\tfrac{3}{2}\omega \\ 1+\rho^{-8} &= 2\rho^{-4}\cos 2\omega \text{ etc.} \end{aligned}$$

usque ad

$$\begin{aligned} 1+\rho^{-n+4} &= 2\rho^{-\frac{1}{2}n+2}\cos(\tfrac{1}{4}n-1)\omega \\ 1+\rho^{n-2} &= 2\rho^{\frac{1}{2}n-1}\cos(\tfrac{1}{4}n-\tfrac{1}{2})\omega \end{aligned}$$

Quamobrem habetur

$$W = 2^{\frac{1}{2}n} \rho^{\frac{1}{4}n} \cos \tfrac{1}{2}\omega \cos \omega \cos \tfrac{3}{2}\omega \ldots \cos(\tfrac{1}{4}n - \tfrac{1}{2})\omega$$

Cosinus in hoc productum ingredientes manifesto omnes positivi sunt, factor $\rho^{\frac{1}{4}n}$ autem fit $= \cos 45^\circ + i \sin 45^\circ = (1+i)\sqrt{\frac{1}{2}}$. Hinc colligimus, W esse productum ex $1+i$ in quantitatem realem positivam, unde necessario esse debebit

$$W = (1+i) \cdot \sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}$$

19.

Operae pretium erit, omnes summationes hactenus evolutas, hic in unum conspectum colligere. Generaliter scilicet est

$T =$	$U =$	prout n est formae
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

et in casu eo, ubi k supponitur $= 1$, quantitati radicali signum positivum tribui debet. Omni itaque iam rigore ea, quae pro valoribus primis ipsius n in art. 3 per inductionem animadverteramus, demonstrata sunt, nihilque superest, nisi ut signa pro valoribus quibuscunque ipsius k in omnibus casibus determinare doceamus. Sed antequam hoc negotium in omni generalitate aggredi liceat, primo casus eos, ubi n est numerus primus vel numeri primi potestas, propius considerare oportebit.

20.

Sit primo n numerus primus impar, patetque per ea, quae in art. 10 exposuimus, esse $W = 1 + 2\Sigma r^a = 1 + 2\Sigma R^{ak}$, si statuatur $R = \cos\omega + i \sin\omega$, denotante a ut illic indefinite omnia residua quadratica ipsius n inter 1 et $n-1$ contenta. Quodsi quoque per b indefinite omnia non-residua quadratica inter eosdem limites exprimimus, nullo negotio perspicitur, omnes numeros ak congruos fieri secundum modulum n vel omnibus a vel omnibus b (nullo ordinis respectu habito), prout k vel residuum sit vel non-residuum. Quamobrem in casu priori erit

$$W = 1 + 2\sum R^a = 1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2}$$

adeoque $W = +\sqrt{n}$, si n est formae $4\mu+1$, atque $W = +i\sqrt{n}$, si n est formae $4\mu+3$.

Contra in casu altero, ubi k est non-residuum ipsius n, erit

$$W = 1 + 2\Sigma R^b$$

Hinc quum manifesto omnes a, b complexum integrum numerorum 1, 2, 3 ... expleant, adeoque sit

$$\Sigma R^a + \Sigma R^b = R + R^2 + R^3 + \text{etc.} + R^{n-1} = -1$$

fiet

$$W = -1 - 2\Sigma R^a = -(1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2})$$

adeoque $W = -\sqrt{n}$, si n est formae $4\mu+1$, atque $W = -i\sqrt{n}$, si n est formae $4\mu+3$.

Hinc itaque colligitur

primo, si n est formae $4\mu+1$, atque k residuum quadraticum ipsius n,

$$T = +\sqrt{n}, \quad U = 0$$

secundo, si n est formae $4\mu+1$, atque k non-residuum ipsius n,

$$T = -\sqrt{n}, \quad U = 0$$

tertio, si n est formae $4\mu+3$, atque k residuum ipsius n,

$$T = 0, \quad U = +\sqrt{n}$$

quarto, si n est formae $4\mu+3$, atque k non-residuum ipsius n,

$$T = 0, \quad U = -\sqrt{n}$$

21.

Sit secundo n quadratum altiorve potestas numeri primi imparis p, statuaturque $n = p^{2\chi}q$, ita ut sit q vel $= 1$ vel $= p$. Hic ante omnia observare convenit, si λ sit integer quicunque per p^χ non divisibilis, fieri

$$r^{\lambda\lambda} + r^{(\lambda+p^\chi q)^2} + r^{(\lambda+2p^\chi q)^2} + r^{(\lambda+3p^\chi q)^2} + \text{etc.} + r^{(\lambda+n-p^\chi q)^2}$$
$$= r^{\lambda\lambda}\left\{1 + r^{2\lambda p^\chi q} + r^{4\lambda p^\chi q} + r^{6\lambda p^\chi q} + \text{etc.} + r^{2\lambda(n-p^\chi q)}\right\} = \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2\lambda p^\chi q}} = 0$$

Hinc facile perspicietur, fieri

$$W = 1 + r^{p^{2\chi}} + r^{4p^{2\chi}} + r^{9p^{2\chi}} + \text{etc.} + r^{(n-p^\chi)^2}$$

Termini enim reliqui progressionis

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

distribui poterunt in $(p^\chi - 1)q$ progressiones partiales, quae singulae sint p^χ terminorum, et per transformationem modo traditam summas evanescentes conficiant.

Hinc colligitur, in casu eo, ubi fit $q = 1$, sive ubi n est potestas numeri primi cum exponente pari, fieri

$$W = p^\chi = +\sqrt{n}, \text{ adeoque } T = +\sqrt{n}, U = 0$$

Contra in casu eo, ubi $q = p$, sive ubi n est potestas numeri primi cum exponente impari, statuemus $r^{p^{2\chi}} = \rho$, unde ρ erit radix propria aequationis $x^p - 1 = 0$, et quidem $\rho = \cos\frac{k}{p}360^\circ + i\sin\frac{k}{p}360^\circ$, ac dein

$$W = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p^{\chi+1}-1)^2} = p^\chi(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p-1)^2})$$

Sed summa seriei $1 + p + p^4 + p^9 + \text{etc.} + p^{(p-1)^2}$ per art. praec. determinatur, unde sponte concluditur, fieri

$$W = \pm\sqrt{n} = T, \text{ si fuerit } p \text{ formae } 4\mu + 1$$
$$W = \pm i\sqrt{n} = iU, \text{ si fuerit } p \text{ formae } 4\mu + 3$$

signo positivo vel negativo valente, prout k fuerit residuum vel non-residuum ipsius p.

22.

Facile quoque ex iis, quae in artt. 20. et 21 exposita sunt, derivatur propositio sequens, quae infra usum notabilem nobis praestabit. Statuatur

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

denotante h integrum quemcunque per p non divisibilem, eritque in casu eo, ubi

$n = p$, vel ubi n est potestas ipsius p cum exponente impari,

$$W' = W, \text{ si fuerit } h \text{ residuum quadraticum ipsius } p$$

$$W' = -W, \text{ si fuerit } h \text{ non-residuum quadraticum ipsius } p$$

Patet enim, W' oriri ex W, si pro k substituatur kh; in casu priori autem k et kh similes erunt, in posteriori dissimiles, quatenus sunt residua vel non-residua ipsius p.

In casu eo autem, ubi n est potestas ipsius p cum exponente pari, manifesto fit $W' = +\sqrt{n}$, adeoque semper $W' = W$.

23.

In artt. 20, 21, 22 consideravimus numeros primos impares, taliumque potestates: superest itaque casus, ubi n est potestas binarii.

Pro $n = 2$ manifesto fit $W = 1 + r = 0$.

Pro $n = 4$ prodit $W = 1 + r + r^4 + r^9 = 2 + 2r$: hinc $W = 2 + 2i$, quoties k est formae $4\mu + 1$, atque $W = 2 - 2i$, quoties k est formae $4\mu + 3$.

Pro $n = 8$ habemus $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$. Hinc erit

$$W = (1+i)\sqrt{8}, \text{ quoties } k \text{ est formae } 8\mu + 1$$

$$W = (-1+i)\sqrt{8}, \text{ quoties } k \text{ est formae } 8\mu + 3$$

$$W = (-1-i)\sqrt{8}, \text{ quoties } k \text{ est formae } 8\mu + 5$$

$$W = (1-i)\sqrt{8}, \text{ quoties } k \text{ est formae } 8\mu + 7$$

Si n est altior potestas binarii, statuamus $n = 2^{2\chi}q$, ita ut q sit vel $= 1$ vel $= 2$, atque χ maior quam 1. Hic ante omnia observari debet, si λ sit integer quicunque per $2^{\chi-1}$ non divisibilis, fieri

$$r^{\lambda\lambda} + r^{(\lambda+2^\chi q)^2} + r^{(\lambda+2.2^\chi q)^2} + r^{(\lambda+3.2^\chi q)^2} + \text{etc.} + r^{(\lambda+n-2^\chi q)^2}$$

$$= r^{\lambda\lambda}\left\{1 + r^{2^{\chi+1}\lambda q} + r^{2.2^{\chi+1}\lambda q} + r^{3.2^{\chi+1}\lambda q} + \text{etc.} + r^{(2n-2^{\chi+1}q)\lambda}\right\} = \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2^{\chi+1}\lambda q}} = 0$$

Hinc facile perspicietur, fieri

$$W = 1 + r^{2^{2\chi-2}} + r^{4.2^{2\chi-2}} + r^{9.2^{2\chi-2}} + \text{etc.} + r^{(n-2^{\chi-1})^2}$$

Statuamus $r^{2^{2\chi-2}} = \rho$, eritque ρ radix aequationis $x^{4q} - 1 = 0$, et quidem $\rho = \cos \frac{k}{4q} 360^\circ + i \sin \frac{k}{4q} 360^\circ$; dein fiet

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(2^{\chi+1}q-1)^2} \\ &= 2^{\chi-1}(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}) \end{aligned}$$

Sed summa seriei $1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}$ per ea, quae de casibus $n = 4$, $n = 8$ explicavimus, determinatur, unde colligimus

in casu eo, ubi $q = 1$, sive ubi n est potestas numeri 4, fieri

$$W = (1+i)2^\chi = (1+i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 4\mu+1$$
$$W = (1-i)2^\chi = (1-i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 4\mu+3$$

quae sunt ipsissimae formulae pro $n = 4$ traditae;

in casu eo autem, ubi $q = 2$, sive ubi n est potestas binarii cum exponente impari maiori quam 3, fieri

$$W = (1+i)2^\chi\sqrt{2} \quad = (1+i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 8\mu+1$$
$$W = (-1+i)2^\chi\sqrt{2} = (-1+i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 8\mu+3$$
$$W = (-1-i)2^\chi\sqrt{2} = (-1-i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 8\mu+5$$
$$W = (1-i)2^\chi\sqrt{2} \quad = (1-i)\sqrt{n}, \text{ si fuerit } k \text{ formae } 8\mu+7$$

quae quoque prorsus conveniunt cum iis, quae pro $n = 8$ tradidimus.

24.

Etiam hic operae pretium erit, rationem summae progressionis

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

ad W determinare, ubi h integrum quemcunque imparem denotat. Quum W' oriatur ex W, mutando k in kh, valor ipsius W' perinde a forma numeri kh pendebit, ut W a forma ipsius k. Statuamus $\frac{W'}{W} = l$, patetque fieri

I. in casu eo, ubi $n = 4$, vel altior potestas binarii cum exponente pari, fieri

$$l = 1, \text{ si fuerit } h \text{ formae } 4\mu+1$$
$$l = -i, \text{ si fuerit } h \text{ formae } 4\mu+3, \text{ atque } k \text{ formae } 4\mu+1$$
$$l = +i, \text{ si fuerit } h \text{ formae } 4\mu+3, \text{ atque } k \text{ eiusdem formae}$$

II. in casu eo, ubi $n = 8$, vel altior potestas binarii cum exponente impari, fieri

$l = 1$, si fuerit h formae $8\mu + 1$,
$l = -1$, si fuerit h formae $8\mu + 5$,
$l = +i$, si fuerit vel h formae $8\mu + 3$, atque k formae $4\mu + 1$,
vel h formae $8\mu + 7$, atque k formae $4\mu + 3$,
$l = -i$, si fuerit vel h formae $8\mu + 3$, atque k formae $4\mu + 3$,
vel h formae $8\mu + 7$, atque k formae $4\mu + 1$.

Per praecc. determinatio summae W pro iis casibus, ubi n est numerus primus vel numeri primi potestas, complete perfecta est: superest itaque, ut eos quoque casus absolvamus, ubi n e pluribus numeris primis compositus est, huc viam nobis sternet theorema sequens.

25.

THEOREMA. *Sit n productum e duobus integris positivis inter se primis a, b, statuaturque*

$$P = 1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b-1)^2 aa}$$
$$Q = 1 + r^{bb} + r^{4bb} + r^{9bb} + \text{etc.} + r^{(a-1)^2 bb}$$

Tum dico fore $W = PQ$.

Demonstr. Designet α indefinite numeros $0, 1, 2, 3 \ldots a-1$, β indefinite numeros $0, 1, 2, 3 \ldots b-1$, ν indefinite numeros $0, 1, 2, 3 \ldots n-1$. Tunc patet esse

$$P = \Sigma r^{aa\beta\beta}, \quad Q = \Sigma r^{bb\alpha\alpha}, \quad W = \Sigma r^{\nu\nu}$$

Hinc erit $PQ = \Sigma r^{aa\beta\beta + bb\alpha\alpha}$, substituendo pro α et β omnes valores, omnibus modis inter se combinatos; hinc porro propter $2ab\alpha\beta = 2\alpha\beta n$, erit $PQ = \Sigma r^{(a\beta + b\alpha)^2}$. Sed nullo negotio perspicitur, singulos valores ipsius $a\beta + b\alpha$ inter se diversos esse, atque alicui valori ipsius ν aequales. Hinc erit $PQ = \Sigma r^{\nu\nu} = W$.

Ceterum notandum est, r^{aa} esse radicem propriam aequationis $x^b - 1 = 0$, atque r^{bb} radicem propriam aequationis $x^a - 1 = 0$.

26.

Sit porro n productum e tribus numeris inter se primis a, b, c, patetque, si statuatur $bc = b'$, etiam a et b' inter se primos fore; adeoque W productum e duobus factoribus

$$1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b'-1)^2 aa}$$
$$1 + r^{b'b'} + r^{4b'b'} + r^{9b'b'} + \text{etc.} + r^{(a-1)^2 b'b'}$$

Sed quum r^{aa} sit radix propria aequationis $x^{bc} - 1 = 0$, erit ipse factor prior productum ex

$$1 + \rho^{bb} + \rho^{4bb} + \rho^{9bb} + \text{etc.} + \rho^{(c-1)^2 bb}$$
$$1 + \rho^{cc} + \rho^{4cc} + \rho^{9cc} + \text{etc.} + \rho^{(b-1)^2 cc}$$

si statuitur $r^{aa} = \rho$. Hinc patet, W esse productum e factoribus tribus

$$1 + r^{bbcc} + r^{4bbcc} + r^{9bbcc} + \text{etc.} + r^{(a-1)^2 bbcc}$$
$$1 + r^{aacc} + r^{4aacc} + r^{9aacc} + \text{etc.} + r^{(b-1)^2 aacc}$$
$$1 + r^{aabb} + r^{4aabb} + r^{9aabb} + \text{etc.} + r^{(c-1)^2 aabb}$$

ubi r^{bbcc}, r^{aacc}, r^{aabb} erunt resp. radices propriae aequationum $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$.

27.

Hinc facile concluditur generaliter, si n sit productum e factoribus quotcunque inter se primis a, b, c etc., W fieri productum e totidem factoribus, qui sint

$$1 + r^{\frac{nn}{aa}} + r^{\frac{4nn}{aa}} + r^{\frac{9nn}{aa}} + \text{etc.} + r^{\frac{(a-1)^2 nn}{aa}}$$
$$1 + r^{\frac{nn}{bb}} + r^{\frac{4nn}{bb}} + r^{\frac{9nn}{bb}} + \text{etc.} + r^{\frac{(b-1)^2 nn}{bb}}$$
$$1 + r^{\frac{nn}{cc}} + r^{\frac{4nn}{cc}} + r^{\frac{9nn}{cc}} + \text{etc.} + r^{\frac{(c-1)^2 nn}{cc}} \quad \text{etc.}$$

ubi $r^{\frac{nn}{ab}}, \frac{nn}{rbb}, r^{\frac{nn}{cc}}$ etc. erunt radices propriae aequationum $x^a - 1 = 0, x^b - 1 = 0$, $x^c - 1 = 0$ etc.

28.

Ex his principiis transitus ad determinationem completam ipsius W pro valore quocunque ipsius n sponte iam obvius est. Decomponatur scilicet n in factores a,

b, c etc. tales, qui sint vel numeri primi inaequales, vel potestates numerorum primorum inaequalium, statuatur $r^{\frac{nn}{aa}} = A$, $r^{\frac{nn}{bb}} = B$, $r^{\frac{nn}{cc}} = C$ etc., eruntque A, B, C etc. radices propriae aequationum $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$ etc., atque W productum e factoribus

$$1 + A + A^4 + A^9 + \text{etc.} + A^{(u-1)^2}$$
$$1 + B + B^4 + B^9 + \text{etc.} + B^{(b-1)^2}$$
$$1 + C + C^4 + C^9 + \text{etc.} + C^{(c-1)^2} \text{ etc.}$$

Sed hi singuli factores per ea, quae in artt 20, 21, 23 docuimus, determinari poterunt, unde etiam valor producti innotescet. Regulas pro determinandis illis factoribus hic in unum obtutum collegisse haud inutile erit. Quum radix A fiat $= \frac{kn}{a} \cdot \frac{360^0}{a}$, aggregatum $1 + A + A^4 + A^9 + \text{etc.} + A^{(a-1)^2}$, quod per L denotabimus, perinde per numerum $\frac{kn}{a}$ determinabitur, ut in disquisitione nostra generali W per k. Duodecim iam casus sunt distinguendi.

I. Si a est numerus primus formae $4\mu + 1$, puta $= p$, vel potestas talis numeri primi cum exponente impari, simulque $\frac{kn}{a}$ residuum quadraticum ipsius p, erit $L = +\sqrt{a}$.

II. Si manentibus reliquis $\frac{kn}{a}$ est non-residuum quadraticum ipsius p, erit $L = -\sqrt{a}$.

III. Si a est numerus primus formae $4\mu + 3$, puta $= p$, vel potestas talis numeri primi cum exponente impari, simulque $\frac{kn}{a}$ residuum quadraticum ipsius p, erit $L = +i\sqrt{a}$.

IV. Si, manentibus reliquis ut in III, $\frac{kn}{a}$ est non-residuum quadraticum ipsius p, erit $L = -i\sqrt{a}$.

V. Si a est quadratum, altiorve potestas numeri primi (imparis) cum exponente pari, erit $L = +\sqrt{a}$.

VI. Si $a = 2$, erit $L = 0$.

VII. Si $a = 4$, altiorve potestas binarii cum exponente pari, simulque $\frac{kn}{a}$ formae $4\mu + 1$, erit $L = (1+i)\sqrt{a}$.

VIII. Si, manentibus reliquis ut in VII, $\frac{kn}{a}$ est formae $4\mu + 3$, erit $L = (1-i)\sqrt{a}$.

IX. Si $a = 8$, altiorve potestas binarii cum exponente impari, simulque $\frac{kn}{a}$ formae $8\mu + 1$, erit $L = (1+i)\sqrt{a}$.

X. Si, manentibus reliquis ut in IX, $\frac{kn}{a}$ est formae $8\mu+3$, erit $L=(-1+i)\sqrt{a}$.
XI. Si manentibus reliquis $\frac{kn}{a}$ est formae $8\mu+5$, erit $L=(-1-i)\sqrt{a}$.
XII. Si manentibus reliquis $\frac{kn}{a}$ est formae $8\mu+7$, erit $L=(1-i)\sqrt{a}$.

29.

Sit exempli caussa $n=2520=8.9.5.7$, atque $k=13$. Hic erit

pro $a=8$, per casum XII, $L=(1-i)\sqrt{8}$
pro factore 9, per casum V, summa respondens erit $=\sqrt{9}$
pro factore 5, per casum II, summa respondens erit $=-\sqrt{5}$
pro factore 7, per casum III, summa respondens erit $=+i\sqrt{7}$

Hinc fit $W=(1-i)\cdot(-i)\cdot\sqrt{2520}=(-1-i)\sqrt{2520}$.

Sit pro eodem valore ipsius n, $k=1$: tunc respondebit

factori 8 summa $(-1+i)\sqrt{8}$
factori 9 summa $\sqrt{9}$
factori 5 summa $\sqrt{5}$
factori 7 summa $-i\sqrt{7}$

Hinc conflatur productum $W=(1+i)\sqrt{2520}$.

30.

Methodus alia, summam W generaliter determinandi, petitur ex iis, quae in artt. 22, 24 exposita sunt. Statuamus $\cos\omega+i\sin\omega=\rho$, atque

$$\rho^{\frac{nn}{aa}}=\alpha,\quad \rho^{\frac{nn}{bb}}=\beta,\quad \rho^{\frac{nn}{cc}}=\gamma \text{ etc.}$$

ita ut habeatur $r=\rho^k$, $A=\alpha^k$, $B=\beta^k$, $C=\gamma^k$ etc. Tunc erit

$$1+\rho+\rho^4+\rho^9+\text{etc.}+\rho^{(n-1)^2}$$

productum e factoribus

$$1+\alpha+\alpha^4+\alpha^9+\text{etc.}+\alpha^{(a-1)^2}$$
$$1+\beta+\beta^4+\beta^9+\text{etc.}+\beta^{(b-1)^2}$$
$$1+\gamma+\gamma^4+\gamma^9+\text{etc.}+\gamma^{(c-1)^2} \text{ etc.}$$

adeoque W productum e factoribus

$$w = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(n-1)^2}$$
$$\mathfrak{A} = \frac{1+A+A^4+A^9+\text{etc.}+A^{(a-1)^2}}{1+\alpha+\alpha^4+\alpha^9+\text{etc.}+a^{(a-1)^2}}$$
$$\mathfrak{B} = \frac{1+B+B^4+B^9+\text{etc.}+B^{(b-1)^2}}{1+\beta+\beta^4+\beta^9+\text{etc.}+\beta^{(b-1)^2}}$$
$$\mathfrak{C} = \frac{1+C+C^4+C^9+\text{etc.}+C^{(c-1)^2}}{1+\gamma+\gamma^4+\gamma^9+\text{etc.}+\gamma^{(c-1)^2}} \text{ etc.}$$

Iam factor primus w determinatus est per disquisitiones supra traditas (art. 19); factores reliqui vero $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. prodeunt per formulas artt. 22, 24, quas ut omnia iuncta habeantur, hic denuo colligimus[1]. Duodecim casus hic sunt distinguendi, scilicet

I. Si a est numerus primus (impar) $= p$, vel talis numeri potestas cum exponente impari, atque k residuum quadraticum ipsius p, erit factor respondens $\mathfrak{A} = +1$.

II. Si manentibus reliquis k est non-residuum quadraticum ipsius p, erit $\mathfrak{A} = -1$.

III. Si a est quadratum numeri primi imparis, altiorve eius potestas cum exponente pari, erit $\mathfrak{A} = +1$.

IV. Si a est $= 4$, aut altior binarii potestas cum exponente pari, simulque k formae $4\mu + 1$, erit $\mathfrak{A} = +1$.

V. Si, manentibus reliquis ut in IV, k est formae $4\mu + 3$, atque $\frac{n}{a}$ formae $4\mu + 1$, erit $\mathfrak{A} = -i$.

VI. Si, manentibus reliquis ut in IV, k est formae $4\mu + 3$, atque $\frac{n}{a}$ formae $4\mu + 3$, erit $\mathfrak{A} = +i$.

VII. Si a est $= 8$, aut altior binarii potestas cum exponente impari, atque k formae $8\mu + 1$, erit $\mathfrak{A} = +1$.

VIII. Si, manentibus reliquis ut in VII, k est formae $8\mu + 5$, erit $\mathfrak{A} = -1$.

IX. Si, manentibus reliquis ut in VII, k est formae $8\mu + 3$, atque $\frac{n}{a}$ formae $4\mu + 1$, erit $\mathfrak{A} = +i$.

[1] Manifesto, quae illic erant k et h, hic erunt $\frac{n}{a}$ et k respectu factoris secundi, $\frac{n}{b}$ et k respectu factoris tertii etc.

X. Si, manentibus reliquis ut in VII, k est formae $8\mu+3$, atque $\frac{n}{a}$ formae $4\mu+3$, erit $\mathfrak{A}=-i$.

XI. Si, manentibus reliquis ut in VII, k est formae $8\mu+7$, atque $\frac{n}{a}$ formae $4\mu+1$ erit $\mathfrak{A}=-i$.

XII. Si, manentibus reliquis ut in VII, k est formae $8\mu+7$, atque $\frac{n}{a}$ formae $4\mu+3$, erit $\mathfrak{A}=+i$.

Casum eum, ubi $a=2$, praeterimus; hic quidem $\mathfrak{A}$ foret $=\frac{0}{0}$ sive indeterminatus, sed tunc semper $W=0$.

Factores reliqui $\mathfrak{B}$, $\mathfrak{C}$ etc. perinde pendent a b, c etc., ut $\mathfrak{A}$ ab a, quatenus in illorum determinationem ingrediuntur.

31.

Secundum hanc methodum alteram exemplum primum art. 29 ita se habet:

Factor w fit $=(1+i)\sqrt{2520}$
Pro $a=8$ factor respondens $\mathfrak{A}$ fit, per casum VIII, $=-1$
Factori ipsius n secundo 9 respondet factor $+1$ (per casum III.)
Factori 5 respondet factor -1 (per casum II.)
Factori 7 respondet factor -1 (per casum II.)

Hinc conflatur productum $W=(-1-i)\sqrt{2520}$, ut in art. 29.

32.

Quum valor ipsius W per methodos *duas* determinari possit, quarum altera relationibus numerorum $\frac{nk}{a}$, $\frac{nk}{b}$, $\frac{nk}{c}$ etc. ad numeros a, b, c etc. innititur, altera vero a relationibus ipsius k ad numeros a, b, c etc. pendet, inter omnes has relationes nexus quidam conditionalis intercedere debet, ita ut quaevis e reliquis determinabilis esse debeat. Supponamus, omnes numeros a, b, c etc. esse numeros primos impares, atque k accipi $=1$; distribuanturque factores a, b, c etc. in duas classes, quarum altera contineat eos, qui sunt formae $4\mu+1$, et qui denotentur per p, p', p'' etc., altera vero constet ex iis, qui sunt formae $4\mu+3$, et qui exprimantur per q, q', q'' etc.: multitudinem posteriorum designabimus per m. His ita factis, observamus primo, n fieri formae $4\mu+1$, si m fuerit par (quorsum etiam referri debet casus is, ubi factores classis alterius omnino desunt, sive ubi $m=0$), contra n fieri formae $4\mu+3$, si m fuerit impar. Iam determinatioipsius W per methodum primam ita perficitur.

Pendeant numeri P, P', P'' etc., Q, Q', Q'' etc. ita a relationibus numerorum $\frac{n}{p}$, $\frac{n}{p'}$, $\frac{n}{p''}$ etc., $\frac{n}{q}$, $\frac{n}{q'}$, $\frac{n}{q''}$ etc. ad numeros p, p', p'' etc., q, q', q'' etc. resp., ut statuatur

$$P = +1, \text{ si } \tfrac{n}{p} \text{ est residuum quadraticum ipsius } p$$
$$P = -1, \text{ si } \tfrac{n}{p} \text{ est non-residuum quadraticum ipsius } p$$

et perinde de reliquis. Tunc erit W productum e factoribus $P\sqrt{p}$, $P'\sqrt{p'}$, $P''\sqrt{p''}$ etc., $iQ\sqrt{q}$, $iQ'\sqrt{q'}$, $iQ''\sqrt{q''}$ etc., adeoque

$$W = PP'P'' \ldots QQ'Q'' \ldots i^m\sqrt{n}$$

Per methodum secundam, aut potius statim per praecepta art. 19, erit

$$W = +\sqrt{n}, \text{ si } n \text{ est formae } 4\mu+1, \text{ vel quod eodem redit, si } m \text{ est par}$$
$$W = +i\sqrt{n}, \text{ si } n \text{ est formae } 4\mu+3, \text{ vel si } m \text{ est impar}$$

Utrumque casum simul complecti licet per formulam sequentem:

$$W = i^{mm}\sqrt{n}$$

Hinc itaque colligitur

$$PP'P'' \ldots QQ'Q'' \ldots = i^{mm-m}$$

Sed i^{mm-m} fit $=1$, quoties m est formae 4μ vel $4\mu+1$, atque $=-1$, quoties m est formae $4\mu+2$ vel $4\mu+3$, unde deducimus sequens elegantissimum

THEOREMA. *Denotantibus a, b, c etc. numeros primos impares positivos inaequales, quorum productum statuitur $= n$, et inter quos m sint formae $4\mu+3$, reliqui formae $4\mu+1$: multitudo eorum ex his numeris a, b, c etc., quorum non-residua resp. sunt $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$ etc., par erit, quoties m est formae 4μ vel $4\mu+1$, impar vero, quoties m est formae $4\mu+2$ vel $4\mu+3$.*

Ita e.g. statuendo $a=3$, $b=5$, $c=7$, $d=11$, habemus tres numeros formae $4\mu+3$, puta 3, 7 et 11; est autem $5.7.11R3$; $3.7.11R5$; $3.5.11R7$; $3.5.7N11$, sive unicus $\frac{n}{d}$ est non-residuum ipsius d.

33.

Celeberrimum *theorema fundamentale* circa residua quadratica nihil aliud est, nisi casus specialis theorematis modo evoluti. Limitando scilicet multitudinemnumerorum

a, b, c etc. ad *duos*, patet, si unus tantum ex ipsis, vel neuter, sit formae $4\mu+3$, fieri debere vel simul aRb, bRa, vel simul aNb, bNa; contra si uterque est formae $4\mu+3$, unus ex ipsis alterius non-residuum esse debebit, atque hic illius residuum. En itaque demonstrationem *quartam* huius gravissimi theorematis, cuius demonstrationem primam et secundam in Disquisitionibus Arithmeticis, tertiam nuper in commentatione peculiari tradidimus (*Commentt.* T. XVI): duas alias principiis rursus omnino diversis innitentes in posterum exponemus. Summopere sane est mirandum, quod hocce venustissimum theorema, quod primo omnes conatus tam pertinaciter eluserat, tot postea viis toto coelo inter se distantibus adiri potuerit.

34.

Etiam theoremata reliqua, quae quasi supplementum ad theorema fundamentale efficiunt, scilicet per quae dignoscuntur numeri primi, quorum residua vel non-residua sunt -1, $+2$ et -2, ex iisdem principiis derivari possunt. Incipiemus a residuo $+2$.

Statuendo $n=8a$, ita ut a sit numerus primus, atque $k=1$, per methodum art. 28, W erit productum e duobus factoribus, quorum alter erit $+\sqrt{a}$, vel $+i\sqrt{a}$, si 8, vel quod idem est 2, est residuum quadraticum ipsius a; contra $-\sqrt{a}$ vel $-i\sqrt{a}$, si 2 est non-residuum ipsius a. Factor secundus autem est

$$\begin{aligned}
&(1+i)\sqrt{8}, \text{ si } a \text{ est formae } 8\mu+1\\
&(-1+i)\sqrt{8}, \text{ si } a \text{ est formae } 8\mu+3\\
&(-1-i)\sqrt{8}, \text{ si } a \text{ est formae } 8\mu+5\\
&(1-i)\sqrt{8}, \text{ si } a \text{ est formae } 8\mu+7
\end{aligned}$$

Sed per art. 18 semper erit $W=(1+i)\sqrt{n}$; dividendo hunc valorem per quatuor valores factoris secundi, patet, factorem primum fieri debere

$$\begin{aligned}
&+\sqrt{a}, \text{ si } a \text{ est formae } 8\mu+1\\
&-i\sqrt{a}, \text{ si } a \text{ est formae } 8\mu+3\\
&-\sqrt{a}, \text{ si } a \text{ est formae } 8\mu+5\\
&+i\sqrt{a}, \text{ si } a \text{ est formae } 8\mu+7
\end{aligned}$$

Hinc sponte sequitur, in casu primo et quarto 2 esse debere residuum ipsius a, in casu secundo et tertio autem non-residuum.

35.

Numeri primi, quorum residuum vel non-residuum est -1, facile dignoscuntur adiumento theorematis sequentis, quod etiam per se ipsum satis memorabile est.

THEOREMA. *Productum e duobus factoribus*

$$W' = 1 + r^{-1} + r^{-4} + \text{etc.} + r^{-(n-1)^2}$$
$$W = 1 + r + r^4 + \text{etc.} + r^{(n-1)^2}$$

est $= n$, *si* n *est impar; vel* $= 0$, *si* n *est impariter par; vel* $= 2n$, *si* n *est pariter par.*

Demonstr. Quum manifesto fiat

$$\begin{aligned} W &= r + r^4 + r^9 + \text{etc.} + r^{nn} \\ &= r^4 + r^9 + \text{etc.} + r^{(n+1)^2} \\ &= r^9 + \text{etc.} + r^{(n+2)^2} \text{ etc.} \end{aligned}$$

productum WW' ita quoque exhiberi poterit

$$\begin{aligned} & 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} \\ & + r^{-1}(r + r^4 + r^9 + r^{16} + \text{etc.} + r^{nn}) \\ & + r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \text{etc.} + r^{(n+1)^2}) \\ & + r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \text{etc.} + r^{(n+2)^2}) \\ & \text{etc.} \\ & + r^{-(n-1)^2}(r^{(n-1)^2} + r^{nn} + r^{(n+1)^2} + r^{(n+2)^2} + \text{etc.} + r^{(2n-2)^2}) \end{aligned}$$

quod aggregatum verticaliter summatum producit

$$\begin{aligned} & n \\ & + r(1 + rr + r^4 + r^6 + \text{etc.} + r^{2n-2}) \\ & + r^4(1 + r^4 + r^8 + r^{12} + \text{etc.} + r^{4n-4}) \\ & + r^9(1 + r^6 + r^{12} + r^{18} + \text{etc.} + r^{6n-6}) \\ & + \text{etc.} \\ & + r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \text{etc.} + r^{2(n-1)^2}) \end{aligned}$$

Iam si n impar est, singulae partes huius aggregati, praeter primam n, erunt $= 0$; secunda enim manifesto fit $\frac{r(1-r^{2n})}{1-rr}$, tertia $\frac{r^4(1-r^{4n})}{1-r^4}$ etc. Quoties vero n par est, excipere insuper oportebit partem

$$r^{\frac{1}{4}nn}(1+r^n+r^{2n}+r^{3n}+\text{etc.}+r^{nn-n})$$

quae fit $=nr^{\frac{1}{4}nn}$. In casu priori itaque fit $WW'=n$, in posteriori autem $=n+nr^{\frac{1}{4}nn}$; sed $r^{\frac{1}{4}nn}$ fit $=+1$, si n est pariter par, tunc itaque prodit $WW'=2n$; contra fit $r^{\frac{1}{4}nn}=-1$, si n est impariter par, ubi itaque evadit $WW'=0$. Q. E. D.

36.

Iam per art. 22 constat, si n sit numerus primus impar, $\frac{W'}{W}$ fieri $=+1$ vel $=-1$, prout -1 fuerit residuum vel non-residuum ipsius n. Hinc in casu priori esse debebit $W^2=+n$, in posteriori $W^2=-n$; quamobrem per art. 13 concludimus, casum priorem tunc tantum locum habere posse, quando n sit formae $4\mu+1$, casumque posteriorem, quando n sit formae $4\mu+3$.

Denique e combinatione conditionum pro residuis $+2$ et -1 inventarum sponte sequitur, -2 esse residuum cuiusvis numeri primi formae $8\mu+1$ vel $8\mu+3$, atque non-residuum cuiusvis numeri primi formae $8\mu+5$ vel $8\mu+7$.

THEOREMATIS FUNDAMENTALIS

IN

DOCTRINA DE RESIDUIS QUADRATICIS

DEMONSTRATIONES ET AMPLIATIONES NOVAE

A U C T O R E

CAROLO FRIDERICO GAUSS

SOCIETATI REGIAE SCIENTIARUM TRADITAE 1817, FEBR. 10.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. IV.
Gottingae MDCCCXVIII.

THEOREMATIS FUNDAMENTALIS

IN

DOCTRINA DE RESIDUIS QUADRATICIS

DEMONSTRATIONES ET AMPLIATIONES NOVAE.

Theorema fundamentale de residuis quadraticis, quod inter pulcherrimas arithmeticae sublimioris veritates refertur, facile quidem per inductionem detectum, longe vero difficilius demonstratum est. Saepius in hoc genere accidere solet, ut veritatum simplicissimarum, quae scrutatori per inductionem sponte quasi se offerunt, demonstrationes profundissime lateant et post multa demum tentamina irrita, longe forte alia quam qua quaesitae erant via, tandem in lucem protrahi possint Dein haud raro fit, quum primum una inventa est via, ut plures subinde patefiant ad eandem metam perducentes, aliae brevius et magis directe, aliae quasi ex obliquo et a principiis longe diversis exorsae, inter quae et quaestionem propositam vix ullum vinculum suspicatus fuisses. Mirus huiusmodi nexus inter veritates abstrusiores non solum peculiarem quandam venustatem hisce contemplationibus conciliat, sed ideo quoque sedulo investigari atque enodari meretur, quod haud raro nova ipsius scientiae subsidia vel incrementa inde demanant.

Etsi igitur theorema arithmeticum, de quo hic agetur, per curas anteriores, quae quatuor demonstrationes inter se prorsus diversas[2] suppeditaverunt, pleneabsolutum

[2]Duae expositae sunt in Disquisitionum Arithmeticarum Sect. quarta et quinta; tertia in commentatione peculiari (Commentt. Soc. Gotting. Vol. XVI), quarta inserta est commentationi: Summatio quarundam serierum singularium (Commentt. Recentiores, Vol. I).

videri possit, tamen denuo ad idem argumentum revertor, duasque alias demonstrationes adiungo, quae novam certe lucem huic rei affundent. Prior quidem tertiae quodammodo affinis est, quod ab eodem lemmate proficiscitur; postea vero iter diversum prosequitur, ita ut merito pro demonstratione nova haberi possit, quae concinnitate ipsa illa tertia si non superior saltem haud inferior videbitur. Contra demonstratio sexta principio plane diverso subtiliori innixa est novumque sistit exemplum mirandi nexus inter veritates arithmeticas primo aspectu longissime ab invicem remotas. Duabus hisce demonstrationibus adiungitur algorithmus novus persimplex ad diiudicandum, utrum numerus integer datus numeri primi dati residuum quadraticum sit an non-residuum.

Alia adhuc affuit ratio, quae ut novas demonstrationes, novem iam abhinc annos promissas, nunc potissimum promulgarem, effecit. Scilicet quum inde ab anno 1805 theoriam residuorum cubicorum atque biquadraticorum, argumentum longe difficilius, perscrutari coepissem, similem fere fortunam, ac olim in theoria residuorum quadraticorum, expertus sum. Protinus quidem theoremata ea, quae has quaestiones prorsus exhauriunt, et in quibus mira analogia cum theorematibus ad residua quadratica pertinentibus eminet, per inductionem detecta fuerunt, quam primum via idonea quaesita essent: omnes vero conatus, ipsorum demonstrationibus ex omni parte perfectis potiundi, per longum tempus irriti manserunt. Hoc ipsum incitamentum erat, ut demonstrationibus iam cognitis circa residua quadratica alias aliasque addere tantopere studerem, spe fultus, ut ex multis methodis diversis una vel altera ad illustrandum argumentum affine aliquid conferre posset. Quae spes neutiquam vana fuit, laboremque indefessum tandem successus prosperi sequuti sunt. Mox vigiliarum fructus in publicam lucem edere licebit: sed antequam arduum hoc opus aggrediar, semel adhuc ad theoriam residuorum quadraticorum reverti, omnia quae de eadem adhuc supersunt agenda absolvere, atque sic huic arithmeticae sublimioris parti quasi valedicere constitui.

THEOREMATIS FUNDAMENTALIS IN THEORIA RESIDUORUM QUADRATICORUM DEMONSTRATIO QUINTA

1.

In introductione iam declaravimus, demonstrationem quintam et tertiam ab eodem lemmate proficisci, quod commoditatis caussa, in signis disquisitioni praesenti adaptatis hoc loco repetere visum est.

LEMMA. *Sit m numerus primus (positivus impar), M integer per m non divisibilis; capiantur residua minima positiva numerorum*

$$M, 2M, 3M, 4M \ldots \tfrac{1}{2}(m-1)M$$

secundum modulum m, quae partim erunt minora quam $\frac{1}{2}m$, partim maiora: posteriorum multitudo sit $= n$. Tunc erit M residuum quadraticum ipsius m, vel nonresiduum, prout n par est, vel impar.

DEMONSTR. Sint e residuis illis ea, quae minora sunt quam $\frac{1}{2}m$, haec a, b, c, d etc., reliqua vero, maiora quam $\frac{1}{2}m$, haec a', b', c', d' etc. Posteriorum complementa ad m, puta $m-a'$, $m-b'$, $m-c'$, $m-d'$ etc. manifesto cuncta minora erunt quam $\frac{1}{2}m$, atque tum inter se tum a residuis a, b, c, d etc. diversa, quamobrem cum his simul sumta, ordine quidem mutato, identica erunt cum omnibus numeris $1, 2, 3, 4 \ldots \frac{1}{2}(m-1)$. Statuendo itaque productum

$$1.2.3.4 \ldots \tfrac{1}{2}(m-1) = P$$

erit

$$P = abcd \ldots \times (m-a')(m-b')(m-c')(m-d') \ldots$$

adeoque

$$(-1)^n P = abcd \ldots \times (a'-m)(b'-m)(c'-m)(d'-m) \ldots$$

Porro fit, secundum modulum m,

$$PM^{\frac{1}{2}(m-1)} \equiv abcd \ldots \times a'b'c'd' \ldots \equiv abcd \ldots \times (a'-m)(b'-m)(c'-m)(d'-m) \ldots$$

adeoque

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n$$

Hinc $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, accepto signo superiori vel inferiori, prout n par est vel impar, unde adiumento theorematis in *Disquisitionibus Arithmeticis* art. 106 demonstrati lemmatis veritas sponte demanat.

2.

THEOREMA. *Sint m, M integri positivi impares inter se primi, n multitudo eorum e residuis minimis positivis numerorum*

$$M, 2M, 3M \ldots \tfrac{1}{2}(m-1)M$$

secundum modulum m, quae sunt maiora quam $\frac{1}{2}m$; ac perinde N multitudo eorum e residuis minimis positivis numerorum

$$m, 2m, 3m \ldots \tfrac{1}{2}(M-1)m$$

secundum modulum M, quae sunt maiora quam $\frac{1}{2}M$. Tunc tres numeri n, N, $\frac{1}{4}(m-1)(M-1)$ vel omnes simul pares erunt. vel unus par duoque reliqui impares.

DEMONSTR. Designemus

per f complexum numerorum $1, 2, 3 \ldots \frac{1}{2}(m-1)$
per f' complexum numerorum $m-1, m-2, m-3 \ldots \frac{1}{2}(m+1)$
per F complexum numerorum $1, 2, 3 \ldots \frac{1}{2}(M-1)$
per F' complexum numerorum $M-1, M-2, M-3 \ldots \frac{1}{2}(M+1)$

Indicabit itaque n, quot numeri Mf residua sua minima positiva secundum modulum m habeant in complexu f', et perinde N indicabit, quot numeri mF habeant residua sua minima positiva secundum modulum M in complexu F'. Denique designet

φ complexum numerorum $1, 2, 3 \ldots \frac{1}{2}(mM-1)$
φ' complexum numerorum $mM-1, mM-2, mM-3 \ldots \frac{1}{2}(mM+1)$

Quum quilibet integer per m non divisibilis secundum modulum m vel alicui residuo ex f vel alicui ex f' congruus esse debeat, ac perinde quilibet integer per M non divisibilis secundum modulum M congruus sit vel alicui residuo ex F vel alicui ex F': omnes numeri φ, inter quos manifesto nullus per m et M simul divisibilis occurrit, in octo classes sequenti modo distribui possunt.

I. In prima classe erunt numeri secundum modulum m alicui numero ex f, secundum modulum M vero alicui numero ex F congrui. Designabimus multitudinem horum numerorum per α.

II. Numeri secundum modulos m, M resp. numeris ex f, F' congrui, quorum multitudinem statuemus $= \beta$.

III. Numeri secundum modulos m, M resp. numeris ex f', F congrui, quorum multitudinem statuemus $= \gamma$.

IV. Numeri secundum modulos m, M resp. numeris ex f', F' congrui, quorum multitudo sit $= \delta$.

V. Numeri per m divisibiles, secundum modulum M vero residuis ex F congrui.

VI. Numeri per m divisibiles, secundum modulum M vero residuis ex F' congrui.

VII. Numeri per M divisibiles, secundum modulum m autem residuis ex f congrui.

VIII. Numeri per M divisibiles, secundum modulum m vero residuis ex f' congrui.

Manifesto classes V et VI simul sumtae complectentur omnes numeros mF, multitudo numerorum in VI contentorum erit $= N$, adeoque multitudo numerorum in V contentorum erit $\frac{1}{2}(M-1) - N$. Perinde classes VII et VIII simul sumtae continebunt omnes numeros Mf, in classe VIII reperientur n numeri, in classe VII autem $\frac{1}{2}(m-1) - n$.

Prorsus simili modo omnes numeri φ' in octo classes IX - XVI distribuentur, in quo negotio si eundem ordinem servamus, facile perspicietur, numeros in classibus

IX, X, XI, XII, XIII, XIV, XV, XVI

contentos resp. esse complementa numerorum in classibus

IV, III, II, I, VI, V, VIII, VII

contentorum ad mM, ita ut in classe IX reperiantur δ numeri; in classe X, γ et sic porro. Iam patet, si omnes numeri primae classis associentur cum omnibus numeris classis nonae, haberi omnes numeros infra mM, qui secundum modulum m alicui numero ex f, secundum modulum M vero alicui numero ex F sunt congrui, quorumque multitudinem aequalem esse multitudini omnium combinationum singulorum f cum singulis F, facile perspicitur. Habemus itaque

$$\alpha + \delta = \tfrac{1}{4}(m-1)(M-1)$$

similique ratione etiam erit

$$\beta + \gamma = \tfrac{1}{4}(m-1)(M-1)$$

Iunctis omnibus numeris classium II, IV, VI, manifesto habebimus omnes numeros infra $\frac{1}{2}mM$, qui alicui residuo ex F' secundum modulum M congrui sunt. Iidem vero numeri ita quoque exhiberi possunt:

$$F', M+F', 2M+F', 3M+F' \ldots \tfrac{1}{2}(m-3)M+F'$$

unde omnium multitudo erit $= \frac{1}{4}(m-1)(M-1)$, sive habebimus

$$\beta + \delta + N = \tfrac{1}{4}(m-1)(M-1)$$

Perinde e iunctione omnium classium III, IV, VIII colligere licet

$$\gamma + \delta + n = \tfrac{1}{4}(m-1)(M-1)$$

Ex his quatuor aequationibus oriuntur sequentes:

$$2\alpha = \tfrac{1}{4}(m-1)(M-1) + n + N$$
$$2\beta = \tfrac{1}{4}(m-1)(M-1) + n - N$$
$$2\gamma = \tfrac{1}{4}(m-1)(M-1) - n + N$$
$$2\delta = \tfrac{1}{4}(m-1)(M-1) - n - N$$

quarum quaelibet theorematis veritatem monstrat.

3.

Quodsi iam supponimus, m et M esse numeros primos, e combinatione theorematis praecedentis cum lemmate art. 1 theorema fundamentale protinus demanabit. Patet enim,

I. quoties uterque m, M, sive alteruter tantum, sit formae $4k+1$, numerum $\frac{1}{4}(m-1)(M-1)$ fore parem, adeoque n et N vel simul pares vel simul impares, et proin vel utrumque m et M alterius residuum quadraticum, vel utrumque alterius non-residuum quadraticum.

II. Quoties autem uterque m, M est formae $4k+3$, erit $\frac{1}{4}(m-1)(M-1)$ impar, hinc unus numerorum n, N par, alter impar, et proin unus numerorum m, M alterius residuum quadraticum, alter alterius non-residuum quadraticum.

Q. E. D.

THEOREMATIS FUNDAMENTALIS IN THEORIA RESIDUORUM QUADRATICORUM DEMONSTRATIO SEXTA.

1.

THEOREMA. *Designante p numerum primum (positivum imparem), n integrum positivum per p non divisibilem, x quantitatem indeterminatam, functio*

$$1 + x^n + x^{2n} + x^{3n} + \text{etc.} + x^{np-n}$$

divisibilis erit per

$$1 + x + xx + x^3 + \text{etc.} + x^{p-1}$$

DEMONSTR. Accipiatur integer positivus g ita ut fiat $gn \equiv 1 \pmod{p}$, statuaturque $gn = 1 + hp$. Tunc erit

$$\frac{1+x^n+x^{2n}+x^{3n}+\text{etc.}+x^{np-n}}{1+x+xx+x^3+\text{etc.}+x^{p-1}} = \frac{(1-x^{np})(1-x)}{(1-x^n)(1-x^p)} = \frac{(1-x^{np})(1-x^{gn}-x+x^{hp+1})}{(1-x^n)(1-x^p)}$$
$$= \frac{1-x^{np}}{1-x^p} \cdot \frac{1-x^{gn}}{1-x^n} - \frac{x(1-x^{np})}{1-x^n} \cdot \frac{1-x^{hp}}{1-x^p}$$

adeoque manifesto functio integra. Q. E. D.

Quaelibet itaque functio integra ipsius x per $\frac{1-x^{np}}{1-x^n}$ divisibilis, etiam divisibilis erit per $\frac{1-x^p}{1-x}$.

2.

Designet α radicem primitivam positivam pro modulo p, i.e. sit α integer positivus talis, ut residua minima positiva potestatum 1, α, $\alpha\alpha$, $\alpha^3 \ldots \alpha^{p-2}$ secundum modulum p sine respectu ordinis cum numeris 1, 2, 3, $4 \ldots p-1$ identica fiant. Designando porro per fx functionem

$$x + x^\alpha + x^{\alpha\alpha} + x^{\alpha^3} + \text{etc.} + x^{\alpha^{p-2}} + 1$$

patet, $fx - 1 - x - xx - x^3 - \text{etc.} - x^{p-1}$ divisibilem fore per $1 - x^p$, adeoque a potiori per $\frac{1-x^p}{1-x} = 1 + x + xx + x^3 + \text{etc.} + x^{p-1}$, per quam itaque functionem ipsa quoque fx divisibilis erit. Hinc vero sequitur, quum x exprimat quantitatem indeterminatam, esse quoque $f(x^n)$ divisibilem per $\frac{1-x^{np}}{1-x^n}$, et proin (art. praec.) etiam per $\frac{1-x^p}{1-x}$, quoties quidem n sit integer per p non divisibilis. Contra, quoties n est integer per p divisibilis, singulae partes functionis $f(x^n)$ unitate diminutae divisibiles erunt per

$1-x^p$; quamobrem in hoc casu etiam $f(x^n)-p$ per $1-x^p$ et proin etiam per $\frac{1-x^p}{1-x}$ divisibilis erit.

3.

THEOREMA. *Statuendo*

$$x - x^\alpha + x^{\alpha\alpha} - x^{\alpha^3} + x^{\alpha^4} - \text{etc.} - x^{\alpha^{p-2}} = \xi$$

erit $\xi\xi \mp p$ *divisibilis per* $\frac{1-x^p}{1-x}$, *accepto signo superiori, quoties* p *est formae* $4k+1$, *inferiori, quoties* p *est formae* $4k+3$.

DEMONSTR. Facile perspicietur, ex $p-1$ functionibus hisce

$$\begin{aligned}
&+ x\xi - xx + x^{\alpha+1} - x^{\alpha\alpha+1} + \text{etc.} + x^{\alpha^{p-2}+1} \\
&- x^\alpha\xi - x^{2\alpha} + x^{\alpha\alpha+\alpha} - x^{\alpha^3+\alpha} + \text{etc.} + x^{\alpha^{p-1}+\alpha} \\
&+ x^{\alpha\alpha}\xi - x^{2\alpha\alpha} + x^{\alpha^3+\alpha\alpha} - x^{\alpha^4+\alpha\alpha} + \text{etc.} + x^{\alpha^p+\alpha\alpha} \\
&- x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} + \text{etc.} + x^{\alpha^{p+1}+\alpha^3}
\end{aligned}$$

etc. usque ad

$$-x^{\alpha^{p-2}}\xi - x^{2\alpha^{p-2}} + x^{\alpha^{p-1}+\alpha^{p-2}} - x^{\alpha^p+\alpha^{p-2}} + \text{etc.} + x^{\alpha^{2p-4}+\alpha^{p-2}}$$

primam fieri $=0$, singulas reliquas autem per $1-x^p$ divisibiles. Quare per $1-x^p$ etiam divisibilis erit omnium summa, quae colligitur

$$\begin{aligned}
&= \xi\xi - (f(xx)-1) + (f(x^{\alpha+1})-1) - (f(x^{\alpha\alpha+1})-1) + (f(x^{\alpha^3+1})-1) - \text{etc.} \\
&\qquad + (f(x^{\alpha^{p-2}+1})-1) \\
&= \xi\xi - f(xx) + f(x^{\alpha+1}) - f(x^{\alpha\alpha+1}) + f(x^{\alpha^3+1}) - \text{etc.} + f(x^{\alpha^{p-2}+1}) = \Omega
\end{aligned}$$

Erit itaque haecce expressio Ω etiam divisibilis per $\frac{1-x^p}{1-x}$. Iam inter exponentes 2, $\alpha+1$, $\alpha\alpha+1$, $\alpha^3+1 \ldots \alpha^{p-2}+1$ unicus tantum erit divisibilis per p, puta $\alpha^{\frac{1}{2}(p-1)}+1$, unde per art. praec. singulae partes expressionis Ω hae

$$f(xx), f(x^{\alpha+1}), f(x^{\alpha\alpha+1}), f(x^{\alpha^3+1}) \text{ etc.}$$

excepto solo termino $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$, divisibiles erunt per $\frac{1-x^p}{1-x}$. Istas itaque partes delere licebit, ita ut per $\frac{1-x^p}{1-x}$ etiam divisibilis maneat functio

$$\xi\xi \mp f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$$

ubi signum superius vel inferius valebit, prout p est formae $4k+1$ vel formae $4k+3$.

Et quum insuper $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})-p$ divisibilis sit per $\frac{1-x^p}{1-x}$, erit etiam $\xi\xi\mp p$ per $\frac{1-x^p}{1-x}$ divisibilis. Q. E. D.

Ne duplex signum ullam ambiguitatem adducere possit, per ε numerum $+1$ vel -1 denotabimus, prout p est formae $4k+1$ vel $4k+3$. Erit itaque $\frac{(1-x)(\xi\xi-\varepsilon p)}{1-x^p}$ functio integra ipsius x, quam per Z designabimus.

4.

Sit q numerus positivus impar, adeoque $\frac{1}{2}(q-1)$ integer. Erit itaque $(\xi\xi)^{\frac{1}{2}(q-1)}-(\varepsilon p)^{\frac{1}{2}(q-1)}$ divisibilis per $\xi\xi-\varepsilon p$, et proin etiam per $\frac{1-x^p}{1-x}$. Statuamus $\varepsilon^{\frac{1}{2}(q-1)}=\delta$, atque

$$\xi^{q-1}-\delta p^{\frac{1}{2}(q-1)}=\tfrac{1-x^p}{1-x}\cdot Y$$

eritque Y functio integra ipsius x, atque $\delta=+1$, quoties unus numerorum p, q. sive etiam uterque, est formae $4k+1$; contra erit $\delta=-1$, quoties uterque p, q est formae $4k+3$.

5.

Iam supponamus, q quoque esse numerum primum (a p diversum) patetque per theorema in *Disquisitionibus Arithmeticis* art. 51 demonstratum,

$$\xi^q-(x^q-x^{q\alpha}+x^{q\alpha\alpha}-x^{q\alpha^3}+\text{etc.}-x^{q\alpha^{p-2}})$$

divisibilem fieri per q, sive formae qX, ita ut X sit functio integra ipsius x etiam respectu coëfficientium numericorum (quod etiam de functionibus reliquis integris hic occurrentibus Z, Y, W subintelligendum est). Designemus pro modulo p atque radice primitiva α indicem numeri q per μ, i.e. sit $q\equiv\alpha^\mu\pmod p$. Erunt itaque numeri q, $q\alpha$, $q\alpha\alpha$, $q\alpha^3\ldots q\alpha^{p-2}$ secundum modulum p resp. congrui numeris α^μ, $\alpha^{\mu+1}$, $\alpha^{\mu+2}\ldots\alpha^{p-2}$, 1, α, $\alpha\alpha\ldots\alpha^{\mu-1}$, adeoque

$$\begin{gathered}x^q-x^{\alpha^\mu}\\ x^{q\alpha}-x^{\alpha^{\mu+1}}\\ x^{q\alpha\alpha}-x^{\alpha^{\mu+2}}\\ x^{q\alpha^3}-x^{\alpha^{\mu+3}}\\ \vdots\end{gathered}$$

$$\begin{array}{l} x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}} \\ x^{q\alpha^{p-\mu-1}} - x \\ x^{q\alpha^{p-\mu}} - x^{\alpha} \\ x^{q\alpha^{p-\mu+1}} - x^{\alpha\alpha} \\ \quad \vdots \\ x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}} \end{array}$$

per $1 - x^p$ divisibiles. Quibus quantitatibus, alternis vicibus positive et negative sumtis atque summatis, patet, per $1 - x^p$ divisibilem esse functionem

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}} \mp \xi$$

valente signo superiori vel inferiori, prout μ par sit vel impar, i.e. prout q sit residuum quadraticum ipsius p vel non-residuum. Statuemus itaque

$$x^q - x^{q\alpha} + x^{q\alpha} - x^{q\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}} - \gamma\xi = (1 - x^p)W$$

faciendo $\gamma = +1$, vel $\gamma = -1$, prout q est residuum quadraticum ipsius p vel non-residuum, patetque, W fieri functionem integram.

6.

His ita praeparatis, e combinatione aequationum praecedentium deducimus

$$q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) + \tfrac{1-x^p}{1-x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi\xi - W\xi(1-x))$$

Supponamus, ex divisione functionis ξX per

$$x^{p-1} + x^{p-2} + x^{p-3} + \text{etc.} + x + 1$$

oriri quotientem U cum residuo T, sive haberi

$$\xi X = \tfrac{1-x^p}{1-x} \cdot U + T$$

ita ut U, T sint functiones integrae, etiam respectu coëfficientium numericorum, et quidem T ordinis certe inferioris, quam divisor. Erit itaque

$$qT - \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) = \tfrac{1-x^p}{1-x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi\xi - W\xi(1-x) - qU)$$

quae aequatio manifesto subsistere nequit, nisi tum membrum a laeva tum membrum a dextra per se evanescat. Erit itaque $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ per q divisibilis, nec non etiam

$\delta p^{\frac{1}{2}(q-1)} - \gamma$, adeoque etiam propter $\delta\delta = 1$, numerus $p^{\frac{1}{2}(q-1)} - \gamma\delta$ per q divisibilis erit.

Quodsi iam per β designatur unitas positive vel negative accepta, prout p est residuum vel non-residuum quadraticum numeri q, erit $p^{\frac{1}{2}(q-1)} - \beta$ per q divisibilis, adeoque etiam $\beta - \gamma\delta$, quod fieri nequit, nisi fuerit $\beta = \gamma\delta$. Hinc vero theorema fundamentale sponte sequitur. Scilicet

I. Quoties vel uterque p, q, vel alteruter tantum est formae $4k+1$, adeoque $\delta = +1$, erit $\beta = \gamma$, et proin vel simul q residuum quadraticum ipsius p, atque p residuum quadraticum ipsius q; vel simul q non-residuum ipsius p, atque p non-residuum ipsius q.

II. Quoties uterque p, q est formae $4k+3$, adeoque $\delta = -1$, erit $\beta = -\gamma$, adeoque vel simul q residuum quadraticum ipsius p, atque p non-residuum ipsius q; vel simul q non-residuum ipsius p, atque p residuum ipsius q. Q. E. D.

Algorithmus novus ad decidendum, utrum numerus integer positivus datus numeri primi positivi dati residuum quadraticum sit an non-residuum.

1.

Antequam solutionem novam huius problematis exponamus, solutionem in *Disquisitionibus Arithmeticis* traditam hic breviter repetemus, quae satis quidem expedite perficitur adiumento theorematis fundamentalis atque theorematum notorum sequentium:

I. Relatio numeri a ad numerum b (quatenus ille huius residuum quadraticum est sive non-residuum), eadem est quae numeri c ad b, si $a \equiv c \pmod{b}$.

II. Si a est productum e factoribus α, β, γ, δ etc., atque b numerus primus, relatio ipsius a ad b ita a relatione horum factorum ad b pendebit, ut a fiat residuum quadraticum ipsius b vel non-residuum, prout inter illos factores reperitur multitudo par vel impar talium, qui sint non-residua ipsius b. Quoties itaque aliquis factor est quadratum, ad eum in hoc examine omnino non erit respiciendum; si quis vero factor est potestas integri cum exponente impari, illius vice ipse hic integer fungi poterit.

III. Numerus 2 est residuum quadraticum cuiusvis numeri primi formae $8m+1$ vel $8m+7$, non-residuum vero cuiusvis numeri primi formae $8m+3$ vel $8m+5$.

Proposito itaque numero a, cuius relatio ad numerum primum b quaeritur: pro a, si maior est quam b, ante omnia substituetur eius residuum minimum positivum secundum modulum b, quo residuo in factores suos primos resoluto, quaestio per theorema II reducta est ad inventionem relationis singulorum horum factorum ad b. Relatio factoris 2, (siquidem adest vel semel, vel ter, vel quinquies etc.) innotescit per theorema III; relatio reliquorum, per theorema fundamentale, pendet a relatione ipsius b ad singulos. Hoc itaque modo loco unius relationis numeri dati ad numerum primum b iam investigandae sunt aliquae relationes numeri b ad alios primos impares ipso b minores, quae problemata eodem modo ad minores modulos deprimentur, manifestoque hae depressiones successivae tandem exhaustae erunt.

2.

Ut exemplo haec solutio illustretur, quaerenda sit relatio numeri 103 ad 379. Quum 103 iam sit minor quam 379, atque ipse numerus primus, protinus applicandum erit theorema fundamentale, quod docet, relationem quaesitam oppositam esse relationi numeri 379 ad 103. Haec iterum aequalis est relationi numeri 70 ad 103, quae ipsa pendet a relationibus numerorum 2, 5, 7 ad 103. Prima harum relationum e theoremate III innotescit. Secunda per theorema fundamentale pendet a relatione numeri 103 ad 5, cui per theorema I aequalis est relatio numeri 3 ad 5; haec iterum per theorema fundamentale pendet a relatione numeri 5 ad 3, cui per theorema I aequalis est relatio numeri 2 ad 3, per theorema III nota. Perinde relatio numeri 7 ad 103 per theorema fundamentale a relatione numeri 103 ad 7 pendet, quae per theorema I aequalis est relationi numeri 5 ad 7; haec iterum per theorema fundamentale pendet a relatione numeri 7 ad 5, cui aequalis est per theorema I relatio numeri 2 ad 5 per theorema III nota. Quodsi iam hanc analysin in synthesin transmutare placet, quaestionis decisio ad quatuordecim momenta referetur, quae complete hic apponimus, ut maior concinnitas solutionis novae eo clarius elucescat.

1. Numerus 2 est residuum quadraticum numeri 103 (theor. III).
2. Numerus 2 est non-residuum quadraticum numeri 3 (theor. III).
3. Numerus 5 est non-residuum quadraticum numeri 3 (ex I et 2).
4. Numerus 3 est non-residuum quadraticum numeri 5 (theor. fund. et 3).
5. Numerus 103 est non-residuum quadraticum numeri 5 (I et 4).

6. Numerus 5 est non-residuum quadraticum numeri 103 (theor. fund. et 5).
7. Numerus 2 est non-residuum quadraticum numeri 5 (theor. III).
8. Numerus 7 est non-residuum quadraticum numeri 5 (I et 7).
9. Numerus 5 est non-residuum quadraticum numeri 7 (theor. fund. et 8).
10. Numerus 103 est non-residuum quadraticum numeri 7 (I et 9).
11. Numerus 7 est residuum quadraticum numeri 103 (theor. fund. et 10).
12. Numerus 70 est non-residuum quadraticum numeri 103 (II, 1, 6, 11).
13. Numerus 379 est non-residuum quadraticum numeri 103 (I et 12).
14. Numerus 103 est residuum quadraticum numeri 379 (theor. fund. et 13).

In sequentibus brevitatis caussa utemur signo in *Comment. Gotting. Vol.* XVI introducto. Scilicet per $[x]$ denotabimus quantitatem x ipsam, quoties x est integer, sive integrum proxime minorem quam x, quoties x est quantitas fracta, ita ut $x-[x]$ semper fiat quantitas non negativa unitate minor.

3.

PROBLEMA. *Denotantibus a, b integros positivos inter se primos, et posito $\left[\frac{1}{2}a\right]=a'$, invenire aggregatum*

$$\left[\frac{b}{a}\right]+\left[\frac{2b}{a}\right]+\left[\frac{3b}{a}\right]+\left[\frac{4b}{a}\right]+\text{etc.}+\left[\frac{a'b}{a}\right]$$

SOL. Designemus brevitatis caussa huiusmodi aggregatum per $\varphi(a,b)$, ita ut etiam fiat

$$\varphi(b,a)=\left[\frac{a}{b}\right]+\left[\frac{2a}{b}\right]+\left[\frac{3a}{b}\right]+\text{etc.}+\left[\frac{b'a}{b}\right]$$

si statuimus $\left[\frac{1}{2}b\right]=b'$. In demonstratione tertia theorematis fundamentalis ostensum est, pro casu eo, ubi a et b sunt impares, fieri

$$\varphi(a,b)+\varphi(b,a)=a'b'$$

facileque eandem methodum sequendo veritas huius propositionis ad eum quoque casum extenditur, ubi alteruter numerorum a, b est impar, uti illic iam addigitavimus. Dividatur, ad instar methodi, per quam duorum integrorum divisor communis maximus investigatur, a per b, sitque β quotiens atque c residuum; dein dividatur b per c et sic porro, ita ut habeantur aequationes

$$a = \beta b + c$$
$$b = \gamma c + d$$
$$c = \delta d + e$$
$$d = \varepsilon e + f \text{ etc.}$$

Hoc modo in serie numerorum continuo decrescentium b, c, d, e, f etc. tandem ad unitatem perveniemus, quum per hyp. a et b sint inter se primi, ita ut aequatio ultima fiat

$$k = \lambda l + 1$$

Quum manifesto habeatur

$$\left[\tfrac{a}{b}\right] = \left[\beta + \tfrac{c}{b}\right] = \beta + \left[\tfrac{c}{b}\right]$$
$$\left[\tfrac{2a}{b}\right] = \left[2\beta + \tfrac{2c}{b}\right] = 2\beta + \left[\tfrac{2c}{b}\right]$$
$$\left[\tfrac{3a}{b}\right] = \left[3\beta + \tfrac{3c}{b}\right] = 3\beta + \left[\tfrac{3c}{b}\right]$$

etc., erit

$$\varphi(b,a) = \varphi(b,c) + \tfrac{1}{2}\beta(b'b' + b')$$

et proin

$$\varphi(a,b) = a'b' - \tfrac{1}{2}\beta(b'b' + b') - \varphi(b,c)$$

Per similia ratiocinia fit, si statuimus $\left[\tfrac{1}{2}c\right] = c'$, $\left[\tfrac{1}{2}d\right] = d'$, $\left[\tfrac{1}{2}e\right] = e'$ etc.,

$$\varphi(b,c) = b'c' - \tfrac{1}{2}\gamma(c'c' + c') - \varphi(a,d)$$
$$\varphi(c,d) = c'd' - \tfrac{1}{2}\delta(d'd' + d') - \varphi(d,e)$$
$$\varphi(d,e) = d'e' - \tfrac{1}{2}\varepsilon(e'e' + e') - \varphi(e,f)$$

etc. usque ad

$$\varphi(k,l) = k'l' - \tfrac{1}{2}\lambda(l'l' + l') - \varphi(l,1)$$

Hinc, quoniam manifesto est $\varphi(l,1) = 0$, colligimus formulam

$$\varphi(a,b) = a'b' - b'c' + c'd' - d'e' + \text{etc.} \pm k'l'$$
$$- \tfrac{1}{2}\beta(b'b' + b') + \tfrac{1}{2}\gamma(c'c' + c') - \tfrac{1}{2}\delta(d'd' + d') + \tfrac{1}{2}\varepsilon(e'e' + e') - \text{etc.} \mp \tfrac{1}{2}\lambda(l'l' + l')$$

4.

Facile iam ex iis, quae in demonstratione tertia exposita sunt, colligitur, relationem numeri b ad a, quoties a sit numerus primus, sponte cognosci e valore

aggregati $\varphi(a, 2b)$. Scilicet prout hoc aggregatum est numerus par vel impar, erit b residuum quadraticum ipsius a vel non-residuum. Ad eundem vero finem ipsum quoque aggregatum $\varphi(a, b)$ adhiberi poterit, ea tamen restrictione, ut casus ubi b impar est ab eo ubi par est distinguatur. Scilicet

I. Quoties b est impar, erit b residuum vel non-residuum quadraticum ipsius a, prout $\varphi(a, b)$ par est vel impar.

II. Quoties b est par, eadem regula valebit, si insuper a est vel formae $8n+1$ vel formae $8n+7$; si vero pro valore pari ipsius b modulus a est vel formae $8n+3$ vel formae $8n+5$, regula opposita applicanda erit, puta, b erit residuum quadraticum ipsius a, si $\varphi(a, b)$ est impar, non-residuum vero, si $\varphi(a, b)$ est par.

Haec omnia ex art. 4 demonstrationis tertiae facillime derivantur.

5.

Exemplum. Si quaeritur relatio numeri 103 ad numerum primum 379, habemus, ad eruendum aggregatum $\varphi(379, 103)$,

$$\begin{array}{r|l|l} a = 379 & a' = 189 & \\ b = 103 & b' = \ 51 & \beta = 3 \\ c = \ 70 & c' = \ 35 & \gamma = 1 \\ d = \ 33 & d' = \ 16 & \delta = 2 \\ e = \ 4 & e' = \ 2 & \varepsilon = 8 \end{array}$$

hinc

$$\varphi(379, 103) = 9639 - 1785 + 560 - 32 - 3978 + 630 - 272 + 24 = 4786$$

unde 103 erit residuum quadraticum numeri 379. Si ad eundem finem aggregatum $(379, 206)$ adhibere malumus, habemus hocce paradigma:

$$\begin{array}{r|r|l} 379 & 189 & \\ 206 & 103 & 1 \\ 173 & \ 86 & 1 \\ 33 & \ 16 & 5 \\ 8 & \ 4 & 4 \end{array}$$

unde deducimus

$$\varphi(379, 206) = 19467 - 8858 + 1376 - 64 - 5356 + 3741 - 680 + 40 = 9666$$

quapropter 103 est residuum quadraticum numeri 379.

6.

Quum ad decidendam relationem numeri b ad a non opus sit, singulas partes aggregati $\varphi(a, b)$ computare, sed sufficiat novisse, quot inter eas sint impares, regula nostra ita quoque exhiberi potest:

Fiat ut supra $a = \beta b + c$, $b = \gamma c + d$, $c = \delta d + e$ etc., donec in serie numerorum a, b, c, d, e etc. ad unitatem perventum sit. Statuatur $\left[\frac{1}{2}a\right] = a'$, $\left[\frac{1}{2}b\right] = b'$, $\left[\frac{1}{2}c\right] = c'$ etc., sitque μ multitudo numerorum imparium in serie a', b', c' etc. eorum, quos immediate sequitur impar; sit porro ν multitudo numerorum imparium in serie β, γ, δ etc. eorum, quibus in serie b', c', d' etc. resp. respondet numerus formae $4n+1$ vel formae $4n+2$. His ita factis, erit b residuum quadraticum vel non-residuum ipsius a, prout $\mu + \nu$ est par vel impar, unico casu excepto, ubi simul est b par atque a vel formae $8n+3$ vel $8n+5$, pro quo regula opposita valet.

In exemplo nostro series a', b', c', d', e' duas successiones imparium sistit, unde $\mu = 2$; in serie b', γ', δ', ε', duo quidem impares adsunt, sed quibus in serie b', c', d', e' respondent numeri formae $4n+3$, unde $\nu = 0$. Fit itaque $\mu + \nu$ par, adeoque 103 residuum quadraticum numeri 379.

THEORIA
RESIDUORUM BIQUADRATICORUM

COMMENTATIO PRIMA

A U C T O R E

CAROLO FRIDERICO GAUSS

SOCIETATI REGIAE TRADITA 1825, APR. 5.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VI.
Gottingae MDCCCXXVII.

THEORIA RESIDUORUM BIQUADRATICORUM.

COMMENTATIO PRIMA.

1.

Theoria residuorum quadraticorum ad pauca theoremata fundamentalia reducitur, pulcherrimis Arithmeticae Sublimioris cimeliis adnumeranda, quae primo per inductionem facile detecta, ac dein multifariis modis ita demonstrata esse constat, ut nihil amplius desiderandum relictum sit.

Longe vero altioris indaginis est theoria residuorum cubicorum et biquadraticorum. Quam quum inde ab anno 1805 perscrutari coepissemus, praeter ea, quae quasi in limine sunt posita, nonnulla quidem theoremata specialia se obtulerunt, tum propter simplicitatem suam, tum propter demonstrationum difficultatem valde insignia: mox vero comperimus, principia Arithmeticae hactenus usitata ad theoriam generalem stabiliendam neutiquam sufficere, quin potius hanc necessario postulare, ut campus Arithmeticae Sublimioris infinities quasi promoveatur, quod quomodo intelligendum sit, in continuatione harum disquisitionum clarissime elucebit. Quamprimum hunc campum novum ingressi sumus, aditus ad cognitionem theorematum simplicissimorum totam theoriam exhaurientium per inductionem statim patuit: sed ipsorum demonstrationes tam profunde latuerunt, ut post multa demum tentamina irrita tandem in lucem protrahi potuerint.

Quum iam ad promulgationem harum lucubrationum accingamur, a theoria residuorum biquadraticorum initium faciemus, et quidem in hac prima commentatione

disquisitiones eas explicabimus, quas iam cis campum Arithmeticae ampliatum absolvere licuit, quae illuc viam quasi sternunt, simulque theoriae divisionis circuli quaedam nova incrementa adiungunt.

2.

Notionem residui biquadratici in *Disquisitionibus Arithmeticis* art. 115 introduximus: scilicet numerus integer a, positivus seu negativus, integri p residuum biquadraticum vocatur, si a secundum modulum p biquadrato congruus fieri potest, et perinde non-residuum biquadraticum, si talis congruentia non exstat. In omnibus disquisitionibus sequentibus, ubi contrarium expressis verbis non monetur, modulum p esse numerum primum (imparem positivum) supponemus, atque a per p non divisibilem, quum omnes casus reliqui ad hunc facillime reduci possint.

3.

Manifestum est, omne residuum biquadraticum numeri p eiusdem quoque residuum quadraticum esse, et proin omne non-residuum quadraticum etiam non-residuum biquadraticum. Hanc propositionem etiam convertere licet, quoties p est numerus primus formae $4n+3$. Nam si in hoc casu a est residuum quadraticum ipsius p, statuamus $a \equiv bb \pmod{p}$, ubi b vel residuum quadraticum ipsius p erit vel non-residuum: in casu priori statuemus $b \equiv cc$, unde $a \equiv c^4$, i.e. a erit residuum biquadraticum ipsius p; in casu posteriori $-b$ fiet residuum quadraticum ipsius p (quoniam -1 est non-residuum cuiusvis numeri primi formae $4n+3$), faciendoque $-b \equiv cc$, erit ut antea $a \equiv c^4$, atque a residuum biquadraticum ipsius p. Simul facile perspicietur, alias solutiones congruentiae $x^4 \equiv a \pmod{p}$, praeter has duas $x \equiv c$ et $x \equiv -c$ in hoc casu non dari. Quum hae propositiones obviae integram residuorum biquadraticorum theoriam pro modulis primis formae $4n+3$ exhauriant, tales modulos a disquisitione nostra omnino excludemus, sive hanc ad modulos primos formae $4n+1$ limitabimus.

4.

Existente itaque p numero primo formae $4n+1$, propositionem art. praec. convertere non licet: nempe exstare possunt residua quadratica, quae non sunt simul residua biquadratica, quod evenit, quoties residuum quadraticum congruum est quadrato non-residui quadratici. Statuendo enim $a \equiv bb$, existente b nonresiduo

quadratico ipsius p, si congruentiae $x^4 \equiv a$ satisfieri posset, per valorem $x \equiv c$, foret $c^4 \equiv bb$, sive productum $(cc-b)(cc+b)$ per p divisibile, unde p vel factorem $cc-b$ vel alterum $cc+b$ metiri deberet, i.e. vel $+b$ vel $-b$ foret residuum quadraticum ipsius p, et proin uterque (quoniam -1 est residuum quadraticum), contra hyp.

Omnes itaque numeri integri per p non divisibiles in tres classes distribui possent, quarum prima contineat residua biquadratica, secunda non-residua biquadratica ea, quae simul sunt residua quadratica, tertia non-residua quadratica. Manifesto sufficit, tali classificationi solos numeros 1, 2, $3 \ldots p-1$ subiicere, quorum semissis ad classem tertiam reduceretur, dum altera semissis inter classem primam et secundam distribueretur.

5.

Sed praestabit, quatuor classes stabilire, quarum indoles ita se habeat.

Sit A complexus omnium residuorum biquadraticorum ipsius p, inter 1 et $p-1$ (inclus.) sitorum, atque e non-residuum quadraticum ipsius p ad arbitrium electum. Sit porro B complexus residuorum minimorum positivorum e productis eA secundum modulum p oriundorum, et perinde C, D resp. complexus residuorum minimorum positivorum e productis eeA, e^3A secundum modulum p prodeuntium. His ita factis facile perspicitur, singulos numeros B inter se diversos fore, et perinde singulos C, nec non singulos D; cifram autem inter omnes hos numeros occurrere non posse. Porro patet, omnes numeros, in A et C contentos, esse residua quadratica ipsius p, omnes autem in B et D non-residua quadratica, ita ut certe complexus A, C nullum numerum cum complexu B vel D communem habere possint. Sed etiam neque A cum C, neque B cum D ullum numerum communem habere potest. Supponamus enim

I. numerum aliquem ex A, e.g. a etiam in C inveniri, ubi prodierit e producto eea' ipsi congruo, existente a' numero e complexu A. Statuatur $a \equiv \alpha^4$, $a' \equiv \alpha'^4$, accipiaturque integer Θ ita, ut fiat $\Theta\alpha' \equiv 1$. His ita factis erit $ee\alpha'^4 \equiv \alpha^4$, adeoque multiplicando per Θ^4,

$$ee \equiv \alpha^4\Theta^4$$

i.e. ee residuum biquadraticum, adeoque e residuum quadraticum, contra hyp.

II. Perinde supponendo, aliquem numerum complexibus B, D communem esse, atque e productis ea, e^3a' prodiisse, existentibus a, a' numeris e complexu A, e congruentia $ea \equiv e^3a'$ sequeretur $a \equiv eea'$, adeoque haberetur numerus, qui e producto eea' oriundus ad C simulque ad A pertineret, quod impossibile esse modo demonstravimus.

Porro facile demonstratur, *omnia* residua quadratica ipsius p, inter 1 et $p-1$ incl. sita, necessario vel in A vel in C, omniaque non-residua quadratica ipsius p inter illos limites necessario vel in B vel in D occurrere debere. Nam

I. Omne tale residuum quadraticum, quod simul est residuum biquadraticum, per hyp. in A invenitur.

II. Residuum quadraticum h (ipso p minus), quod simul est non-residuum biquadraticum, statuatur $\equiv gg$, ubi g erit non-residuum quadraticum. Accipiatur integer γ talis, ut fiat $e\gamma \equiv g$, eritque γ residuum quadraticum ipsius p, quod statuemus $\equiv kk$. Hinc erit

$$h \equiv gg \equiv ee\gamma\gamma \equiv eek^4$$

Quare quum residuum minimum ipsius k^4 inveniatur in A, numerus h, quippe qui ex illius producto per ee oritur, necessario in C contentus erit.

III. Designante h non-residuum quadraticum ipsius p inter limites 1 et $p-1$, eruatur inter eosdem limites numerus integer g talis, ut habeatur $eg \equiv h$. Erit itaque g residum quadraticum, et proin vel in A vel in C contentus: in casu priori h manifesto inter numeros B, in posteriori autem inter numeros D invenietur.

Ex his omnibus colligitur, cunctos numeros 1, 2, $3 \ldots p-1$ inter quatuor series A, B, C, D ita distribui, ut quivis illorum in una harum reperiatur, unde singulae series $\frac{1}{4}(p-1)$ numeros continere debent. In hac classificatione classes A et C quidem numeros suos essentialiter possident, sed distinctio inter classes B et D eatenus arbitraria est, quatenus ab electione numeri e pendet, qui ipse semper ad B referendus est; quapropter si eius loco alius e classe D adoptatur, classes B, D inter se permutabuntur.

6.

Quum -1 sit residuum quadraticum ipsius p, statuamus, $-1 \equiv ff \pmod{p}$, unde quatuor radices congruentiae $x^4 \equiv 1$ erunt 1, f, -1, $-f$. Quodsi itaque a est residuum biquadraticum ipsius p, puta $\equiv \alpha^4$, quatuor radices congruentiae

$x^4 \equiv a$ erunt α, $f\alpha$, $-\alpha$, $-f\alpha$, quas inter se incongruas esse facile perspicitur. Hinc patet, si colligantur residua minima positiva biquadratorum 1, 16, 81, $256 \ldots (p-1)^4$, quaterna semper aequalia fore, ita ut $\frac{1}{4}(p-1)$ residua biquadratica diversa habeantur complexum A formantia. Si residua minima biquadratorum usque ad $(\frac{1}{2}p-\frac{1}{2})^4$ tantum colliguntur, singula bis aderunt.

7.

Productum duorum residuorum biquadraticorum manifesto est residuum biquadraticum, sive e multiplicatione duorum numerorum classis A semper prodit productum, cuius residuum minimum positivum ad eandem classem pertinet. Perinde producta numeri ex B in numerum ex D, vel numeri ex C in numerum ex C, habebunt residua sua minima in A.

In B autem cadent residua productorum $A.B$ et $C.D$; in C residua productorum $A.C$, $B.B$ et $D.D$; denique in D residua productorum $A.D$ et $B.C$.

Demonstrationes tam obviae sunt, ut sufficiat, unam indicavisse. Sint e.g. c et d numeri ex C et D, atque $c \equiv eea$, $d \equiv e^3a'$, denotantibus a, a' numeros ex A. Tunc e^4aa' erit residuum biquadraticum, i.e. ipsius residuum minimum ad A referetur: quare quum productum cd fiat $\equiv e.e^4aa'$, illius residuum minimum in B contentum erit.

Simul facile iam diiudicari potest, ad quamnam classem referendum sit productum e pluribus factoribus. Scilicet tribuendo classi A, B, C, D resp. characterem 0, 1, 2, 3, character producti vel aggregato characterum singulorum factorum aequalis erit, vel eius residuo minimo secundum modulum 4.

8.

Operae pretium visum est, hasce propositiones elementares absque adminiculo theoriae residuorum potestatum evolvere, qua in auxilium vocata omnia adhuc multo facilius demonstrare licet.

Sit g radix primitiva pro modulo p, i.e. numerus talis, ut in serie potestatum g, gg, $g^3 \ldots$ nulla ante hanc g^{p-1} unitati secundum modulum p congrua evadat. Tunc residua minima positiva numerorum 1, g, gg, $g^3 \ldots g^{p-2}$ praeter ordinem cum his 1, 2, $3 \ldots p-1$ convenient, et in quatuor classes sequenti modo distribuentur:

ad	residua minima numerorum
A	$1,\ g^4, g^8,\ g^{12} \dots g^{p-5}$
B	$g,\ g^5, g^9,\ g^{13} \dots g^{p-4}$
C	$gg, g^6, g^{10}, g^{14} \dots g^{p-3}$
D	$g^3, g^7, g^{11}, g^{15} \dots g^{p-2}$

Hinc omnes propositiones praecedentes sponte demanant.

Ceterum sicuti hic numeri $1,\ 2,\ 3 \dots p-1$ in quatuor classes distributi sunt, quarum complexus per A, B, C, D designamus, ita *quemvis* integrum per p non divisibilem, ad normam ipsius residui minimi secundum modulum p, alicui harum classium adnumerare licebit.

9.

Denotabimus per f residuum minimum potestatis $g^{\frac{1}{4}(p-1)}$ secundum modulum p, unde quum fiat $ff \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ (*Disquis. Arithm.* art. 62), patet, characterem f hic idem significare quod in art. 6. Potestas $g^{\frac{1}{4}\lambda(p-1)}$ itaque, denotante λ integrum positivum, congrua erit secundum modulum p numero 1, f, -1, $-f$, prout λ formae $4m$, $4m+1$, $4m+2$, $4m+3$ resp., sive prout residuum minimum ipsius g^λ in A, B, C, D resp. reperitur. Hinc nanciscimur criterium persimplex ad diiudicandum, ad quam classem numerus datus h per p non divisibilis referendus sit; pertinebit scilicet h ad A, B, C vel D, prout potestas $h^{\frac{1}{4}(p-1)}$ secundum modulum p numero 1, f, -1 vel $-f$ congrua evadit.

Tamquam corollarium hinc sequitur, -1 semper ad classem A referri, quoties p sit formae $8n+1$, ad classem C vero, quoties p sit formae $8n+5$. Demonstratio huius theorematis a theoria residuorum potestatum independens ex iis, quae in *Disquisitionibus Arithmeticis* art. 115, III docuimus, facile adornari potest.

10.

Quum *omnes* radices primitivae pro modulo p prodeant e residuis potestatum g^λ, accipiendo pro λ omnes numeros ad $p-1$ primos, facile perspicitur, illas inter complexus B et D aequaliter dispertitas fore, basi g semper in B contenta. Quodsi loco numeri g radix alia primitiva e complexu B pro basi accipitur, classificatio eadem manebit; si vero radix primitiva e complexu D tamquam basis adoptatur, classes B et D inter se permutabuntur.

Si classificatio criterio in art. praec. prolato superstruitur, discrimen inter classes B et D inde pendebit, utram radicem congruentiae $xx \equiv -1 \pmod{p}$ pro numero characteristico f adoptemus.

11.

Quo facilius disquisitiones subtiliores, quas iam aggressuri sumus, per exempla illustrari possint, constructionem classium pro omnibus modulis infra 100 hic apponimus. Radicem primitivam pro singulis minimam adoptavimus.

$$p = 5$$
$$g = 2, f = 2$$

A	1
B	2
C	4
D	3

$$p = 13$$
$$g = 2, f = 8$$

A	$1, \quad 3, \quad 9$
B	$2, \quad 5, \quad 6$
C	$4, \ 10, \ 12$
D	$7, \quad 8, \ 11$

$$p = 17$$
$$g = 2, f = 12$$

A	$1, \ 4, \ 13, \ 16$
B	$3, \ 5, \ 12, \ 14$
C	$2, \ 8, \quad 9, \ 15$
D	$6, \ 7, \ 10, \ 11$

$$p = 29$$
$$g = 2, f = 12$$

A	$1, \quad 7, \ 16, \ 20, \ 23, \ 24, \ 25$
B	$2, \quad 3, \ 11, \ 14, \ 17, \ 19, \ 21$
C	$4, \quad 5, \quad 6, \quad 9, \ 13, \ 22, \ 28$
D	$8, \ 10, \ 12, \ 15, \ 18, \ 26, \ 27$

$p = 37$

$g = 2, f = 31$

A	$1,\ \ 7,\ \ 9,\ 10,\ 12,\ 16,\ 26,\ 33,\ 34$
B	$2,\ 14,\ 15,\ 18,\ 20,\ 24,\ 29,\ 31,\ 32$
C	$3,\ \ 4,\ 11,\ 21,\ 25,\ 27,\ 28,\ 30,\ 36$
D	$5,\ \ 6,\ \ 8,\ 13,\ 17,\ 19,\ 22,\ 23,\ 35$

$p = 41$

$g = 6, f = 32$

A	$1,\ \ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40$
B	$6,\ 14,\ 15,\ 17,\ 19,\ 22,\ 24,\ 26,\ 27,\ 35$
C	$2,\ \ 5,\ \ 8,\ \ 9,\ 20,\ 21,\ 32,\ 33,\ 36,\ 39$
D	$3,\ \ 7,\ 11,\ 12,\ 13,\ 28,\ 29,\ 30,\ 34,\ 38$

$p = 53$

$g = 2, f = 30$

A	$1,\ 10,\ 13,\ 15,\ 16,\ 24,\ 28,\ 36,\ 42,\ 44,\ 46,\ 47,\ 49$
B	$2,\ \ 3,\ 19,\ 20,\ 26,\ 30,\ 31,\ 32,\ 35,\ 39,\ 41,\ 45,\ 48$
C	$4,\ \ 6,\ \ 7,\ \ 9,\ 11,\ 17,\ 25,\ 29,\ 37,\ 38,\ 40,\ 43,\ 52$
D	$5,\ \ 8,\ 12,\ 14,\ 18,\ 21,\ 22,\ 23,\ 27,\ 33,\ 34,\ 50,\ 51$

$p = 61$

$g = 2, f = 11$

A	$1,\ 9,\ 12,\ 13,\ 15,\ 16,\ 20,\ 22,\ 25,\ 34,\ 42,\ 47,\ 56,\ 57,\ 58$
B	$2,\ 7,\ 18,\ 23,\ 24,\ 26,\ 30,\ 32,\ 33,\ 40,\ 44,\ 50,\ 51,\ 53,\ 55$
C	$3,\ 4,\ \ 5,\ 14,\ 19,\ 27,\ 36,\ 39,\ 41,\ 45,\ 46,\ 48,\ 49,\ 52,\ 60$
D	$6,\ 8,\ 10,\ 11,\ 17,\ 21,\ 28,\ 29,\ 31,\ 35,\ 37,\ 38,\ 43,\ 54,\ 59$

$p = 73$

$g = 5, f = 27$

A	$1,\ \ 2,\ \ 4,\ \ 8,\ \ 9,\ 16,\ 18,\ 32,\ 36,\ 37,\ 41,\ 55,\ 57,\ 64,\ 65,\ 69,\ 71,\ 72$
B	$5,\ \ 7,\ 10,\ 14,\ 17,\ 20,\ 28,\ 33,\ 34,\ 39,\ 40,\ 45,\ 53,\ 56,\ 59,\ 63,\ 66,\ 68$
C	$3,\ \ 6,\ 12,\ 19,\ 23,\ 24,\ 25,\ 27,\ 35,\ 38,\ 46,\ 48,\ 49,\ 50,\ 54,\ 61,\ 67,\ 70$
D	$11,\ 13,\ 15,\ 21,\ 22,\ 26,\ 29,\ 30,\ 31,\ 42,\ 43,\ 44,\ 47,\ 51,\ 52,\ 58,\ 60,\ 62$

$p = 89$

$g = 3, f = 34$

A	1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44, 45, 50, 57, 64, 67, 73, 78, 81, 85, 87, 88
B	3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46, 48, 56, 61, 65, 66, 75, 77, 82 83, 86
C	5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47, 49, 53, 55, 68, 69, 71, 72, 79 80, 84
D	13, 15, 19, 26, 27, 29, 30, 31, 35, 37, 38, 51, 52, 54, 58, 59, 60, 62, 63, 70 74, 76

$p = 97$

$g = 5, f = 22$

A	1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47, 50, 54, 61, 62, 64, 73, 75, 81, 88, 91, 93, 96
B	5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45, 52, 56, 67, 68, 74, 76, 77, 78 80, 83, 84, 92
C	2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48, 49, 53, 65, 66, 70, 72, 79, 85 86, 89, 94, 95
D	7, 10, 15, 26, 28, 34, 37, 38, 39, 40, 42, 46, 51, 55, 57, 58, 59, 60, 63, 69 71, 82, 87, 90

12.

Quum numerus 2 sit residuum quadraticum omnium numerorum primorum formae $8n+1$, non-residuum vero omnium formae $8n+5$, pro modulis primis formae prioris 2 in classe A vel C, pro modulis formae posterioris in classe B vel D invenietur. Quum discrimen inter classes B et D non sit essentiale, quippe quod tantummodo ab electione numeri f pendet, modulos formae $8n+5$ aliquantisper seponemus. Modulos formae $8n+1$ autem *inductioni* subiiciendo, invenimus 2 pertinere ad A pro $p = 73$, 89, 113, 233, 257, 281, 337, 353 etc.; contra 2 pertinere ad C pro $p = 17$, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457 etc.

Ceterum quum pro modulo primo formae $8n+1$ numerus -1 sit residuum biquadraticum, patet, -2 semper cum $+2$ ad eandem classem referendum esse.

13.

Si exempla art. praec. inter se comparantur, primo saltem aspectu criterium nullum simplex se offerre videtur, per quod modulos priores a posterioribus dignoscere liceret. Nihilominus *duo* huiusmodi criteria dantur, elegantia et simplicitate perinsignia, ad quorum alterum considerationes sequentes viam sternent.

Modulus p, tamquam numerus primus formae $8n+1$, reduci poterit, et quidem unico tantum modo, sub formam $aa+2bb$ (*Disquiss. Arithm.* art. 182, II); radices a, b positive accipi supponemus. Manifesto a impar erit, b vero par; statuemus autem $b = 2^\lambda c$, ita ut c sit impar. Iam observamus

I. quum habeatur $p \equiv aa \pmod{c}$ ipsum p esse residuum quadraticum ipsius c, et proin etiam singulorum factorum primorum, in quos c resolvitur: vicissim itaque, per theorema fundamentale, singuli hi factores primi erunt residua quadratica ipsius p, et proin etiam illorum productum c erit residuum quadraticum ipsius p. Quod quum etiam de numero 2 valeat, patet, b esse residuum quadraticum ipsius p, et proin bb, nec non $-bb$, residuum biquadraticum.

II. Hinc $-2bb$ ad eandem classem referri debet, in qua invenitur numerus 2; quare quum $aa \equiv -2bb$, manifestum est, 2 vel in classe A, vel in classe C inveniri, prout a sit vel residuum quadraticum ipsius p, vel non-residuum quadraticum.

III. Iam supponamus, a in factores suos primos resolutum esse, e quibus ii, qui sunt vel formae $8m+1$ vel $8m+7$, denotentur per α, α', α'' etc., ii vero, qui sunt vel formae $8m+3$ vel $8m+5$, per β, β', β'' etc.: posteriorum multitudo sit $= \mu$. Quoniam $p \equiv 2bb \pmod{a}$, erit p residuum quadraticum eorum factorum primorum ipsius a, quorum residuum quadraticum est 2, i.e. factorum α, α', α'' etc.; non-residuum quadraticum vero factorum eorum, quorum non-residuum quadraticum est 2, i.e. factorum β, β', β'' etc. Quocirca, vice versa, per theorema fundamentale, singuli α', α', α'' etc. erunt residua quadratica ipsius p, singuli β, β', β'' etc. autem non-residua quadratica. Ex his itaque concluditur, productum a fore residuum quadraticum ipsius p, vel non-residuum, prout μ par sit vel impar.

IV. Sed facile confirmatur, productum omnium α, α', α'' etc. fieri formae $8m+1$ vel $8m+7$, idemque valere de producto omnium β, β', β'' etc., si horum multitudo fuerit par, ita ut in hoc casu etiam productum a necessario fieri debeat formae $8m+1$ vel $8m+7$; contra productum omnium β, β', β'' etc., quoties ipsorum

multitudo impar sit, fieri formae $8m+3$ vel $8m+5$, idemque adeo in hoc casu valere de producto a.

Ex his omnibus itaque colligitur theorema elegans:

Quoties a est formae $8m+1$ vel $8m+7$, numerus 2 in complexu A contentus erit; quoties vero a est formae $8m+3$ vel $8m+5$, numerus 2 in complexu C invenietur.

Quod confirmatur per exempla in art. praec. enumerata; priores enim moduli ita discerpuntur: $73 = 1 + 2.36$, $89 = 81 + 2.4$, $113 = 81 + 2.16$, $233 = 225 + 2.4$, $257 = 225 + 2.16$, $281 = 81 + 2.100$, $337 = 49 + 2.144$, $353 = 225 + 2.64$; posteriores vero ita: $17 = 9 + 2.4$, $41 = 9 + 2.16$. $97 = 25 + 2.36$, $137 = 9 + 2.64$, $193 = 121 + 2.36$, $241 = 169 + 2.36$, $313 = 25 + 2.144$, $401 = 9 + 2.196$, $409 = 121 + 2.144$, $433 = 361 + 2.36$, $449 = 441 + 2.4$, $457 = 169 + 2.144$.

14.

Quum discerptio numeri p in quadratum simplex et duplex nexum tam insignem cum classificatione numeri 2 prodiderit, operae pretium esse videtur tentare, num discerptio in duo quadrata, cui numerum p aeque obnoxium esse constat, similem forte successum suppeditet. Ecce itaque discerptiones numerorum p, pro quibus 2 pertinet ad classem

A	C
$9+64$	$1+16$
$25+64$	$25+16$
$49+64$	$81+16$
$169+64$	$121+16$
$1+256$	$49+144$
$25+256$	$225+16$
$81+256$	$169+144$
$289+64$	$1+400$
	$9+400$
	$289+144$
	$49+400$
	$441+16$

Ante omnia observamus, duorum quadratorum, in quae p discerpitur, alterum impar esse debere, quod statuemus $= aa$, alterum par, quod statuemus $= bb$. Quoniam aa fit formae $8n+1$, patet, valoribus impariter paribus ipsius b respondere valores ipsius p formae $8n+5$, ab inductione nostra hic exclusos, quippe qui numerum 2 in classe B vel D haberent. Pro valoribus autem ipsius p, qui sunt formae $8n+1, b$ esse debet pariter par, et si inductioni, quam schema allatum ob oculos sistit, fidem habere licet, numerus 2 ad classem A referendus erit pro omnibus modulis, pro quibus b est formae $8n$, ad classem C vero pro omnibus modulis, pro quibus b est formae $8n+4$. Sed hoc theorema longe altioris indaginis est, quam id, quod in art. praec. eruimus, demonstrationique plures disquisitiones praeliminares sunt praemittendae, ordinem, quo numeri complexuum A, B, C, D se invicem sequuntur, spectantes.

15.

Designemus multitudinem numerorum e complexu A, quos immediate sequitur numerus e complexu A, B, C, D resp., per (00), (01), (02), (03); perinde multitudinem numerorum e complexu B, quos sequitur numerus e complexu A, B, C, D resp. per (10), (11), (12), (13); similiterque sint in complexu C resp. (20), (21), (22), (23) numeri, in complexu D vero (30), (31), (32), (33) numeri, quos sequitur numerus e complexu A, B, C, D. Proponimus nobis, has sedecim multitudines a priori determinare. Quo commodius lectores ratiocinia generalia cum exemplis comparare possint, valores numericos terminorum schematis (S)

(00), (01), (02), (03)
(10), (11), (12), (13)
(20), (21), (22), (23)
(30), (31), (32), (33)

pro singulis modulis, pro quibus classificationes in art. 11 tradidimus, hic adscribere visum est.

$p=5$	$p=13$	$p=17$	$p=29$
0, 1, 0, 0	0, 1, 2, 0	0, 2, 1, 0	2, 3, 0, 2
0, 0, 0, 1	1, 1, 0, 1	2, 0, 1, 1	1, 1, 2, 3
0, 0, 0, 0	0, 1, 0, 1	1, 1, 1, 1	2, 1, 2, 1
0, 0, 1, 0	1, 0, 1, 1	0, 1, 1, 2	1, 2, 3, 1

$p=37$	$p=41$	$p=53$	$p=61$
2, 1, 2, 4	0, 4, 3, 2	2, 3, 6, 2	4, 3, 2, 6
2, 2, 4, 1	4, 2, 2, 2	4, 4, 2, 3	3, 3, 6, 3
2, 2, 2, 2	3, 2, 3, 2	2, 4, 2, 4	4, 3, 4, 3
2, 4, 1, 2	2, 2, 2, 4	4, 2, 3, 4	3, 6, 3, 3

$p=73$	$p=89$	$p=97$
5, 6, 4, 2	3, 8, 6, 4	2, 6, 7, 8
6, 2, 5, 5	8, 4, 5, 5	6, 8, 5, 5
4, 5, 4, 5	6, 5, 6, 5	7, 5, 7, 5
2, 5, 5, 6	4, 5, 5, 8	8, 5, 5, 6

Quum moduli formae $8n+1$ et $8n+5$ diverso modo se habeant, utrosque seorsim tractare oportet: a prioribus initium faciemus.

16.

Character (00) indicat, quot modis diversis aequationi $\alpha+1=\alpha'$ satisfieri possit, denotantibus α, α' indefinite numeros e complexu A. Quum pro modulo formae $8n+1$, qualem hic subintelligimus, α' et $p-\alpha'$ ad eundem complexum pertineant, concinnius dicemus, (00) exprimere multitudinem modorum diversorum, aequationi $1+\alpha+\alpha'=p$, satisfaciendi: manifesto huius aequationis vice etiam congruentia $1+\alpha+\alpha'\equiv 0 \pmod{p}$ fungi potest.

Perinde

(01) indicat multitudinem solutionum congruentiae $1+\alpha+\beta\equiv 0 \pmod{p}$
(02) multitudinem solutionum congruentiae $1+\alpha+\gamma\equiv 0$
(03) multitudinem solutionum congruentiae $1+\alpha+\delta\equiv 0$
(11) multitudinem solutionum congruentiae $1+\beta+\beta'\equiv 0$ etc.

exprimendo indefinite per β et β' numeros e complexu B, per γ numeros e complexu C, per δ numeros e complexu D. Hinc statim colligimus sex aequationes sequentes:

$$(01)=(10),\ (02)=(20),\ (03)=(30),\ (12)=(21),\ (13)=(31),\ (23)=(32)$$

E quavis solutione data congruentiae $1+\alpha+\beta\equiv 0$ demanat solutio congruentiae $1+\delta+\delta'\equiv 0$, accipiendo pro δ numerum inter limites $1\ldots p-1$eum qui reddit $\beta\delta\equiv 1$

(qui manifesto erit e complexu D), et pro δ' residuum minimum positivum producti $\alpha\delta$ (quod itidem erit e complexu D); perinde patet regressus a solutione data congruentiae $1+\delta+\delta' \equiv 0$ ad solutionem congruentiae $1+\alpha+\beta \equiv 0$, si β accipitur ita, ut fiat $\beta\delta \equiv 1$, simulque statuitur $\alpha \equiv \beta\delta'$. Hinc concludimus, utramque congruentiam aequali solutionum multitudine gaudere, sive esse $(01) = (33)$.

Simili modo e congruentia $1+\alpha+\gamma \equiv 0$ deducimus $\gamma'+\gamma''+1 \equiv 0$, si γ' accipitur e complexu C ita ut fiat $\gamma\gamma' \equiv 1$, atque γ'' ex eodem complexu congruus producto $\alpha\gamma'$. Unde facile colligimus, has duas congruentias aequalem solutionum multitudinem admittere, sive esse $(02) = (22)$.

Perinde e congruentia $1+\alpha+\delta \equiv 0$ deducimus $\beta+\beta'+1 \equiv 0$, accipiendo β, β' ita ut fiat $\beta\delta \equiv 1, \beta\alpha \equiv \beta'$, eritque adeo $(03) = (11)$.

Denique e congruentia $1+\beta+\gamma \equiv 0$ simili modo tum congruentiam $\delta+1+\beta' \equiv 0$, tum hanc $\gamma'+\delta'+1 \equiv 0$ derivamus, atque hinc concludimus $(12) = (13) = (23)$.

Nacti sumus itaque, inter sedecim incognitas nostras, undecim aequationes, ita ut illae ad quinque reducantur, schemaque S ita exhiberi possit:

$$\begin{array}{cccc} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i \end{array}$$

Facile vero tres novae aequationes conditionales adiiciuntur. Quum enim quemvis numerum complexus A, excepto ultimo $p-1$, sequi debeat numerus ex aliquo complexuum A, B, C vel D, habebimus

$$(00)+(01)+(02)+(03) = 2n-1$$

et perinde

$$(10)+(11)+(12)+(13) = 2n$$
$$(20)+(21)+(22)+(23) = 2n$$
$$(30)+(31)+(32)+(33) = 2n$$

In signis modo introductis tres primae aequationes suppeditant:

$$h+i+k+l = 2n-1$$
$$i+l+2m = 2n$$
$$k+m = n$$

Quarta cum secunda fit identica. Adiumento harum aequationum tres incognitarum

eliminare licet, quo pacto omnes sedecim iam ad duas reductae sunt.

17.

Ut vero determinationem completam nanciscamur, investigare conveniet multitudinem solutionum congruentiae

$$1+\alpha+\beta+\gamma \equiv 0 \pmod{p}$$

designantibus α, β, γ indefinite numeros e complexibus A, B, C. Manifesto valor $\alpha = p-1$ non est admissibilis, quum fieri nequeat $\beta+\gamma \equiv 0$: substituendo itaque pro α deinceps valores reliquos, prodibunt h, i, k, l valores ipsius $1+\alpha$ ad A, B, C, D resp. pertinentes. Pro quovis autem valore *dato* ipsius $1+\alpha$ ad A pertinente, puta pro $1+\alpha = \alpha^0$, congruentia $\alpha^0+\beta+\gamma \equiv 0$ totidem solutiones admittet, quot congruentia $1+\beta'+\gamma' \equiv 0$ (statuendo scilicet $\beta \equiv \alpha^0\beta'$, $\gamma \equiv \alpha^0\gamma'$), i.e. solutiones $(12) = m$. Perinde pro quovis valore dato ipsius $1+\alpha$ ad B pertinente, puta pro $1+\alpha = \beta^0$, congruentia $\beta^0+\beta+\gamma \equiv 0$ totidem solutiones habebit, quot haec $1+\alpha'+\beta' \equiv 0$ (scilicet statuendo $\beta \equiv \beta^0\alpha'$, $\gamma \equiv \beta^0\beta'$), i.e. solutiones $(01) = i$. Similiter pro quolibet valore dato ipsius $1+\alpha$ ad C pertinente, puta pro $1+\alpha = \gamma^0$, congruentia $\gamma^0+\beta+\gamma \equiv 0$ totidem modis diversis solvi poterit, quot haec $1+\delta+\alpha' \equiv 0$ (nempe statuendo $\beta \equiv \gamma^0\delta, \gamma \equiv \gamma^0\alpha'$), i.e. solutionum multitudo erit $(03) = l$. Denique pro quovis valore dato ipsius $1+\alpha$ ad D pertinente, puta pro $1+\alpha = \delta^0$, congruentia $\delta^0+\beta+\gamma \equiv 0$ totidem solutiones habebit, quot haec $1+\gamma'+\delta' \equiv 0$ (statuendo $\beta \equiv \delta^0\gamma'$, $\gamma \equiv \delta^0\delta'$), i.e. $(23) = m$ solutiones. Omnibus itaque collectis, patet, congruentiam $1+\alpha+\beta+\gamma \equiv 0$ admittere

$$hm+ii+kl+lm$$

solutiones diversas.

Prorsus vero simili modo eruimus, si pro β singuli deinceps numeri complexus B substituantur, summam $1+\beta$ obtinere resp. (10), (11), (12), (13) sive i, l, m, m valores ad A, B, C, D pertinentes, et pro quovis valore dato ipsius $1+\beta$ ad hos complexus pertinente, congruentiam $1+\beta+\alpha+\gamma \equiv 0$ resp. (02), (31), (20), (13) sive k, m, k, m solutiones diversas admittere, ita ut multitudo omnium solutionum fiat

$$= ik + lm + km + mm$$

Ad eundem valorem perducimur, si evolutionem considerationi valorum summae $1+\gamma$ superstruimus.

18.

Ex hac duplici eiusdem multitudinis expressione nanciscimur aequationem:

$$0 = hm + ii + kl - ik - km - mm$$

atque hinc, eliminando h adiumento aequationis $h = 2m - k - 1$,

$$0 = (k-m)^2 + ii + kl - ik - kk - m$$

Sed duae aequationes ultimae art. 16 suppeditant $k = \frac{1}{2}(l+i)$, quo valore substituto $ii + kl - ik - kk$ transit in $\frac{1}{4}(l-i)^2$, adeoque aequatio praecedens, per 4 multiplicata, in hanc

$$0 = 4(k-m)^2 + (l-i)^2 - 4m$$

Hinc, quoniam $4m = 2(k+m) - 2(k-m) = 2n - 2(k-m)$, sequitur

$$2n = 4(k-m)^2 + 2(k-m) + (l-i)^2$$

sive

$$8n + 1 = (4(k-m)+1)^2 + 4(l-i)^2$$

Statuendo itaque

$$4(k-m) + 1 = a, \quad 2l - 2i = b$$

habebimus

$$p = aa + bb$$

Sed constat, p unico tantum modo in duo quadrata discerpi posse, quorum alterum impar accipi debet pro aa, alterum par pro bb, ita ut aa, bb sint numeri ex asse determinati. Sed etiam a ipse erit numerus prorsus determinatus; radix enim quadrati positive accipi debet, vel negative, prout radix positiva est formae $4M+1$ vel $4M+3$. De determinatione signi ipsius b mox loquemur.

Iam combinatis his novis aequationibus cum tribus ultimis art. 16, quinque numeri h, i, k, l, m per a, b et n penitus determinantur sequenti modo:

$$8h = 4n - 3a - 5$$
$$8i = 4n + a - 2b - 1$$
$$8k = 4n + a - 1$$
$$8l = 4n + a + 2b - 1$$
$$8m = 4n - a + 1$$

Si loco ipsius n modulum p introducere malumus, schema S, singulis terminis ad evitandas fractiones per 16 multiplicatis, ita se habet:

$$\left.\begin{array}{|c|c|c|c|}
p-6a-11 & p+2a-4b-3 & p+2a-3 & p+2a+4b-3 \\
p+2a-4b-3 & p+2a+4b-3 & p-2a+1 & p-2a+1 \\
p+2a-3 & p-2a+1 & p+2a-3 & p-2a+1 \\
p+2a+4b-3 & p-2a+1 & p-2a+1 & p+2a-4b-3
\end{array}\right.'\ ]$$

19.

Superest, ut signum ipsi b tribuendum assignare doceamus. Iam supra, art. 10, monuimus, distinctionem inter complexus B et D, per se non essentialem, ab electione numeri f pendere, pro quo alterutra radix congruentiae $xx \equiv -1$ accipi debet, illasque inter se permutari, si loco alterius radicis altera adoptetur. Iam quum inspectio schematis modo allati doceat, similem permutationem cum mutatione signi ipsius b cohaerere, praevidere licet, nexum inter signum ipsius b atque numerum f exstare debere. Quem ut cognoscamus, ante omnia observamus, si, denotante μ integrum non negativum, pro z accipiantur omnes numeri $1, 2, 3 \ldots p-1$, fieri secundum modulum p, vel $\Sigma z^\mu \equiv 0$, vel $\Sigma z^\mu \equiv -1$, prout μ vel non-divisibilis sit per $p-1$, vel divisibilis. Pars posterior theorematis inde patet, quod pro valore ipsius μ per $p-1$ divisibili, habetur $z^\mu \equiv 1$: partem priorem vero ita demonstramus. Denotante g radicem primitivam, omnes z convenient cum residuis minimis omnium g^y, accipiendo pro y omnes numeros $0, 1, 2, 3 \ldots p-2$, eritque adeo $\Sigma z^\mu \equiv \Sigma g^{\mu y}$. Sed fit

$$\Sigma g^{\mu y} = \tfrac{g^{\mu(p-1)}-1}{g^\mu - 1}, \text{ adeoque } (g^\mu - 1)\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0$$

Hinc vero sequitur, quoniam pro valore ipsius μ per $p-1$ non-divisibili g^μ ipsi 1 congruus sive $g^\mu - 1$ per p divisibilis esse nequit, $\Sigma z^\mu \equiv 0$. Q. E. D.

Iam si potestas $(z^4+1)^{\frac{1}{4}(p-1)}$ secundum theorema binomiale evolvitur, per lemma praec. fiet

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \pmod{p}$$

Sed residua minima omnium z^4 exhibent omnes numeros A, quovis quater occurrente; habebimus itaque inter residua minima ipsius z^4+1

$$4(00) \text{ ad } A$$
$$4(01) \text{ ad } B$$
$$4(02) \text{ ad } C$$
$$4(03) \text{ ad } D$$

pertinentia, quatuorque erunt $=0$ (puta pro $z^4 \equiv p-1$). Hinc, considerando criteria complexuum A, B, C, D, deducimus

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv 4(00)+4f(01)-4(02)-4f(03)$$

adeoque

$$-2 \equiv 4(00)+4f(01)-4(02)-4f(03)$$

sive substitutis pro (00), (01) etc. valoribus in art. praec inventis,

$$-2 \equiv -2a-2-2bf$$

Hinc itaque colligimus, semper fieri debere $a+bf \equiv 0$, sive, multiplicando per f,

$$b \equiv af$$

quae congruentia determinationi signi ipsius b, si numerus f iam electus est, vel determinationi numeri f, si signum ipsius b aliunde praescribitur, inservit.

20.

Postquam problema nostrum pro modulis formae $8n+1$ complete solvimus, progredimur ad casum alterum, ubi p est formae $8n+5$: quem eo brevius absolvere licebit, quod omnia ratiocinia parum a praecedentibus differunt.

Quum pro tali modulo -1 ad classem C pertineat, complementa numerorum complexuum A, B, C, D ad summam p, in classibus C, D, A, B resp. contenta erunt. Hinc facile colligitur

signum	denotare multitudinem solutionum congruentiae
(00)	$1+\alpha+\gamma\equiv 0$
(01)	$1+\alpha+\delta\equiv 0$
(02)	$1+\alpha+\alpha'\equiv 0$
(03)	$1+\alpha+\beta\equiv 0$
(10)	$1+\beta+\gamma\equiv 0$
(11)	$1+\beta+\delta\equiv 0$
(12)	$1+\beta+\alpha\equiv 0$
(13)	$1+\beta+\beta'\equiv 0$
(20)	$1+\gamma+\gamma'\equiv 0$
(21)	$1+\gamma+\delta\equiv 0$
(22)	$1+\gamma+\alpha\equiv 0$
(23)	$1+\gamma+\beta\equiv 0$
(30)	$1+\delta+\gamma\equiv 0$
(31)	$1+\delta+\delta'\equiv 0$
(32)	$1+\delta+\alpha\equiv 0$
(33)	$1+\delta+\beta\equiv 0$

unde statim habentur sex aequationes:

$$(00)=(22),\quad (01)=(32),\quad (03)=(12),\quad (10)=(23),\quad (11)=(33),\quad (21)=(30)$$

Multiplicando congruentiam $1+\alpha+\gamma\equiv 0$ per numerum γ' e complexu C ita electum, ut fiat $\gamma\gamma'\equiv 1$, accipiendoque pro γ'' residuum minimum producti $\alpha\gamma'$, quod manifesto quoque complexui C adnumerandum erit, prodit $\gamma'+\gamma''+1\equiv 0$, unde colligimus $(00)=(20)$.

Prorsus simili modo habentur aequationes $(01)=(13)$, $(03)=(31)$, $(10)=(11)=(21)$.

Adiumento harum undecim aequationum sedecim incognitas nostras ad quinque reducere, schemaque S ita exhibere possumus:

$$\begin{array}{cccc} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m \end{array}$$

Porro habemus aequationes

$$(00)+(01)+(02)+(03)=2n+1$$
$$(10)+(11)+(12)+(13)=2n+1$$
$$(20)+(21)+(22)+(23)=2n$$
$$(30)+(31)+(32)+(33)=2n+1$$

sive, adhibendo signa modo introducta, has tres (I):

$$h+i+k+l=2n+1$$
$$2m+i+l=2n+1$$
$$h+m=n$$

quarum itaque adiumento incognitas nostras iam ad duas reducere licet.

Aequationes reliquas e consideratione multitudinis solutionum congruentiae $1+\alpha+\beta+\gamma \equiv 0$ derivabimus (per α, β, γ, etiam hic indefinite numeros e complexibus A, B, C resp. denotantes). Scilicet perpendendo *primo*, $1+\alpha$ praebere h, i, k, l numeros resp. ad A, B, C, D pertinentes, et pro quovis valore dato ipsius α in his quatuor casibus resp. haberi solutiones m, l, i, m, multitudo omnium solutionum erit

$$= hm+il+ik+lm$$

Secundo quum $1+\beta$ exhibeat m, m, l, i numeros ad A, B, C, D pertinentes, et pro quovis valore *dato* ipsius β in his quatuor casibus exstent solutiones h, m, h, m, multitudo omnium solutionum erit

$$= hm+mm+hl+im$$

unde derivamus aequationem

$$0 = mm+hl+im-il-ik-lm$$

quae adiumento aequationis $k=2m-h$, ex (I) petitae, transit in hanc:

$$0 = mm+hl+hi-il-im-lm$$

Iam ex aequationibus I habemus etiam $l+i=1+2h$, unde

$$2i = 1+2h+(i-l)$$
$$2l = 1+2h-(i-l)$$

Quibus valoribus in aequatione praecedente substitutis, prodit:

$$0 = 4mm - 4m - 1 - 8hm + 4hh + (i-l)^2$$

Quodsi tandem pro $4m$ hic substituimus $2(h+m)-2(h-m)$ sive, propter aequationem ultimam in I, $2n-2(h-m)$, obtinemus:

$$0 = 4(h-m)^2 - 2n + 2(h-m) - 1 + (i-l)^2$$

adeoque

$$8n+5 = (4(h-m)+1)^2 + 4(i-l)^2$$

Statuendo itaque

$$4(h-m)+1 = a, \quad 2i-2l = b$$

fiet

$$p = aa + bb$$

Iam quum in hoc quoque casu p unico tantum modo in duo quadrata, par alterum, alterum impar, discerpi possit, aa et bb erunt numeri prorsus determinati; manifesto enim aa quadrato impari, bb pari aequalis statui debet. Praeterea *signum* ipsius a ita erit stabiliendum, ut fiat $a \equiv 1 \pmod 4$, signumque ipsius b ita, ut habeatur $b \equiv af \pmod p$, uti per ratiocinia iis, quibus in art. praec. usi sumus, prorsus similia facile demonstratur.

His praemissis quinque numeri h, i, k, l, m per a, b et n ita determinantur:

$$8h = 4n + a - 1$$
$$8i = 4n + a + 2b + 3$$
$$8k = 4n - 3a + 3$$
$$8l = 4n + a - 2b + 3$$
$$8m = 4n - a + 1$$

aut si expressiones per p praeferimus, termini schematis S per 16 multiplicati ita se habebunt:

$p+2a-7$	$p+2a+4b+1$	$p-6a+1$	$p+2a-4b+1$
$p-2a-3$	$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$
$p+2a-7$	$p-2a-3$	$p+2a-7$	$p-2a-3$
$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$	$p-2a-3$

21

Postquam problema nostrum solvimus, ad disquisitionem principalem revertimur, determinationem completam complexus, ad quem numerus 2 pertinet, iam aggressuri.

I. Quoties p est formae $8n+1$, iam constat, numerum 2 vel in complexu A vel in complexu C inveniri. In casu priori facile perspicitur, etiam numeros $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ ad A pertinere, in posteriori vero ad C. Iam perpendamus, si α et $\alpha+1$ sint numeri contigui complexus A, etiam $p-\alpha-1$, $p-\alpha$ tales numeros esse, sive, quod idem est, numeros complexus A tales, quos sequatur numerus ex eodem complexu, binos semper associatos esse, (α et $p-1-\alpha$). Talium itaque numerorum multitudo, (00), semper erit par, nisi quis exstat sibi ipse associatus, i.e. nisi $\frac{1}{2}(p-1)$ ad A pertinet, in quo casu multitudo illa impar erit. Hinc colligimus, (00) imparem esse, quoties 2 ad complexum A, parem vero, quoties 2 ad C pertineat. Sed habemus

$$16(00) = aa + bb - 6a - 11$$

sive statuendo $a = 4q+1$, $b = 4r$ (v. art. 14),

$$(00) = qq - q + rr - 1$$

Quoniam igitur $qq-q$ manifesto semper par est, (00) impar erit vel par, prout r par est vel impar, adeoque 2 vel ad A vel ad C pertinebit, prout b est vel formae $8m$ vel formae $8m+4$. Quod est ipsum theorema, in art. 14 per inductionem inventum.

II. Sed etiam casum alterum, ubi p est formae $8n+5$, aeque complete absolvere licet. Numerus 2 hic vel ad B, vel ad D pertinet, perspiciturque facile, in casu priori $\frac{1}{2}(p-1)$ ad B, $\frac{1}{2}(p+1)$ ad D, in casu posteriori autem $\frac{1}{2}(p-1)$ ad D, $\frac{1}{2}(p+1)$ ad B pertinere. Iam perpendamus, si β sit numerus ex B talis, quem sequatur numerus ex D, fore etiam numerum $p-\beta-1$ ex B atque $p-\beta$ ex D, i.e. numeros illius proprietatis binos associatos semper adesse. Erit itaque illorum multitudo, (13), par, excepto casu, in quo unus eorum sibi ipse associatus est, i.e. ubi $\frac{1}{2}(p-1)$ ad B, $\frac{1}{2}(p+1)$ ad D pertinet; tunc scilicet (13) impar erit. Hinc colligimus, (13) parem esse, quoties 2 ad D, imparem vero, quoties 2 ad B pertineat. Sed habemus

$$16(13) = aa + bb + 2a + 4b + 1$$

sive statuendo $a = 4q+1$, $b = 4r+2$,

$$(13) = qq + q + rr + 2r + 1$$

Erit itaque (13) impar, quoties r par est; contra (13) par erit, quoties r est impar: unde colligimus, 2 pertinere ad B, quoties b sit formae $8m+2$, ad D vero, quoties b sit formae $8m+6$.

Summa harum investigationum ita enunciari potest:

Numerus 2 *pertinet ad complexum* A, B, C *vel* D, *prout numerus* $\frac{1}{2}b$ *est formae* $4m$, $4m+1$, $4m+2$ *vel* $4m+3$.

22.

In *Disquisitionibus Arithmeticis* theoriam generalem divisionis circuli, atque solutionis aequationis $x^p - 1 = 0$ explicavimus, interque alia docuimus, si μ sit divisor numeri $p-1$, functionem $\frac{x^p-1}{x-1}$ in μ factores ordinis $\frac{p-1}{\mu}$ resolvi posse adiumento aequationis auxiliaris ordinis μ. Praeter theoriam generalem huius resolutionis simul casus speciales, ubi $\mu = 2$ vel $\mu = 3$, in illo opere artt. 356-358 seorsim consideravimus, aequationemque auxiliarem a priori assignare docuimus, i.e. absque evolutione schematis residuorum minimorum potestatum alicuius radicis primitivae pro modulo p. Iam vel nobis non monentibus lectores attenti facile percipient nexum arctissimum casus proximi istius theoriae, puta pro $\mu = 4$, cum investigationibus hic in artt. 15-20 explicatis, quarum adiumento, ille quoque sine difficultate complete absolvi poterit. Sed hanc tractationem ad aliam occasionem nobis reservamus, ideoque etiam in commentatione praesente disquisitionem in forma pure arithmetica perficere maluimus, theoria aequationis $x^p - 1 = 0$ nullo modo immixta. Contra coronidis loco adhuc quaedam alia theoremata nova pure arithmetica, cum argumento hactenus pertractato arctissime coniuncta, adiiciemus.

23.

Si potestas $(x^4+1)^{\frac{1}{2}(p-1)}$ secundum theorema binomiale evolvitur, tres termini aderunt, in quibus exponens ipsius x per $p-1$ divisibilis est, puta

$$x^{2(p-1)}, Px^{p-1} \text{ atque } 1$$

denotando per P coëfficientem medium

$$\frac{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p-3)\cdot\frac{1}{2}(p-5)\ldots\frac{1}{2}(p+3)}{1\cdot 2\cdot 3\ldots\frac{1}{4}(p-1)}$$

Substituendo itaque pro x deinceps numeros 1, 2, $3\ldots p-1$, obtinebimus per lemma art. 19

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2-P$$

At perpendendo ea quae in art. 19 exposuimus, insuperque, quod numeri complexuum A, B, C, D, ad potestatem exponentis $\frac{1}{2}(p-1)$ evecti congrui sunt, secundum modulum p, numeris $+1$, -1, $+1$, -1 resp., facile intelligitur fieri

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv 4(00)-4(01)+4(02)-4(03)$$

adeoque per schemata in fine artt. 18, 20 tradita

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2a-2$$

Comparatio horum duorum valorum suppeditat elegantissimum theorema: scilicet habemus

$$P \equiv 2a \pmod{p}$$

Denotando quatuor producta

$$\begin{aligned}
&1.2.3\ldots\tfrac{1}{4}(p-1)\\
&\tfrac{1}{4}(p+3).\tfrac{1}{4}(p+7).\tfrac{1}{4}(p+11)\ldots\tfrac{1}{2}(p-1)\\
&\tfrac{1}{2}(p+1).\tfrac{1}{2}(p+3).\tfrac{1}{2}(p+5)\ldots\tfrac{3}{4}(p-1)\\
&\tfrac{1}{4}(3p+1).\tfrac{1}{4}(3p+5).\tfrac{1}{4}(3p+9)\ldots(p-1)
\end{aligned}$$

resp. per q, r, s, t, theorema praecedens ita exhibetur:

$$2a \equiv \frac{r}{q} \pmod{p}$$

Quum quilibet factorum ipsius q complementum suum ad p habeat in t, erit $q \equiv t \pmod{p}$, quoties multitudo factorum par est, i.e. quoties p est formae $8n+1$, contra $q \equiv -t$, quoties multitudo factorum impar est, sive p formae $8n+5$. Perinde in casu priori erit $r \equiv s$, in posteriori $r \equiv -s$. In utroque casu erit $qr \equiv st$, et quum constet, haberi $qrst \equiv -1$, erit $qqrr \equiv -1$,adeoque $qr \equiv \pm f \pmod{p}$. Combinando

hanc congruentiam cum theoremate modo invento obtinemus $rr \equiv \pm 2af$, et proin, per artt. 19, 20

$$2b \equiv \pm rr \pmod{p}$$[3]

Valde memorabile est, discerptionem numeri p in duo quadrata per operationes prorsus directas inveniri posse; scilicet radix quadrati imparis erit residuum absolute minimum ipsius $\frac{r}{2q}$, radix quadrati paris vero residuum absolute minimum ipsius $\frac{1}{2}rr$ secundum modulum p. Expressionem $\frac{r}{2q}$, cuius valor pro $p = 5$ fit $= 1$, pro valoribus maioribus ipsius p, ita quoque exhibere licet:

$$\frac{6.10.14.18...(p-3)}{2.3.4.5...\frac{1}{4}(p-1)}$$

Sed quum insuper noverimus, quonam signo affecta prodeat ex hac formula radix quadrati imparis, eo scilicet, ut semper fiat formae $4m+1$, attentione perdignum est, quod simile criterium generale respectu signi radicis quadrati paris hactenus inveniri non potuerit. Quale si quis inveniat, et nobiscum communicet, magnam de nobis gratiam feret. Interim hic adiungere visum est valores numerorum a, b, f, quales pro valoribus ipsius p infra 200 e residuis minimis expressionum $\frac{r}{2q}$, $\frac{1}{2}rr$, qr prodeunt.

[3] atque $\{(a \mp b)q\}^2 \equiv a \equiv (\frac{r-qrr}{2})^2$

p	a	b	f
5	+1	+2	2
13	+3	−2	5
17	+1	−4	13
29	+5	+2	12
37	+1	−6	31
41	+5	+4	9
53	−7	−2	23
61	+5	−6	11
73	−3	−8	27
89	+5	−8	34
97	+9	+4	22
101	+1	−10	91
109	−3	+10	33
113	−7	+8	15
137	−11	+4	37
149	−7	−10	44
157	−11	−6	129
173	+13	+2	80
181	+9	+10	162
193	−7	+12	81
197	+1	−14	183

THEORIA
RESIDUORUM BIQUADRATICORUM

COMMENTATIO SECUNDA

A U C T O R E

CAROLO FRIDERICO GAUSS

SOCIETATI REGIAE TRADITA 1831, APR. 15.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VII.
Gottingae MDCCCXXXII.

THEORIA RESIDUORUM BIQUADRATICORUM.

COMMENTATIO SECUNDA

24.

In commentatione prima ea, quae ad classificationem biquadraticam numeri $+2$ requiruntur, complete absoluta sunt. Dum scilicet omnes numeros per modulum p (qui supponitur esse numerus primus formae $4n+1$) non divisibiles inter quatuor complexus A, B, C, D distributos concipimus, prout singuli ad potestatem exponentis $\frac{1}{4}(p-1)$ evecti congrui fiunt secundum modulum p ipsi $+1$, $+f$, -1, $-f$, denotante f radicem alterutram congruentiae $ff \equiv -1 \pmod{p}$: invenimus, diiudicationem, cuinam complexui adnumerandus sit numerus $+2$, pendere a discerptione numeri p in duo quadrata, ita quidem, ut si statuatur $p = aa + bb$, denotante aa quadratum impar, bb quadratum par, si porro *signa* ipsorum a, b ita accepta supponantur, ut habeatur $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$, numerus $+2$ ad complexum A, B, C, D pertinere debeat prout $\frac{1}{2}b$ sit formae $4n$, $4n+1$, $4n+2$, $4n+3$ resp.

Sponte quoque hinc demanat regula classificationi numeri -2 inserviens. Scilicet quum -1 pertineat ad classem A pro valore pari ipsius $\frac{1}{2}b$, ad classem C vero pro impari: pertinebit, per theorema art. 7, numerus -2 ad classem A, B, C, D, prout $\frac{1}{2}b$ est formae $4n$, $4n+3$, $4n+2$, $4n+1$ resp.

Haec theoremata etiam sequenti modo exprimi possunt:

Pertinet	$+2$	-2
ad complexum	si b, secundum modulum	8, fit congruus ipsi
A	0	0
B	$2a$	$6a$
C	$4a$	$4a$
D	$6a$	$2a$

Facile intelligitur, theoremata sic enunciata haud amplius pendere a conditione $a \equiv 1 \pmod 4$, sed etiamnum valere, si fuerit $a \equiv 3 \pmod 4$, dummodo conditio altera, $af \equiv b \pmod p$, conservetur.

Aeque facile perspicitur, summam horum theorematum eleganter contrahi posse in formulam unicam, puta:

si a et b positive accipiuntur, semper fit

$$b^{\frac{1}{2}ab} \equiv a^{\frac{1}{2}ab} 2^{\frac{1}{4}(p-1)} \pmod p$$

25.

Videamus nunc, quatenus inductio classificationem numeri 3 indigitet. Tabula art. 11 ulterius continuata (semper adoptata radice primitiva minima), monstrat, $+3$ pertinere

ad complexum

A pro			B pro			C pro			D pro		
p	a	b	p	a	b	p	a	b	p	a	b
13	-3	$+2$	17	$+1$	-4	37	$+1$	-6	5	$+1$	$+2$
109	-3	$+10$	29	$+5$	$+2$	61	$+5$	-6	41	$+5$	-4
181	$+9$	$+10$	53	-7	$+2$	73	-3	-8	149	-7	$+10$
193	-7	-12	89	$+5$	-8	97	$+9$	$+4$	173	$+13$	$+2$
229	-15	$+2$	101	$+1$	$+10$	157	-11	-6			
277	$+9$	$+14$	113	-7	-8	241	-15	-4			
			137	-11	-4						
			197	$+1$	-14						
			233	$+13$	$+8$						
			257	$+1$	-16						
			269	$+13$	$+10$						
			281	$+5$	$+16$						
			293	$+17$	$+2$						

Primo saltem aspectu nexum simplicem inter valores numerorum a, b, quibus idem complexus respondet, non animadvertimus. At si perpendimus, diiudicationem similem in theoria residuorum quadraticorum per regulam simpliciorem absolvi respectu numeri -3, quam respectu numeri $+3$, spes affulget successus aeque secundi in theoria residuorum biquadraticorum. Invenimus autem, -3 pertinere ad complexum

A pro		
p	a	b
37	+1	−6
61	+5	−6
157	−11	−6
193	−7	−12

B pro		
p	a	b
5	+1	+2
17	+1	−4
89	+5	−8
113	−7	−8
137	−11	−4
149	−7	+10
173	+13	+2
233	+13	+8
257	+1	−16
281	+5	+16

C pro		
p	a	b
13	−3	+2
73	−3	−8
97	+9	+4
109	−3	+10
181	+9	+10
229	−15	+2
241	−15	−4
277	+9	+14

D pro		
p	a	b
29	+5	+2
41	+5	−4
53	−7	+2
101	+1	+10
197	+1	−14
269	+13	+10
293	+17	+2

ubi lex inductionis sponte se offert. Scilicet pertinet -3 ad complexum

A, quoties b per 3 divisibilis est, sive $b \equiv 0 \pmod 3$
B, quoties $a+b$ per 3 est divisibilis, sive $b \equiv 2a \pmod 3$
C, quoties a per 3 est divisibilis, sive $a \equiv 0 \pmod 3$
D, quoties $a-b$ per 3 divisibilis est, sive $b \equiv a \pmod 3$

26.

Numerum $+5$ adscribendum invenimus complexui

A pro $p = 101,\ 109,\ 149,\ 181,\ 269$
B pro $p = 13,\ 17,\ 73,\ 97,\ 157,\ 193,\ 197,\ 233,\ 277,\ 293$
C pro $p = 29,\ 41,\ 61,\ 89,\ 229,\ 241,\ 281$
D pro $p = 37,\ 53,\ 113,\ 137,\ 173,\ 257$

In considerationem vocatis valoribus numerorum a, b singulis p respondentibus, lex hic aeque facile, ut pro classificatione numeri -3, prehenditur. Scilicet incidimus in complexum

A, quoties $b \equiv 0 \pmod 5$
B, quoties $b \equiv a$
C, quoties $a \equiv 0$
D, quoties $b \equiv 4a$

Manifestum est, has regulas complecti casus omnes, quum pro $b \equiv 2a$, vel $b \equiv 3a \pmod 5$, fieret $aa + bb \equiv 0$, Q.E.A., quum per hypothesin p sit numerus primus a 5 diversus.

27.

Perinde inductio ad numeros -7, -11, $+13$, $+17$, -19, -23 applicata satisque producta sequentes regulas indigitat:

Pro numero -7.

A	$a \equiv 0$, vel $b \equiv 0 \pmod 7$
B	$b \equiv 4a$, vel $b \equiv 5a$
C	$b \equiv a$, vel $b \equiv 6a$
D	$b \equiv 2a$, vel $b \equiv 3a$

Pro numero -11.

A	$b \equiv 0,\ 5a$, vel $6a \pmod{11}$
B	$b \equiv a,\ 3a$ vel $4a$
C	$a \equiv 0$, vel $b \equiv 2a$ vel $9a$
D	$b \equiv 7a,\ 8a$ vel $10a$

Pro numero $+13$.

A	$b \equiv 0,\ 4a,\ 9a \pmod{13}$
B	$b \equiv 6a,\ 11a,\ 12a$
C	$a \equiv 0;\ b \equiv 3a,\ 10a$
D	$b \equiv a,\ 2a,\ 7a$

Pro numero $+17$.

A	$a \equiv 0;\ b \equiv 0,\ a,\ 16a \pmod{17}$
B	$b \equiv 2a,\ 6a,\ 8a,\ 14a$
C	$b \equiv 5a,\ 7a,\ 10a,\ 12a$
D	$b \equiv 3a,\ 9a,\ 11a,\ 15a$

Pro numero -19.

A	$b \equiv 0,\ 2a,\ 5a,\ 14a,\ 17a \pmod{19}$
B	$b \equiv 3a,\ 7a,\ 11a,\ 13a,\ 18a$
C	$a \equiv 0;\ b \equiv 4a,\ 9a,\ 10a,\ 15a$
D	$b \equiv a,\ 6a,\ 8a,\ 12a,\ 16a$

Pro numero -23.

A	$a \equiv 0;\ b \equiv 0,\ 7a,\ 10a,\ 13a,\ 16a \pmod{23}$
B	$b \equiv 2a,\ 3a,\ 4a,\ 11a,\ 15a,\ 17a$
C	$b \equiv a,\ 5a,\ 9a,\ 14a,\ 18a,\ 22a$
D	$b \equiv 6a,\ 8a,\ 12a,\ 19a,\ 20a,\ 21a$

28.

Theoremata specialia hoc modo per inductionem eruta confirmari inveniuntur, quousque haec continuetur, formamque criteriorum pulcherrimam manifestant. Si vero inter se conferuntur, ut conclusiones generales inde petantur, primo statim aspectu se offerunt observationes sequentes.

Criteria diiudicationis, ad quemnam complexum referendus sit numerus primus $\pm q$ (sumendo signum superius vel inferius, prout q est formae $4n+1$ vel $4n+3$), pendent a formis numerorum a, b inter se collatorum respectu moduli q. Scilicet

I. quoties $a \equiv 0 \pmod{q}, \pm q$ pertinet ad complexum determinatum, qui est A pro $q = 7,\ 17,\ 23$, nec non C pro $q = 3,\ 11,\ 13,\ 19$, unde coniectura oritur, casum priorem generaliter valere, quoties q sit formae $8n \pm 1$, posteriorem vero, quoties q sit formae $8n \pm 3$. Ceterum complexus B et D iam absque inductione excluduntur pro valore ipsius a per q divisibili, ubi fit $p \equiv bb \pmod{q}$, i.e. ubi p est residuum quadraticum ipsius q, unde per theorema fundamentale $\pm q$ esse debet residuum quadraticum ipsius p.

II. Quoties autem a per q non est divisibilis, criterium pendet a valore expressionis $\frac{b}{a} \pmod{q}$. Admittit quidem haec expressio q valores diversos, puta 0, 1, 2, $3 \ldots q-1$ sed quoties q est formae $4n+1$, excludendi sunt bini valores expressionis

$\sqrt{-1} \pmod q$, qui manifesto nequeunt esse valores expressionis $\frac{b}{a} \pmod q$, quum $p = aa + bb$ semper supponatur esse numerus primus a q diversus. Quapropter multitudo valorum admissibilium expressionis $\frac{b}{a} \pmod q$ est $= q-2$, pro $q \equiv 1 \pmod 4$, dum manet $= q$ pro $q \equiv 3 \pmod 4$.

Iam hi valores in quaternas classes distribuuntur, puta, ut quidam, indefinite per α denotandi, respondeant complexui A; alii per β denotandi complexui B; alii γ complexui C; denique reliqui δ complexui D, ita scilicet, ut $\pm q$ complexui A, B, C, D adscribendus sit, prout habeatur $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, $b \equiv \delta a \pmod q$.

At *lex* huius distributionis abstrusior videtur, etiamsi quaedam generalia promte animadvertantur. Multitudo in ternis classibus eadem reperitur, puta $= \frac{1}{4}(q-1)$ vel $\frac{1}{4}(q+1)$, dum in una (et quidem in eadem, quae respondet complexui cum criterio $a \equiv 0$) unitate minor est, ita ut multitudo omnium criteriorum diversorum respectu singulorum complexuum fiat eadem, puta $= \frac{1}{4}(q-1)$ vel $\frac{1}{4}(q+1)$. Porro animadvertimus, 0 semper in prima classe (inter α) reperiri nec non complementa numerorum α, β, γ, δ ad q, puta $q-\alpha$, $q-\beta$, $q-\gamma$, $q-\delta$ resp. in classe prima, quarta, tertia, secunda. Denique valores expressionum $\frac{1}{a}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta} \pmod q$ pertinere videmus ad classem primam, quartam, tertiam, secundam, quoties criterium $a \equiv 0$ respondet complexui A; ad classem tertiam, secundam, primam, quartam resp. autem, quoties criterium $a \equiv 0$ refertur ad complexum C. Sed ad haec fere limitantur, quae per inductionem assequi licet, nisi audacius ea, quae infra e fontibus genuinis haurientur, anticipare nobis arrogemus.

29.

Antequam ulterius progrediamur, observare convenit, criteria pro numeris primis (positive sumtis, si sunt formae $4n+1$, negative, si formae $4n+3$) sufficere ad diiudicationem pro omnibus reliquis numeris, si modo theorema art. 7, atque criteria pro -1 et ± 2 in subsidium vocentur. Ita e.g. si desiderantur criteria pro numero $+3$, criteria in art. 25 prolata, quae referuntur ad -3, etiamnum pro $+3$ valebunt, quoties $\frac{1}{2}b$ est numerus par: contra complexus A, B, C, D cum complexibus C, D, A, B permutandi erunt, quoties $\frac{1}{2}b$ est impar, unde sequuntur praecepta haecce:

	$+3$ pertinet
ad complexum	si
A	$b \equiv 0 \pmod{12}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 2 \pmod{4}$
B	$b \equiv 8a$ vel $10a \pmod{12}$
C	$b \equiv 6a \pmod{12}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{4}$
D	$b \equiv 2a$ vel $4a \pmod{12}$

Perinde criteria pro ± 6 petuntur e combinatione criteriorum pro ∓ 2 et -3; scilicet

	$+6$ pertinet
ad complexum	si
A	$b \equiv 0, \quad 2a, 22a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 4a \pmod{8}$
B	$b \equiv 4a, \quad 6a, \ 8a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 2a \pmod{8}$
C	$b \equiv 10a, 12a, 14a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{8}$
D	$b \equiv 16a, 18a, 20a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 6a \pmod{8}$

	-6 vero
ad complexum	si
A	$b \equiv 0, \ 10a, 14a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 4a \pmod{8}$
B	$b \equiv 4a, \ 8a, 18a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 6a \pmod{8}$
C	$b \equiv 2a, 12a, 22a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{8}$
D	$b \equiv 6a, 16a, 20a \pmod{24}$; vel simul $a \equiv 0 \pmod{3}, b \equiv 2a \pmod{8}$

Simili modo criteria pro numero $+21$ concinnabuntur e criteriis pro -3 et -7; criteria pro -105 e criteriis pro -1, -3, $+5$, -7, etc.

30.

Amplissimam itaque messem theorematum specialium aperit inductio, theoremati pro numero 2 affinium: sed desideratur vinculum commune, desiderantur demonstrationes rigorosae, quum methodus, per quam in commentatione prima numerum 2 absolvimus, ulteriorem applicationem non patiatur. Non desunt quidem methodi diversae, per quas demonstrationibus pro casibus particularibus potiri liceret, iis potissimum, qui distributionem residuorum quadraticorum inter complexus A, C spectant, quibus tamen non immoramur; quum theoria generalis *omnes* casus com-

plectens in votis esse debeat. Cui rei quum inde ab anno 1805 meditationes nostras dicare coepissemus, mox certiores facti sumus, fontem genuinum theoriae generalis in campo arithmeticae promoto quaerendum esse, uti iam in art. 1 addigitavimus.

Quemadmodum scilicet arithmetica sublimior in quaestionibus hactenus pertractatis inter solos numeros integros reales versatur, ita theoremata circa residua biquadratica tunc tantum in summa simplicitate ac genuina venustate resplendent, quando campus arithmeticae ad quantitates imaginarias extenditur, ita ut absque restrictione ipsius obiectum constituant numeri formae $a+bi$, denotantibus i, pro more quantitatem imaginariam $\sqrt{-1}$, atque a, b indefinite omnes numeros reales integros inter $-\infty$ et $+\infty$. Tales numeros vocabimus *numeros integros complexos*, ita quidem, ut reales complexis non opponantur, sed tamquam species sub his contineri censeantur. Commentatio praesens tum doctrinam elementarem de numeris complexis, tum prima initia theoriae residuorum biquadraticorum sistet, quam ab omni parte perfectam reddere in continuatione subsequente suscipiemus[4].

31.

Ante omnia quasdam denominationes praemittimus, per quarum introductionem brevitati et perspicuitati consuletur.

Campus numerorum complexorum $a+bi$ continet

I. numeros reales, ubi $b=0$, et, inter hos, pro indole ipsius a

1) cifram

2) numeros positivos

3) numeros negativos

II. numeros imaginarios, ubi b cifrae inaequalis. Hic iterum distinguuntur

1) numeri imaginarii absque parte reali, i.e. ubi $a=0$

2) numeri imaginarii cum parte reali, ubi neque b neque $a=0$.

Priores si placet numeri imaginarii puri, posteriores numeri imaginarii mixti vocari possunt.

[4]Obiter saltem hic adhuc monere convenit, campum ita definitum imprimis theoriae residuorum biquadraticorum accommodatum esse. Theoria residuorum cubicorum simili modo superstruenda est considerationi numerorum formae $a+bh$, ubi h est radix imaginaria aequationis $h^3-1=0$, puta $h=-\frac{1}{2}+\sqrt{\frac{3}{4}}.i$; et perinde theoria residuorum potestatum altiorum introductionem aliarum quantitatum imaginariarum postulabit.

Unitatibus in hac doctrina utimur quaternis, $+1$, -1, $+i$, $-i$, quae simpliciter positiva, negativa, positiva imaginaria, negativa imaginaria audient.

Producta terna cuiuslibet numeri complexi per -1, $+i$, $-i$ illius *socios* vel *numeros illi associatos* appellabimus. Excepta itaque cifra (quae sibi ipsa associata est), semper quaterni numeri *inaequales* associati sunt.

Contra numero complexo *coniunctum* vocamus eum, qui per permutationem ipsius i cum $-i$ inde oritur. Inter numeros imaginarios itaque bini *inaequales* semper coniuncti sunt, dum numeri reales sibi ipsi sunt coniuncti, siquidem denominationem ad hos extendere placet.

Productum numeri complexi per numerum ipsi coniunctum utriusque *normam vocamus*. Pro norma itaque numeri realis, ipsius quadratum habendum est.

Generaliter octonos numeros nexos habemus, puta

$$\begin{array}{r|l} a+bi & a-bi \\ -b+ai & -b-ai \\ -a-bi & -a+bi \\ b-ai & b+ai \end{array}$$

ubi duas quaterniones numerorum associatorum, quatuor biniones coniunctorum conspicimus, omniumque norma communis est $aa+bb$. Sed octo numeri ad quatuor inaequales reducuntur, quoties vel $a=\pm b$, vel alteruter numerorum a, $b=0$.

E definitionibus allatis protinus demanant sequentia:

Producto duorum numerorum complexorum coniunctum est productum e numeris, qui illis coniuncti sunt.

Idem valet de producto e pluribus factoribus, nec non de quotientibus.

Norma producti e duobus numeris complexis aequalis est producto ex horum normis.

Hoc quoque theorema extenditur ad producta e quotcunque factoribus et ad quotientes.

Cuiusvis numeri complexi (excipiendo cifram, quod plerumque abhinc tacite subintelligemus) norma est numerus *positivus*.

Ceterum nihil obstat, quominus definitiones nostrae ad valores fractos vel adeo irrationales ipsorum a, b extendantur; sed $a+bi$ tunc tantum numerus complexus integer audiet, quando *uterque* a, b est integer, atque tunc tantum rationalis, quando *uterque* a, b rationalis est.

32.

Algorithmus operationum arithmeticarum circa numeros complexos vulgo notus est: divisio, per introductionem normae, ad multiplicationem reducitur, quum habeatur

$$\frac{a+bi}{c+di} = (a+bi)\cdot\frac{c-di}{cc+dd} = \frac{ac+bd}{cc+dd} + \frac{bc-ad}{cc+dd}\cdot i$$

Extractio radicis quadratae perficitur adiumento formulae

$$\sqrt{(a+bi)} = \pm(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} + i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}})$$

si b est numerus positivus, vel huius

$$\sqrt{(a+bi)} = \pm(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} - i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}})$$

si b est numerus negativus. Usui transformationis quantitatis complexae $a+bi$ in $r(\cos\varphi + i\sin\varphi)$ ad calculos facilitandos, non opus est hic immorari.

33.

Numerum integrum complexum, qui in factores duos ab unitatibus diversos[5] resolvi potest, vocamus numerum complexum compositum; contra numerus primus complexus dicetur, qui talem resolutionem in factores non admittit. Hinc statim patet, quemvis numerum compositum realem etiam esse compositum complexum. At numerus primus realis poterit esse numerus complexus compositus, et quidem hoc valebit de numero 2 atque de omnibus numeris primis realibus positivis formae $4n+1$ (excepto numero 1), quippe quos in bina quadrata positiva decomponi posse constat; puta, fit $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$, $13 = (3+2i)(3-2i)$, $17 = (1+4i)(1-4i)$ etc.

Contra numeri primi reales positivi formae $4n+3$ semper sunt numeri primi complexi. Si enim talis numerus q esset $= (a+bi)(\alpha+\beta i)$, foret etiam $q = (a-bi)(\alpha-\beta i)$, adeoque $qq = (aa+bb)(\alpha\alpha+\beta\beta)$: at qq unico tantum modo in factores positivos unitate maiores resolvi potest, puta in $q\times q$, unde esse deberet $q = aa+bb = \alpha\alpha+bb$, Q.E.A; quum summa duorum quadratorum nequeat esse formae $4n+3$.

[5] sive, quod idem est, tales, quorum normae unitate sint maiores.

Numeri reales negativi manifesto easdem denominationes servant, quas positivi, idemque valet de numeris imaginariis puris.

Superest itaque, ut inter numeros imaginarios mixtos, compositos a primis dignoscere doceamus, quod fit per sequens

THEOREMA. *Quivis numerus integer imaginarius mixtus* $a+bi$ *est vel numerus primus complexus, vel numerus compositus, prout ipsius norma est vel numerus primus realis, vel numerus compositus.*

Dem. I. Quoniam numeri complexi compositi norma semper est numerus compositus, patet, numerum complexum, cuius norma sit numerus primus realis, necessario esse debere numerum primum complexum. Q. E. P.

II. Si vero norma $aa+bb$ est numerus compositus, sit p numerus primus positivus realis illam metiens. Duo iam casus distinguendi sunt.

1) Si p est formae $4n+3$, constat, $aa+bb$ per p divisibilem esse non posse, nisi p simul metiatur ipsos a, b, unde $a+bi$ erit numerus compositus.

2) Si p non est formae $4n+3$, certo in duo quadrata decomponi poterit: statuemus itaque $p=\alpha\alpha+\beta\beta$. Quum fiat

$$(a\alpha+b\beta)(a\alpha-b\beta)=aa(\alpha\alpha+\beta\beta)-\beta\beta(aa+bb)$$

adeoque per p divisibilis, p certo alterutrum factorem $a\alpha+b\beta$, $a\alpha-b\beta$ metietur, et quum insuper fiat

$$(a\alpha+b\beta)^2+(b\alpha-a\beta)^2=(a\alpha-b\beta)^2+(b\alpha+a\beta)^2=(aa+bb)(\alpha\alpha+\beta\beta)$$

adeoque per pp divisibilis, patet, in casu priori etiam $b\alpha-a\beta$, in posteriori $b\alpha+a\beta$ per p divisibilem esse debere. Quare in casu priori

$$\tfrac{a+bi}{\alpha+\beta i}=\tfrac{a\alpha+b\beta}{p}+\tfrac{b\alpha-a\beta}{p}\cdot i$$

erit numerus integer complexus, in posteriori autem

$$\tfrac{a+bi}{\alpha-\beta i}=\tfrac{a\alpha-b\beta}{p}+\tfrac{b\alpha+a\beta}{p}\cdot i$$

integer erit. Quum itaque numerus propositus vel per $\alpha+\beta i$ vel per $\alpha-\beta i$ divisibilis sit, quotientisque norma $=\tfrac{aa+bb}{p}$ per hyp. ab unitate diversa fiat, patet, $a+bi$ in utroque casu esse numerum complexum compositum. Q. E. S.

34.

Totum itaque ambitum numerorum primorum complexorum exhauriunt quatuor species sequentes:

1) quatuor unitates, 1, $+i$, -1, $-i$, quas tamen, dum de numeris primis agemus, plerumque tacite subintelligemus exclusas.

2) numerus $1+i$ cum tribus sociis $-1+i$, $-1-i$, $1-i$.

3) numeri primi reales positivi formae $4n+3$ cum ternis sociis.

4) numeri complexi, quorum normae sunt numeri primi reales formae $4n+1$ unitate maiores, et quidem cuivis normae tali datae semper octoni numeri primi complexi et non plures respondebunt, quum talis norma unico tantum modo in bina quadrata decomponi possit.

35.

Quemadmodum numeri integri reales in pares et impares distribuuntur, atque illi iterum in pariter pares et impariter pares, ita inter numeros complexos distinctio aeque essentialis se offert: sunt scilicet

vel per $1+i$ non divisibiles, puta numeri $a+bi$, ubi alter numerorum a, b est impar, alter par;

vel per $1+i$ neque vero per 2 divisibiles, quoties uterque a, b est impar;

vel per 2 divisibiles, quoties uterque a, b est par.

Numeri primae classis commode dici possunt numeri complexi impares, secundae semipares, tertiae pares.

Productum e pluribus factoribus complexis semper impar erit, quoties omnes factores sunt impares; semipar, quoties unus factor est semipar, reliqui impares; par autem, quoties inter factores vel saltem duo semipares inveniuntur, vel saltem unus par.

Norma cuiusvis numeri complexi imparis est formae $4n+1$; norma numeri semiparis est formae $8n+2$; denique norma numeri paris est productum numeri formae $4n+1$ in numerum 4 vel altiorem binarii potestatem.

36.

Quum nexus inter quaternos numeros complexos socios analogus sit nexui inter binos numeros reales oppositos (i.e. absolute aequales signisque oppositis affectos), atque ex his vulgo positivus tamquam primarius merito considerari soleat:quaestio

oritur, num similis distinctio inter quaternos numeros complexos socios stabiliri possit, et pro utili haberi debeat. Ad quam decidendam perpendere oportet, principium distinctionis ita comparatum esse debere, ut productum duorum numerorum, qui inter socios suos pro primariis valent, semper fiat numerus primarius inter socios suos. At mox certiores fimus, tale principium omnino non dari, nisi distinctio ad numeros integros restringatur: quinadeo distinctio *utilis* ad numeros impares limitanda erit. Pro his vero finis propositus duplici modo attingi potest. Scilicet

I. Productum duorum numerorum $a+bi$, $a'+b'i$ ita comparatorum, ut a, a' sint formae $4n+1$, atque b, b' pares, eadem proprietate gaudebit, ut pars realis fiat $\equiv 1 \pmod 4$, atque pars imaginaria par. Et facile perspicietur, inter quaternos numeros impares associatos unum solum sub illa forma contentum esse.

II. Si numerus $a+bi$ ita comparatus est, ut $a-1$ et b vel simul pariter pares sint, vel simul impariter pares, eius productum per numerum complexum eiusdem formae eadem forma gaudebit, facileque perspicitur, e quaternis numeris imparibus associatis unum solum sub hac forma contineri.

Ex his duobus principiis aeque fere idoneis posterius adoptabimus, scilicet inter quaternos numeros complexos impares associatos eum pro primario habebimus, qui secundum modulum $2+2i$ unitati positivae fit congruus: hoc pacto plura insignia theoremata maiori concinnitate enunciare licebit. Ita e.g. sunt numeri primi complexi primarii $-1+2i$, $-1-2i$, $+3+2i$, $+3-2i$, $+1+4i$, $+1-4i$ etc., nec non reales -3, -7, -11, -19 etc. manifesto semper signo negativo afficiendi. Numero complexo impari primario coniunctus quoque primarius erit.

Pro numeris semiparibus et paribus in genere similis distinctio nimis arbitraria parumque utilis foret. E numeris primis associatis $1+i$, $1-i$, $-1+i$, $-1-i$ unum quidem prae reliquis pro primario eligere possumus, sed ad compositos talem distinctionem non extendemus.

37.

Si inter factores numeri complexi compositi inveniuntur tales, qui ipsi sunt compositi, atque hi iterum in factores suos resolvuntur, manifesto tandem ad factores primos delabimur, i.e. quivis numerus compositus in factores primos resolubilis est. Inter quos si qui non primarii reperiuntur, singulorum loco substituatur productum

primarii associati per $i, -1$ vel $-i$. Hoc pacto patet, quemvis numerum complexum compositum M reduci posse ad formam

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \dots$$

ita ut A, B, C etc. sint numeri primi complexi primarii inaequales, atque $\mu = 0$, 1, 2 vel 3. Circa hanc resolutionem theorema se offert, unico tantum modo eam fieri posse, quod theorema obiter quidem consideratum per se manifestum videri posset, sed utique demonstratione eget. Ad quam sternit viam sequens

THEOREMA. *Productum $M = A^{\alpha} B^{\beta} C^{\gamma} \dots$, denotantibus A, B, C etc. numeros primos complexos primarios diversos, divisibile esse nequit per ullum numerum primum complexum primarium, qui inter A, B, C etc. non reperitur.*

Dem. Sit P numerus primus complexus primarius inter A, B, C etc. non contentus, sintque p, a, b, c etc. normae numerorum P, A, B, C etc. Hinc facile colligitur, normam numeri M fore $= a^{\alpha} b^{\beta} c^{\gamma}$ etc., unde hic numerus, si M per P divisibilis esset, per p divisibilis esse deberet. Quum singulae normae sint vel numeri primi reales (e serie 2, 5, 13, 17 etc.), vel numerorum primorum realium quadrata (e serie 9, 49, 121 etc.), sponte patet, illud evenire non posse, nisi p cum aliqua norma a, b, c etc. identica fiat: supponemus itaque $p = a$. At quum P, A per hyp. sint numeri primi complexi primarii non identici, facile perspicietur, haec simul consistere non posse, nisi P, A sint numeri complexi imaginarii coniuncti, et proin $p = a$ numerus primus realis impar, (non quadratum numeri primi): supponemus itaque $A = k + li$, $P = k - li$. Hinc (extendendo notionem et signum congruentiae ad numeros integros complexos) erit $A \equiv 2k \pmod{P}$, unde facile colligitur

$$M \equiv 2^{\alpha} k^{\alpha} B^{\beta} C^{\gamma} \dots \pmod{P}$$

Quapropter dum M per P divisibilis supponitur, erit etiam

$$2^{\alpha} k^{\alpha} B^{\beta} C^{\gamma} \dots$$

per P divisibilis, adeoque norma huius numeri, quae fit

$$= 2^{2\alpha} k^{2\alpha} b^{\beta} c^{\gamma} \dots$$

divisibilis per p. At quum 2 et k per p certo non sint divisibiles, hinc sequitur, p

cum aliquo numerorum b, c etc. identicum esse debere: sit e.g. $p = b$. Hinc vero concludimus, esse vel $B = k + li$, vel $B = k - li$, i.e. vel $B = A$, vel $B = P$, utrumque contra hyp.

Ex hoc theoremate alterum, quod resolutio in factores primos unico tantum modo perfici potest, facillime derivatur, et quidem per ratiocinia iis, quibus in *Disquisitionibus Arithmeticis* pro numeris realibus usi sumus (art. 16), prorsus analoga: quapropter illis hic immorari superfluum foret.

38.

Progredimur iam ad congruentiam numerorum secundum modulos complexos. Sed in limine huius disquisitionis convenit indicare, quomodo ditio quantitatum complexarum intuitui subiici possit.

Sicuti omnis quantitas realis per partem rectae utrinque infinitae ab initio arbitrario sumendam, et secundum segmentum arbitrarium pro unitate acceptum aestimandam exprimi, adeoque per punctum alterum repraesentari potest, ita ut puncta ab altera initii plaga quantitates positivas, ab altera negativas repraesentent: ita quaevis quantitas complexa repraesentari poterit per aliquod punctum in plano infinito, in quo recta determinata ad quantitates reales refertur, scilicet quantitas complexa $x + iy$ per punctum, cuius abscissa $= x$, ordinata (ab altera lineae abscissarum plaga positive, ab altera negative sumta) $= y$. Hoc pacto dici potest, quamlibet quantitatem complexam mensurare inaequalitatem inter situm puncti ad quod refertur atque situm puncti initialis, denotante unitate positiva deflexum arbitrarium determinatum versus directionem arbitrariam determinatam; unitate negativa deflexum aeque magnum versus directionem oppositam; denique unitatibus imaginariis deflexus aeque magnos versus duas directiones laterales normales.

Hoc modo metaphysica quantitatum, quas imaginarias dicimus, insigniter illustratur. Si punctum initiale per (0) denotatur, atque duae quantitates complexae m, m' ad puncta M, M' referuntur, quorum situm relative ad (0) exprimunt, differentia $m - m'$ nihil aliud erit nisi situs puncti M relative ad punctum M': contria, producto mm' repraesentante situm puncti N relative ad (0), facile perspicies, hunc situm perinde determinari per situm puncti M ad (0), ut situs puncti M' determinatur per situm puncti cui respondet unitas positiva, ita ut haud inepte dicas, situs punctorum respondentium quantitatibus complexis mm',m, m', 1 formare *proportionem.*

Sed uberiorem huius rei tractationem ad aliam occasionem nobis reservamus. Difficultates, quibus theoria quantitatum imaginariarum involuta putatur, ad magnam partem a denominationibus parum idoneis originem traxerunt (quum adeo quidam usi sint nomine absono quantitatum impossibilium). Si, a conceptibus, quos offerunt varietates duarum dimensionum, (quales in maxima puritate conspiciuntur in intuitionibus spatii) profecti, quantitates positivas directas, negativas inversas, imaginarias laterales nuncupavissemus, pro tricis simplicitas, pro caligine claritas successisset.

39.

Quae in art. praec. prolata sunt, ad quantitates complexas continuas referuntur: in arithmetica, quae tantummodo circa numeros integros versatur, schema numerorum complexorum erit systema punctorum aequidistantium et in rectis aequidistantibus ita dispositorum, ut planum infinitum in infinite multa quadrata aequalia dispertiant. Omnes numeri per numerum complexum datum $a+bi=m$ divisibiles item infinite multa quadrata formabunt, quorum latera $=\sqrt{(aa+bb)}$ sive areae $=aa+bb$; quadrata posteriora ad priora inclinata erunt, quoties quidem neuter numerorum a, b est $=0$. Cuivis numero per modulum m non divisibili respondebit punctum vel intra tale quadratum situm vel in latere duobus quadratis contiguo; posterior tamen casus locum habere nequit, nisi a, b divisorem communem habent: porro patet, numeros secundum modulum m congruos in quadratis suis locos congruentes occupare. Hinc facile concluditur, si colligantur omnes numeri intra quadratum determinatum siti, nec non omnes qui forte in duobus eius lateribus non oppositis iaceant, denique his adscribatur numerus per m divisibilis, haberi systema completum residuorum incongruorum secundum modulum m, i.e. quemvis integrum alicui ex illis et quidem unico tantum congruum esse debere. Nec difficile foret ostendere, horum residuorum multitudinem aequalem esse moduli normae, puta $=aa+bb$. Sed consultum videtur, hoc gravissimum theorema alio modo pure arithmetico demonstrare.

40.

THEOREMA. *Secundum modulum complexum datum $m=a+bi$, cuius norma $aa+bb=p$, et pro quo a, b sunt numeri inter se primi, quilibet integer complexus congruus erit alicui residuo e serie $0, 1, 2, 3 \ldots p-1$, et non pluribus.*

Demonstr. I. Sint α, β integri tales qui faciant $\alpha a + \beta b = 1$, unde erit

$$i = \alpha b - \beta a + m(\beta + \alpha i)$$

Proposito itaque numero integro complexo $A + Bi$, habebimus

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha B i)$$

Quare denotando per h residuum minimum positivum numeri $A+(\alpha b-\beta a)B$ secundum modulum p, statuendoque

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki)$$

erit

$$A + Bi = h + m(\beta B + ak + (\alpha B - bk)i)$$

sive

$$A + Bi \equiv h \,(\text{mod. } m). \qquad \text{Q. E. P.}$$

II. Quoties eidem numero complexo duo numeri reales h, h' secundum modulum m congrui sunt, etiam inter se congrui erunt. Statuamus itaque $h - h' = m(c + di)$, unde fit

$$(h - h')(a - bi) = p(c + di)$$

adeoque

$$(h - h')a = pc, \quad (h - h')b = -pd$$

nec non, propter $a\alpha + b\beta = 1$,

$$h - h' = p(c\alpha - d\beta), \text{ i.e. } h \equiv h' \,(\text{mod. } p)$$

Quapropter h et h', siquidem sunt inaequales, ambo simul in complexu numerorum 0, 1, 2, $3 \ldots p-1$ contenti esse nequeunt. Q. E. S.

41.

THEOREMA. *Secundum modulum complexum $m = a+bi$, cuius norma $aa+bb = p$, et pro quo a, b non sunt inter se primi, sed divisorem communem maximum λ habent (quem positive acceptum supponimus), quilibet numerus complexus congruus est residuo $x+yi$ tali, ut x sit aliquis numerorum $0, 1, 2, 3 \ldots \frac{p}{\lambda} - 1$, atque y aliquis horum 0, 1, 2, $3 \ldots \lambda - 1$, et quidem unico tantum inter omnia p residua, quae tali forma gaudent.*

Demonstr. I. Accipiendo integros α, β ita, ut fiat $\alpha a + \beta b = \lambda$, erit $\lambda i = \alpha b - \beta a + m(\beta + \alpha i)$. Iam sit $A + Bi$ numerus complexus propositus, y residuum minimum positivum ipsius B secundum modulum λ, atque x residuum minimum positivum ipsius $A + (\alpha b - \beta a) \cdot \frac{B-y}{\lambda}$ secundum modulum $\frac{p}{\lambda}$, statuaturque

$$A + (\alpha b - \beta a) \cdot \tfrac{B-y}{\lambda} = x + \tfrac{p}{\lambda} \cdot k$$

Hinc erit

$$\begin{aligned} A + Bi - (x + yi) &= \tfrac{p}{\lambda} \cdot k + (B - y)i - (\alpha b - \beta a)\tfrac{B-y}{\lambda} \\ &= \tfrac{p}{\lambda} \cdot k + \tfrac{B-y}{\lambda} \cdot m(\beta + \alpha i) \\ &= (\tfrac{a}{\lambda} - \tfrac{b}{\lambda} \cdot i)km + \tfrac{B-y}{\lambda}(\beta + \alpha i)m \end{aligned}$$

i.e. per m divisibilis, sive $A + Bi \equiv x + yi \pmod{m}$ Q. E. P.

II. Supponamus, secundum modulum m eidem numero complexo congruos esse duos numeros $x+yi$, $x'+y'i$, qui proin etiam inter se congrui erunt secundum modulum m. A potiori itaque secundum modulum λ congrui erunt, adeoque $y \equiv y' \pmod{\lambda}$. Quodsi igitur uterque y, y' inter numeros 0, 1, 2, $3 \ldots \lambda - 1$ contentus esse supponitur, necessario debet esse $y = y'$. Hoc pacto vero etiam fiet $x \equiv x' \pmod{m}$, i.e. $x - x'$ per m, adeoque $\frac{x-x'}{\lambda}$ integer per $\frac{a}{\lambda} + \frac{b}{\lambda} \cdot i$ divisibilis, sive

$$\tfrac{x-x'}{\lambda} \equiv 0 \pmod{\tfrac{a}{\lambda} + \tfrac{b}{\lambda} \cdot i}$$

Hinc autem, quum $\frac{a}{\lambda}$, $\frac{b}{\lambda}$ sint numeri inter se primi, concluditur per partem secundam theorematis art. praec., $\frac{x-x'}{\lambda}$ etiam per normam numeri $\frac{a}{\lambda} + \frac{b}{\lambda} \cdot i$, i.e. per numerum $\frac{p}{\lambda\lambda}$ divisibilem fore, adeoque $x - x'$ per $\frac{p}{\lambda}$. Quapropter si etiam uterque x, x' in complexu numerorum 0, 1, 2, $3 \ldots \frac{p}{\lambda} - 1$ contentus esse supponitur, necessario erit $x = x'$, sive residua $x + yi$, $x' + y'i$ identica. Q. E. S.

Ceterum sponte patet, huc quoque referendum esse casum, ubi modulus est numerus realis, puta $b = 0$, et proin $\lambda = \pm a$, nec non eum, ubi modulus est numerus pure imaginarius, puta $a = 0$, et proin $\lambda = \pm b$. In utroque casu habetur $\frac{p}{\lambda} = \lambda$.

42.

Referendo itaque omnes numeros complexos secundum modulum datum inter se congruos ad eandem classem, incongruos ad diversas, omnino aderunt p classes totum numerorum integrorum ambitum exhaurientes, denotante p normam moduli. Complexus totidem numerorum e singulis classibus desumtorum exhibebit systema completum residuorum incongruorum, quale in artt. 40, 41 assignavimus. Et in hocce quidem systemate electio residuorum classes suas quasi repraesentantium innixa erat principio ei, ut in quavis classe adoptaretur residuum $x+yi$ tale, pro quo y habeat valorem minimum, atque inter omnia, quibus idem valor minimus ipsius y inest, id, pro quo valor ipsius x est minimus, exclusis valoribus negativis tum pro x tum pro y. Sed ad alia proposita aliis principiis uti conveniet, imprimisque notandus est modus is, ubi residua talia adoptantur, quae per modulum divisa offerunt quotientes simplicissimos. Manifesto si $\alpha+\beta i$, $\alpha'+\beta' i$, $\alpha''+\beta'' i$ etc. sunt quotientes e divisione numerorum congruorum per modulum oriundi, differentiae tum quantitatum α, α', α'' etc. inter se erunt numeri integri, tum differentiae inter quantitates β, β', β'' etc., patetque, semper adesse residuum unum, pro quo α et β iaceant inter limites 0 et 1, limite priori incluso, posteriori excluso: tale residuum simpliciter vocamus residuum minimum. Si magis placet, loco illorum limitum etiam hi adoptari possunt $-\frac{1}{2}$ et $+\frac{1}{2}$ (altero admisso, altero excluso): residuum tali limitationi respondens *absolute minimum* dicemus.

Circa haec residua minima offerunt se problemata sequentia.

43.

Residuum minimum numeri complexi dati $A+Bi$ secundum modulum $a+bi$, cuius norma $=p$, invenitur sequenti modo. Si $x+yi$ est residuum minimum quaesitum, erit $(x+yi)(a-bi)$ residuum minimum producti $(A+Bi)(a-bi)$ secundum modulum $(a+bi)(a-bi)$, i.e. secundum modulum p. Statuendo itaque

$$aA+bB=Fp+f, \quad aB-bA=Gp+g$$

ita ut f, g sint residua minima numerorum $aA+bB$, $aB-bA$ secundum modulum p, erit

$$x + yi = \tfrac{f+gi}{a-bi}$$

sive

$$x = \tfrac{af-bg}{p} = A - aF + bG$$
$$y = \tfrac{ag+bf}{p} = B - aG - bF$$

Manifesto residua minima f, g vel inter limites 0 et $p-1$, vel inter hos $-\frac{1}{2}p$ et $+\frac{1}{2}p$ accipi debent, prout numeri complexi vel residuum simpliciter minimum vel absolute minimum desideratur.

44.

Constructio systematis completi residuorum minimorum pro modulo dato pluribus modis effici potest. Methodus prima ita procedit, ut primo determinentur limites, intra quos termini reales iacere debent, ac dein pro singulis valoribus intra hos limites sitis assignentur limites partium imaginariarum. Criterium generale residui minimi $x+yi$ pro modulo $a+bi$ in eo consistit, ut tum $ax+by = \xi$, tum $ay-bx = \eta$ iaceat inter limites 0 et $aa+bb$, quoties de residuis simpliciter minimis agitur, vel inter limites $-\frac{1}{2}(aa+bb)$ et $+\frac{1}{2}(aa+bb)$, quoties residua absolute minima desiderantur, limite altero excluso. Regulae speciales distinctionem casuum, quos varietas signorum numerorum a, b affert, requirerent, cui tamen evolvendae, quum nulli difficultati obnoxia sit, hic immorari supersedemus: sufficiat, methodi indolem per unicum exemplum exposuisse.

Pro modulo $5+2i$ residua simpliciter minima $x+yi$ ita comparata esse debent, ut tum $5x+2y = \xi$, tum $5y-2x = \eta$ aequetur alicui numerorum 0, 1, 2, $3 \ldots 28$. Aequatio $29x = 5\xi - 2\eta$ ostendit, valores positivos ipsius x maiores esse non posse quam $\frac{5.28}{29}$, negativos abstrahendo a signo non maiores quam $\frac{2.28}{29}$. Omnes itaque valores admissibiles ipsius x erunt -1, 0, 1, $2, 3$, 4. Pro $x = -1$ debet esse $2y$ aequalis alicui numerorum 5, 6, $7 \ldots 33$, atque $5y$ alicui horum -2, -1, 0, $1 \ldots 26$; hinc valor minimus ipsius y est $+3$, maximus $+5$. Tractando perinde valores reliquos ipsius x, oritur sequens sehema omnium residuorum minimorum:

x	y
-1	3, 4, 5
0	0, 1, 2, 3, 4, 5
$+1$	1, 2, 3, 4, 5, 6
$+2$	1, 2, 3, 4, 5, 6
$+3$	2, 3, 4, 5, 6
$+4$	2, 3, 4

Simili modo pro residuis absolute minimis, ξ et η alicui numerorum -14, -13, $-12 \ldots +14$ aequales esse debent; hinc $29x$ nequit esse extra limites -7.14 et $+7.14$, adeoque x alicui numerorum -3, -2, -1, 0, 1, 2, 3 aequalis esse debet. Pro $x = -3$ erit $2y = \xi - 5x = \xi + 15$ alicui numerorum 1, 2, $3 \ldots 29$ aequalis, $5y = \eta + 2x = \eta - 6$ autem alicui horum -20, -19, $-18 \ldots +8$: hinc prodit pro y valor unicus $+1$. Tractando eodem modo valores reliquos ipsius x, habemus schema omnium residuorum absolute minimorum:

x	y
-3	$+1$
-2	-2, -1, 0, $+1$, $+2$
-1	-3, -2, -1, 0, $+1$, $+2$
0	-2, -1, 0, $+1$, $+2$
$+1$	-2, -1, 0, $+1$, $+2$, $+3$
$+2$	-2, -1, 0, $+1$, $+2$,
$+3$	-1

45.

In applicatione methodi secundae duos casus distinguere conveniet.s

In casu priori, ubi a et b divisorem communem non habent, fiat $\alpha a + \beta b = 1$, sitque k residuum minimum positivum ipsius $\beta a - \alpha b$ secundum modulum p. Hinc aequationes identicae

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b), \quad b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b)$$

docent, esse $ak \equiv -b$, $bk \equiv a \pmod{p}$. Statuendo itaque ut supra $ax + by = \xi$,$ay - bx = \eta$, erit $\eta \equiv k\xi$, $\xi \equiv -k\eta \pmod{p}$. Omnes itaque numeri $\xi + \eta i$, quibus

residua simpliciter minima $x+yi$ respondent, habebuntur, dum vel pro ξ deinceps accipiuntur valores 0, 1, 2, $3 \ldots p-1$, et pro η residua minima positiva productorum $k\xi$ secundum modulum p, vel ordine alio pro η illi valores et pro ξ residua minima productorum $-k\eta$. E singulis $\xi+\eta i$ dein respondentes $x+yi$ invenientur per formulam

$$x+yi = \tfrac{\xi+\eta i}{a-bi} = \tfrac{a\xi-b\eta}{p} + \tfrac{a\eta+b\xi}{p} \cdot i$$

Ceterum obvium est, η, dum ξ unitate crescat, vel augmentum k vel decrementum $p-k$ pati, adeoque $x+yi$

$$\text{vel mutationem } \tfrac{a-kb}{p} + \tfrac{ak+b}{p} \cdot i \text{ vel hanc } \tfrac{a-kb}{p} + b + (\tfrac{ak+b}{p} - a)i$$

quae observatio ad constructionem faciliorem reddendam inservit.

Denique patet, si residua absolute minima $x+yi$ desiderentur, haec praecepta eatenus tantum mutari, quatenus ipsi ξ deinceps tribuendi sint valores inter limites $-\frac{1}{2}p$ et $+\frac{1}{2}p$, dum pro η accipere oporteat residua absolute minima productorum $k\xi$. Ecce conspectum residuorum minimorum pro modulo $5+2i$ hoc modo adornatorum:

Residua simpliciter minima.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
0	0	$10+25i$	$+5i$	$20+21i$	$+2+5i$
$1+17i$	$-1+3i$	$11+13i$	$+1+3i$	$21+9i$	$+3+3i$
$2+5i$	$+i$	$12+i$	$+2+i$	$22+26i$	$+2+6i$
$3+22i$	$+1+4i$	$13+18i$	$+1+4i$	$23+14i$	$+3+4i$
$4+10i$	$+2i$	$14+6i$	$+2+2i$	$24+2i$	$+4+2i$
$5+27i$	$-1+5i$	$15+23i$	$+1+5i$	$25+19i$	$+3+5i$
$6+15i$	$+3i$	$16+11i$	$+2+3i$	$26+7i$	$+4+3i$
$7+3i$	$+1+i$	$17+28i$	$+1+6i$	$27+24i$	$+3+6i$
$8+20i$	$+4i$	$18+16i$	$+2+4i$	$28+12i$	$+4+4i$
$9+8i$	$+1+2i$	$19+4i$	$+3+2i$		

Residua absolute minima.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
$-14-6i$	$-2-2i$	$-4-10i$	$-2i$	$+5-2i$	$+1$
$-13+11i$	$-3+i$	$-3+7i$	$-1+i$	$+6-14i$	$+2-2i$
$-12-i$	$-2-i$	$-2-5$	$-i$	$+7+3i$	$+1+i$
$-11-13i$	$-1-3i$	$-1+12i$	$-1+2i$	$+8-9i$	$+2-i$
$-10+4i$	-2	0	0	$+9+8i$	$+1+2i$
$-9-8i$	$-1-2i$	$+1-12i$	$+1-2i$	$+10-4i$	$+2$
$-8+9i$	$-2+i$	$+2+5i$	$+i$	$+11+13i$	$+1+3i$
$-7-3i$	$-1-i$	$+3-7i$	$+1-i$	$+12+i$	$+2+i$
$-6+14i$	$-2+2i$	$+4+10i$	$+2i$	$+13-11i$	$+3-i$
$-5+2i$	-1			$+14+6i$	$+2+2i$

Casum secundum, ubi a, b non sunt inter se primi, facile ad casum praecedentem reducere licet. Sit λ divisor communis maximus numerorum a, b, atque $a=\lambda a'$, $b=\lambda b'$. Denotet F indefinite residuum minimum pro modulo λ, quatenus tamquam numerus complexus consideratur, i.e. exhibeat indefinite numerum talem $x+yi$, ut x, y sint vel inter limites 0 et λ, vel inter hos $-\frac{1}{2}\lambda$ et $+\frac{1}{2}\lambda$ (prout de residuis vel simpliciter vel absolute minimis agitur): denotet porro F' indefinite residuum minimum pro modulo $a'+b'i$. Tunc erit $(a'+b'i)F+F'$ indefinite residuum minimum pro modulo $a+bi$, prodibitque systema completum horum residuorum, dum omnia F cum omnibus F' combinantur.

46.

Duo numeri complexi inter se primi dicuntur, si praeter unitates alios divisores communes non admittunt: quoties autem tales divisores communes adsunt, ii divisores communes maximi vocantur, quorum norma maxima est.

Si duorum numerorum propositorum resolutio in factores primos praesto est, determinatio divisoris communis maximi prorsus eodem modo perficitur, ut pro numeris realibus (*Disquiss. Ar.* art. 18). Simul hinc elucet, omnes divisores communes duorum numerorum datorum metiri debere eorundem divisorem communem maximum hoc modo inventum. Quare quum sponte iam pateat, ternos numeros huic socios etiam esse divisores communes, semper quaterni numeri, et non plures, divisores

communes maximi appellandi erunt, horumque norma erit multiplum normae cuiusvis alius divisoris communis.

Si resolutio duorum numerorum propositorum in factores simplices non adest, divisor communis maximus adiumento similis algorithmi eruitur, ut pro numeris realibus. Sint m, m' duo numeri propositi, formeturque per divisionem repetitam series m'', m''' etc. ita, ut m'' sit residuum absolute minimum ipsius m secundum modulum m', dein m'' residuum absolute minimum ipsius m' secundum modulum m'' et sic porro. Denotando normas numerorum m, m', m'', m''' etc. resp. per p, p', p'', p''' etc., erit $\frac{p''}{p'}$ norma quotientis $\frac{m''}{m'}$, adeoque per definitionem residui absolute minimi certo non maior quam $\frac{1}{2}$; idem valet de $\frac{p'''}{p''}$ etc. Quapropter integri reales positivi p', p'', p''' etc. seriem continuo decrescentem formabunt, unde necessario tandem ad terminum 0 pervenietur, sive, quod idem est, in serie m, m', m'', m'' etc. tandem ad terminum perveniemus, qui praecedentem absque residuo metitur. Sit hic $m^{(n+1)}$, statuamusque

$$m = km' + m''$$
$$m' = k'm'' + m'''$$
$$m'' = k''m''' + m''''$$

etc. usque ad

$$m^{(n)} = k^{(n)} m^{(n+1)}$$

Percurrendo has aequationes ordine inverso, elucet, $m^{(n+1)}$ singulos terminos praecedentes $m^{(n)} \dots m''$, m', m metiri; percurrendo autem easdem aequationes ordine directo, manifestum est, quemvis divisorem communem numerorum m, m etiam metiri singulos sequentes. Conclusio prior docet, $m^{(n+1)}$ esse divisorem communem numerorum m, m'; posterior autem, hunc divisorem esse maximum.

Ceterum quoties residuum ultimum $m^{(n+1)}$ alicui quatuor unitatum 1, -1, i, $-i$ aequale evadit, hoc indicium erit, m et m' inter se primos esse.

47.

Si aequationes art. praec., omissa ultima, ita combinantur, ut m'', m''', $m'''' \dots m^{(n)}$ eliminentur, orietur aequatio talis

$$m^{(n+1)} = hm + h'm'$$

ubi h, h' erunt integri, et quidem, si designatione in *Disquiss. Ar.* art. 27 introducta

uti placet

$$h = \pm \left[k', k'', k''' \dots k^{(n-1)}\right] = \pm \left[k^{(n-1)}, k^{(n-2)} \dots k'', k'\right]$$
$$h' = \mp \left[k, k', k'', k''' \dots k^{(n-1)}\right] = \mp \left[k^{(n-1)}, k^{n-2)} \dots k'', k', k\right]$$

valentibus signis superioribus vel inferioribus, prout n par est vel impar. Hoc theorema ita enunciamus:

Divisor communis maximus duorum numerorum complexorum m, m' redigi potest ad formam $hm + h'm'$, ita ut h, h' sint integri.

Manifesto enim hoc non solum de eo divisore communi maximo valet, ad quem algorithmus art. praec. deduxit, sed etiam de tribus illi associatis, pro quibus loco coëfficientium h, h' accipere oportebit vel hos hi, $h'i$ vel $-h$, $-h'$, vel $-hi$, $-h'i$.

Quoties itaque numeri m, m' inter se primi sunt, satisfieri poterit aequationi

$$1 = hm + h'm'$$

Propositi sint e.g. numeri $31 + 6i = m$, $11 - 20i = m'$. Hic invenimus

$$\begin{array}{llll} k & = & i, & m'' = +11 - 5i \\ k' & = +1 - i, & m''' & = + \ 5 - 4i \\ k'' & = +2, & m'''' & = + \ 1 + 3i \\ k''' & = -1 - 2i, & m''''' & = \quad + i \\ k'''' & = +3 - i & & \end{array}$$

atque hinc

$$\left[k', k'', k'''\right] = -6 - 5i$$
$$\left[k, k', k'', k'''\right] = +4 - 10i$$

et proin

$$m''''' = i = (6 + 5i)m + (4 - 10i)m'$$

nec non

$$1 = (5 - 6i)m + (-10 - 4i)m'$$

quod calculo instituto confirmatur.

48.

Per praecedentia omnia, quae ad theoriam congruentiarum primi gradus in arithmetica numerorum complexorum requiruntur, praeparata sunt: sed quum illaessentialiter non differat ab ea, quae pro arithmetica numerorum realium locum

habet, atque in *Disquisitionibus Arithmeticis* copiose exposita est, praecipua momenta hic adscripsisse sufficiet.

I. Congruentia $mt \equiv 1 \pmod{m'}$ aequivalet aequationi indeterminatae $mt + m'u = 1$, et si huic satisfit per valores $t = h, u = h'$, illius solutio generaliter exhibetur per $t \equiv h \pmod{m'}$: conditio autem solubilitatis est, ut modulus m' cum coëfficiente m divisorem communem non habeat.

II. Solutio congruentiae $ax + b \equiv c \pmod{M}$ in casu eo, ubi a, M sunt inter se primi, pendet a solutione huius

$$at \equiv 1 \pmod{M}$$

cui si satisfacit $t = h$, illius solutio generalis continetur in formula

$$x \equiv (c - b)h \pmod{M}$$

III. Congruentia $ax + b \equiv c \pmod{M}$ in casu eo, ubi a, M divisorem communem λ habent, aequivalet huic

$$\tfrac{a}{\lambda} \cdot x \equiv \tfrac{c-b}{\lambda} \pmod{\tfrac{M}{\lambda}}$$

Dum itaque pro λ adoptatur divisor communis maximus numerorum a, M, solutio congruentiae propositae ad casum praecedentem reducitur, patetque, ad resolubilitatem requiri et sufficere, ut λ etiam differentiam $c - b$ metiatur.

49.

Hactenus elementaria tantum attigimus, quae tamen nexus caussa omittere non licuit. In disquisitionibus altioribus arithmetica numerorum complexorum arithmeticae realium in eo similis est, quod theoremata elegantiora et simpliciora prodeunt, dum tales modulos, qui sunt numeri primi, solos admittimus: revera illorum extensio ad modulos compositos plerumque prolixior quam difficilior est, et laboris potius quam artis. Quapropter in sequentibus imprimis de modulis primis agetur.

50.

Denotante X functionem indeterminatae x talem

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \text{etc.} + Mx + N$$

ubi n est integer realis positivus, A, B, C etc. integri reales vel imaginarii, m autem

integer complexus: vocabimus hic quoque *radicem* congruentiae $X \equiv 0 \pmod{m}$ quemlibet integrum, qui pro x substitutus ipsi X valorem per modulum m divisibilem conciliat. Solutiones per radices secundum modulum congruas non spectabimus tamquam diversas.

Quoties modulus est numerus primus, talis congruentia ordinis n hic quoque plures quam n solutiones diversas admittere non potest. Denotante α integrum quemvis determinatum (complexum), X adiumento divisionis per $x - \alpha$ indefinite ad formam $X = (x-\alpha)X' + h$ reduci potest, ita ut h fiat integer determinatus atque X' functio ordinis $n-1$ cum coëfficientibus integris. Iam quoties α est radix congruentiae $X \equiv 0 \pmod{m}$, manifesto h divisibilis erit per m, sive habebitur indefinite $X \equiv (x-\alpha)X' \pmod{m}$.

Perinde si denotante β integrum determinatum, X' ad formam $(x-\beta)X'' + h'$ reducitur, X'' erit functio ordinis $n-2$ cum coëfficientibus integris. Si vero β supponitur esse radix congruentiae $X \equiv 0$, etiam satisfacere debet huic $(\beta-\alpha)X' \equiv 0$, nec non huic $X' \equiv 0$, siquidem radices α, β sunt incongruae, unde colligimus, etiam h' per m divisibilem esse debere, sive indefinite $X \equiv (x-\alpha)(x-\beta)X'' \pmod{m}$.

Simili modo accedente radice tertia γ prioribus incongrua, habebimus indefinite $X \equiv (x-\alpha)(x-\beta)(x-\gamma)X'''$, ita ut X''' sit functio ordinis $n-3$ cum coëfficientibus integris. Eodem modo ulterius procedere licet, patetque simul, coëfficientem termini altissimi in singulis functionibus esse $= A$, quem per m non divisibilem esse supponere licet, alioquin enim congruentia $X \equiv 0$ essentialiter ad ordinem inferiorem referenda esset. Quoties itaque adsunt n radices incongruae, puta $\alpha, \beta, \gamma \ldots \nu$, habebimus indefinite

$$X \equiv A(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\nu) \pmod{m}$$

quapropter substitutio novi valoris singulis $\alpha, \beta, \gamma \ldots \nu$ incongrui certo ipsi X valorem per m non divisibilem conciliaret, unde theorematis veritas sponte sequitur.

Ceterum haec demonstratio essentialiter convenit cum ea, quam in *Disq. Ar.* art. 43 tradidimus, et cuius singula momenta pro numeris complexis perinde valent ac pro realibus.

51.

Quae in Sectione tertia *Disquisitionum Arithmeticarum* circa residua potestatum tradita sunt, ad maximam partem, levibus mutationibus adhibitis, etiam in arithmetica numerorum complexorum valent: quinadeo demonstrationes theorematum plerumque retineri possent. Ne tamen quid desit, theoremata principalia demonstrationibus concisis firmata proferemus, ubi semper subintelligendum est, modulum esse numerum primum.

THEOREMA. *Denotante k integrum per modulum m, cuius norma $= p$, non divisibilem, erit $k^{p-1} \equiv 1 \,(mod.\, m)$.*

Demonstr. Constituant a, b, c etc. systema completum residuorum incongruorum pro modulo m, ita tamen, ut residuum per m divisibile omissum sit, adeoque multitudo illorum numerorum, quorum complexum denotamus per C, sit $= p-1$. Sit porro C' complexus productorum ka, kb, kc etc. Ex his productis per hyp. nullum erit divisibile per m, quare singula habebunt residua congrua in complexu C, puta fieri poterit $ak \equiv a'$, $bk \equiv b'$, $ck \equiv c'$ etc. (mod. m), ita ut numeri a', b', c' etc. ipsi in complexu C inveniantur: denotemus complexum numerorum a', b', c' etc. per C''. Sint P, P', P'' producta e singulis numeris complexuum C, C', C'' resp., sive

$$P = abc \ldots$$
$$P' = k^{p-1}abc \ldots = k^{p-1}P$$
$$P'' = a'b'c' \ldots$$

Quum numeri complexus C'' deinceps congrui sint numeris complexus C', erit $P'' \equiv P'$ sive $P'' \equiv k^{p-1}P$. At quum facile perspiciatur, binos quosvis numeros complexus C'' inter se incongruos, adeoque omnes inter se diversos esse, necessario numeri complexus C'' cum numeris complexus C prorsus conveniunt, ordine tantummodo mutato, unde fit $P'' = P$. Erit itaque $(k^{p-1} - 1)P$ numerus per m divisibilis, unde, quum m sit numerus primus singulos factores ipsius P non metiens, necessario $k^{p-1} - 1$ per m divisibilis esse debebit. Q. E. D.

52.

THEOREMA. *Denotante k, ut in art. praec., integrum per modulum m non divisibilem, atque t exponentem minimum (praeter 0), pro quo $k^t \equiv 1 \,(mod.\, m)$, erit t divisor cuiusvis alius exponentis u, pro quo $k^u \equiv 1 \,(mod.\, m)$.*

Demonstr. Si t non esset divisor ipsius u, sit gt multiplum ipsius u proxime maius quam u, adeoque $gt-u$ integer positivus minor quam t. Ex $k^t \equiv 1$, $k^u \equiv 1$, sequitur $0 \equiv k^{gt} - k^u \equiv k^u(k^{gt-u} - 1)$, adeoque $k^{gt-u} \equiv 1$, i.e. datur potestas ipsius k cum exponente minori quam t unitati congrua, contra hyp.

Tamquam corollarium hinc sequitur, t certo metiri numerum $p-1$.

Numeros tales k, pro quibus $t = p-1$, etiam hic *radices primitivas* pro modulo m vocabimus: quales revera adesse iam ostendemus.

53.

Resolvatur numerus $p-1$ in factores suos primos, ita ut habeatur

$$p - 1 = a^\alpha b^\beta c^\gamma \dots$$

designantibus a, b, c etc. numeros primos reales positivos inaequales. Sint A, B, C etc. integri (complexi) per m non divisibiles, atque resp. congruentiis

$$x^{\frac{p-1}{a}} \equiv 1, x^{\frac{p-1}{b}} \equiv 1, x^{\frac{p-1}{c}} \equiv 1 \text{ etc.}$$

secundum modulum m non satisfacientes, quales dari e theoremate art. 50 manifestum est. Denique sit h congruus secundum modulum m producto

$$A^{\frac{p-1}{a^\alpha}} B^{\frac{p-1}{b^\beta}} C^{\frac{p-1}{c^\gamma}} \dots$$

Tunc dico, h fore radicem primitivam.

Demonstr. Denotando per t exponentem infimae potestatis h^t unitati congruae, erit, si h non esset radix primitiva, t submultiplum ipsius $p-1$, sive $\frac{p-1}{t}$ integer unitate maior. Manifesto hic integer factores suos primos reales inter hos a, b, c etc. habebit: supponamus itaque, (quod licet), $\frac{p-1}{t}$ esse divisibilem per a, statuamusque $p-1 = atu$. Erit itaque, propter $h^t \equiv 1$, etiam $h^{tu} \equiv 1$ sive

$$A^{\frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} C^{\frac{p-1}{a^\gamma} \cdot \frac{p-1}{a}} \dots \equiv 1$$

At manifesto $\frac{p-1}{ab^\beta}$ est integer, adeoque

$$B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} = \left(B^{p-1}\right)^{\frac{p-1}{ab^\beta}} \equiv 1$$

perinde etiam

$$C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \equiv 1, \text{ et sic porro; quapropter esse debet } A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$$

Iam determinetur integer positivus λ talis, ut fiat

$$\lambda b^\beta c^\gamma \ldots \equiv 1 \pmod{a}$$

quod fieri poterit, quum numerus primus a ipsum $b^\beta c^\gamma \ldots$ non metiatur, statuaturque $\lambda b^\beta c^\gamma \ldots = 1 + a\mu$. Manifesto fit

$$A^{\lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1, \text{ sive, quoniam } \lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a} = (1+a\mu)\frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}$$

habemus $A^{(p-1)\mu}\cdot A^{\frac{p-1}{a}} \equiv 1$, atque hinc, quum sponte sit $A^{(p-1)\mu} \equiv 1$, etiam $A^{\frac{p-1}{a}} \equiv 1$, quod est contra hypothesin. Suppositio itaque, t esse submultiplum ipsius $p-1$, consistere nequit, eritque adeo necessario h radix primitiva.

54.

Denotante h radicem primitivam pro modulo m, cuius norma $= p$, termini progressionis

$$1, h, hh, h^3 \ldots h^{p-2}$$

inter se incongrui erunt, unde facile colligitur, quemlibet integrum non divisibilem per modulum uni ex istis congruum esse debere, sive illam seriem exhibere systema completum residuorum incongruorum exclusa cifra. Exponens eius potestatis, cui numerus datus congruus est, vocari potest huius *index*, dum h tamquam *basis* consideratur. Ecce quaedam exempla, ubi cuivis indici residuum absolute minimum apposuimus.

Exemplum primum.

$$m = 5 + 4i, \quad p = 41, \quad h = 1 + 2i$$

Ind.	Residuum	Ind.	Residuum	Ind.	Residuum	Ind.	Residuum	Ind.	Residuum
0	$+1$	8	-4	16	$-2+2i$	24	$+2i$	32	$+1+i$
1	$+1+2i$	9	$-3+i$	17	$-1+2i$	25	$-3i$	33	$+1+3i$
2	$+1-i$	10	$-i$	18	$+4i$	26	$+2+2i$	34	$+2$
3	$+3+i$	11	$+2-i$	19	$+1+3i$	27	$+2+i$	35	-3
4	$-2i$	12	$-1-i$	20	-1	28	$+4$	36	$+2-2i$
5	$+3i$	13	$+1-3i$	21	$-1-2i$	29	$+3-i$	37	$+1-2i$
6	$-2-2i$	14	-2	22	$-1+i$	30	$+i$	38	$-4i$
7	$-2-i$	15	$+3$	23	$-3-i$	31	$-2+i$	39	$-1-3i$

Exemplum secundum.

$m = 7, p = 49, h = 1 + 2i$

Ind.	Residuum	Ind.	Residuum	Ind.	Residuum	Ind.	Residuum	Ind.	Residuum
0	$+1$	10	$-1-i$	20	$+2i$	30	$+2-2i$	40	$+3$
1	$+1+2i$	11	$+1-3i$	21	$+3+2i$	31		41	$+3-i$
2	$-3-3i$	12	$-i$	22	$-1+i$	32	$+2$	42	$-2-2i$
3	$+3-2i$	13	$+2-i$	23	$-3-i$	33	$-3i$	43	$+2+i$
4	$-3i$	14	$-3+3i$	24	-1	34	$+1+i$	44	$-2i$
5	$-1-3i$	15	$-2-3i$	25	$-1-2i$	35	$-1+3i$	45	$-3-2i$
6	$-2+2i$	16	-3	26	$+3$	36		46	$+1-i$
7	$+1-2i$	17	$-3+i$	27	$-3+2i$	37	$-2+i$	47	$+3+i$
8	-2	18	$+2+2i$	28	$+3i$	38	$+3-3i$		
9	$-2+3i$	19	$-2-i$	29	$+1+3i$	39	$+2+3i$		

55.

Adiicimus circa radices primitivas et algorithmum indicum quasdam observationes, demonstrationibus propter facilitatem omissis.

I. Indices secundum modulum $p-1$ congrui in systemate dato residuis secundum modulum m congruis respondent et vice versa.

II. Residua, quae respondent indicibus ad $p-1$ primis, etiam sunt radices primitivae et vice versa.

III. Si accepta radice primitiva h pro basi, radicis alius primitivae h' index est t, et vice versa t' index ipsius h, dum h' pro basi accipitur, erit $tt' \equiv 1 \pmod{p-1}$; et si iisdem positis indices cuiusdam alius numeri in his duobus systematibus resp. sunt u, u', erit $tu' \equiv u$, $t'u \equiv u' \pmod{p-1}$.

IV. Dum numeri $1, 1+i$ eorumque terni socii (tamquam nimis ieiuni) a modulis nobis considerandis excluduntur, restant numeri primi ii, quos in art. 34 tertio et quarto loco posuimus. Posteriorum normae erunt numeri primi reales formae $4n+1$; priorum normae autem quadrata numerorum primorum realium imparium: in utroque igitur casu $p-1$ per 4 divisibilis est.

V. Denotando indicem numeri -1 per u, erit $2u \equiv 0 \pmod{p-1}$, adeoque vel $u \equiv 0$, vel $u \equiv \frac{1}{2}(p-1)$: at quum index 0 respondeat residuo $+1$, index numeri -1 necessario debet esse $\frac{1}{2}(p-1)$.

VI. Perinde denotando per u indicem numeri i, erit $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$, adeoque vel $u \equiv \frac{1}{4}(p-1)$ vel $u \equiv \frac{3}{4}(p-1)$. Sed hic ambiguitas ab electione radicis primitivae pendet. Scilicet si radice primitiva h pro basi accepta index numeri i

est $\frac{1}{4}(p-1)$, index fiet $\frac{3}{4}(p-1)$, dum pro basi accipitur h^μ, designante μ integrum positivum formae $4n+3$ ad $p-1$ primum, e.g. ipsum numerum $p-2$, et vice versa. Quare semissis altera radicum primitivarum conciliat numero i indicem $\frac{1}{4}(p-1)$, altera indicem $\frac{3}{4}(p-1)$, manifestoque pro illis basibus $-i$ indicem $\frac{3}{4}(p-1)$, pro his indicem $\frac{1}{4}(p-1)$ habebit.

VII. Quoties modulus est numerus primus realis positivus formae $4n+3$, puta $=q$, adeoque $p=qq$, indices omnium numerorum realium per $q+1$ divisibiles erunt; denotante enim t indicem numeri realis k, erit, propter $k^{q-1} \equiv 1 \pmod{q}$, $(q-1)t \equiv 0 \pmod{qq-1}$, adeoque $\frac{t}{q+1}$ integer. Perinde indices numerorum pure imaginariorum ut ki per $\frac{1}{2}(q+1)$ divisibiles erunt. Patet itaque, radices primitivas pro talibus modulis inter solos numeros mixtos quaerendas esse.

VIII. Contra pro modulo m, qui est numerus primus complexus mixtus, (cuiusque proin norma p est numerus primus realis formae $4n+1$), radices primitivae quaelibet etiam inter numeros reales eligi possunt, inter quos completum adeo systema residuorum incongruorum monstrare licet (art. 40). Manifesto autem quilibet numerus realis, qui est radix primitiva pro modulo complexo m, simul erit in arithmetica numerorum realium radix primitiva pro modulo p, et vice versa.

56.

Etiamsi theoria residuorum et non-residuorum quadraticorum in arithmetica numerorum complexorum sub ipsa theoria residuorum biquadraticorum contenta sit, tamen antequam ad hanc transeamus, illius theoremata palmaria hic seorsim proferemus: brevitatis vero caussa de solo casu principali, ubi modulus est numerus primus complexus (impar), hic loquemur.

Sit m talis modulus, atque p eius norma. Manifesto quivis integer (per m non divisibilis, quod hic semper subintelligendum) quadrato secundum modulum m congruus fieri vel potest vel non potest, prout illius index, radice aliqua primitiva pro basi accepta, par est vel impar; in casu priori ille integer residuum quadraticum ipsius m dicetur, in posteriori non-residuum. Hinc concluditur, inter $p-1$ numeros qui systema completum residuorum incongruorum (per m non divisibilium) exhibeant, semissem ad residua quadratica, semissem alteram ad non-residua quadratica referri. Cuivis vero alii numero extra illud systema idemcharacter hoc respectu tribuendus

est, quo gaudet numerus systematis illi congruus.

Porro ibinde sequitur, productum e duobus residuis quadraticis, nec non productum e duobus non-residuis esse residuum quadraticum; contra productum e residuo quadratico in non-residuum fieri non-residuum; et generaliter productum e quotcunque factoribus esse residuum quadraticum vel non-residuum, prout multitudo non-residuorum inter factores par sit vel impar.

Pro distinguendis residuis quadraticis a non-residuis statim se offert criterium generale sequens:

Numerus k per modulum non divisibilis huius residuum vel non-residuum quadraticum est, prout habetur vel $k^{\frac{1}{2}(p-1)} \equiv 1$, vel $k^{\frac{1}{2}(p-1)} \equiv -1 \pmod{m}$.

Veritas huius theorematis statim inde sequitur, quod, accepta radice primitiva quacunque pro basi, index potestatis $k^{\frac{1}{2}(p-1)}$ fit vel $\equiv 0$ vel $\equiv \frac{1}{2}(p-1)$, prout index numeri k par est vel impar.

57.

Facile quidem est, pro modulo dato systema residuorum incongruorum completum in duas classes, puta residua et non-residua quadratica distinguere, quo pacto simul omnibus reliquis numeris classes suae sponte assignantur. At longe altioris indaginis est quaestio de criteriis ad distinguendum modulos eos, pro quibus numerus datus est residuum quadraticum, ab iis, pro quibus est non-residuum.

Quod quidem attinet ad unitates reales $+1$ et -1, hae in arithmetica numerorum complexorum sunt reapse quadrata, adeoque etiam residua quadratica pro *quovis* modulo. Aeque facile e criterio art. praec. sequitur, numerum i (et perinde $-i$) esse residuum quadraticum cuiusvis moduli, cuius norma p sit formae $8n+1$, non-residuum vero cuiusvis moduli, cuius norma sit formae $8n+5$. Quum manifesto nihil intersit, utrum numerus m, an aliquis numerorum ipsi associatorum im, $-m$, $-im$ pro modulo adoptetur, supponere licebit, modulum esse associatorum primarium (art. 36, II), adeoque statuendo modulum $= a+bi$, esse a imparem, b parem. Quo pacto quum semper sit $aa \equiv 1 \pmod{8}$, bb vero vel $\equiv 0$ vel $\equiv 4 \pmod{8}$, prout b sit pariter par vel impariter par, patet numeros $+i$ et $-i$ in casu priori esse residua quadratica moduli, in posteriori nonresidua.

58.

Quum diiudicatio characteris numeri compositi, utrum sit residuum quadraticum an non-residuum, pendeat a characteribus factorum, manifesto sufficiet, si evolutionem criteriorum ad distinguendos modulos, pro quibus numerus datus k sit residuum quadraticum, ab iis, pro quibus sit non-residuum, ad tales valores ipsius k limitemus, qui sint numeri primi, insuperque inter associatos primarii. In qua investigatione *inductio* protinus theoremata maxime elegantia suppeditat.

Incipiamus a numero $1+i$, qui invenitur esse residuum quadraticum modulorum $-1+2i,\ +3-2i,\ -5-2i,\ -1-6i,\ +5+4i,\ +5-4i,\ -7,\ +7+2i,\ -5+6i,$ etc.
non-residuum quadraticum autem sequentium
$-1-2i,\ -3,\ +3+2i,\ +1+4i,\ +1-4i,\ -5+2i,\ -1+6i,\ +7-2i,\ -5-6i,\ -3+8i,$
$-3-8i,\ +5+8i,\ +5-8i,\ +9+4i,\ +9-4i$ etc.

Si hunc conspectum, in quo semper e quaternis modulis associatis primarium apposuimus, attente examinamus, facile animadvertimus, modulos $a+bi$ in priori classe omnes esse tales, pro quibus $a+b$ fiat $\equiv +1 \pmod 8$, in posteriori vero tales, pro quibus $a+b \equiv -3 \pmod 8$. Manifesto hoc criterium, si loco moduli primarii m adoptamus associatum $-m$, ita immutari debet, ut pro modulis prioris classis sit $a+b \equiv -1$, pro modulis posterioris $\equiv +3 \pmod 8$. Quare, siquidem inductio non fefellerit, generaliter, designante $a+bi$ numerum primum, in quo a impar, b par, $1+i$ fit eius residuum quadraticum vel non-residuum quadraticum, prout $a+b \equiv \pm 1$, vel $\equiv \pm 3 \pmod 8$.

Pro numero $-1-i$ eadem regula valet, quae pro $1+i$. Contra considerando $1-i$ tamquam productum ex $-i$ in $1+i$, manifestum est, numero $1-i$ eundem characterem competere, qui tribuendus sit ipsi $1+i$, quoties b sit pariter par, oppositum autem, quoties b sit impariter par, unde facile colligitur, $1-i$ esse residuum quadraticum numeri primi $a+bi$, quoties sit $a-b \equiv \pm 1$, nonresiduum autem, quoties habeatur $a-b \equiv \pm 3 \pmod 8$, semper supponendo, a esse imparem, b parem.

Ceterum haec secunda propositio e priori etiam deduci potest adiumento theorematis generalioris, quod ita enunciamus:

In theoria residuorum quadraticorum character numeri $\alpha+\beta i$ respectu moduli $a+bi$ idem est, qui numeri $\alpha-\beta i$ respectu moduli $a-bi$.

Demonstratio huius theorematis inde petitur, quod uterque modulus eandem normam p habet, atque quoties $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ per $a+bi$ divisibilis est, etiam $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ per $a-bi$ divisibilis evadit, quoties autem $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ per $a+bi$ divisibilis est, etiam $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ per $a-bi$ divisibilis esse debet.

59.

Progrediamur ad numeros primos impares.

Numerum $-1+2i$ invenimus esse residuum quadraticum modulorum $+3+2i$, $+1-4i$, $-5+2i$, $-5-2i$, $-1-6i$, $+7-2i$, $-3+8i$, $+5+8i$, $+5-8i$, $+9+4i$ etc.

non-residuum autem modulorum $-1-2i$, -3, $+3-2i$, $+1+4i$, $-1+6i$, $+5+4i$, $+5-4i$, -7, $+7+2i$, $-5+6i$, $-5-6i$, $-3-8i$, $+9-4i$ etc.

Reducendo modulos prioris classis ad residua eorum absolute minima secundum modulum $-1+2i$, haec sola invenimus $+1$ et -1, puta $+3+2i\equiv-1$, $+1-4i\equiv-1$, $-5+2i\equiv+1$, $-5-2i\equiv-1$ etc.

Contra omnes moduli posterioris classis congrui inveniuntur secundum modulum $-1+2i$ vel ipsi $+i$, vel ipsi $-i$.

At numeri $+1$, -1 ipsi sunt residua quadratica moduli $-1+2i$, atque $+i$ et $-i$ eiusdem non-residua: quocirca, quatenus inductioni fidem habere licet, prodit theorema: Numerus $-1+2i$ est residuum vel non-residuum quadraticum numeri primi $a+bi$, prout hic est residuum vel non-residuum quadraticum ipsius $-1+2i$, siquidem $a+bi$ est primarius e quaternis associatis, vel potius, si a est impar, b par.

Ceterum ex hoc theoremate sponte sequuntur theoremata analoga circa numeros $+1-2i$, $-1-2i$, $+1+2i$.

60.

Instituendo similem inductionem circa numerum -3 vel $+3$, invenimus, utrumque esse residuum quadraticum modulorum $+3+2i$, $+3-2i$,$-1+6i$, $-1-6i$, -7, $-5+6i$,

$-5-6i$, $-3+8i$, $-3-8i$, $+9+4i$, $+9-4i$ etc.

non-residuum vero horum $-1+2i$, $-1-2i$, $+1+4i$, $+1-4i$, $-5+2i$, $-5-2i$, $+5+4i$, $+5-4i$, $+7+2i$, $+7-2i$, $+5+8i$, $+5-8i$ etc.

Priores secundum modulum 3 congrui sunt alicui ex his quatuor numeris $+1$, -1, $+i$, $-i$; posteriores autem alicui ex his $+1+i$, $+1-i$, $-1+i$, $-1-i$. Illi sunt ipsa residua quadratica numeri 3, hi non-residua.

Docet itaque haec inductio, numerum primum $a+bi$, supponendo a imparem, b parem, ad numerum -3 (nec non ad $+3$) eandem relationem habere, quam hic habet ad illum, quatenus scilicet alter alterius residuum quadraticum sit aut non-residuum.

Extendendo similem inductionem ad alios numeros primos, ubique hanc elegantissimam reciprocitatis legem confirmatam invenimus, deferimurque ad theorema hocce fundamentale circa residua quadratica in arithmetica numerorum complexorum

Denotantibus $a+bi$, $A+Bi$ numeros primos tales, ut a, A sint impares, b, B pares: erit vel uterque alterius residuum quadraticum, vel uterque alterius nonresiduum.

At non obstante summa theorematis simplicitate, ipsius demonstratio magnis difficultatibus premitur, quibus tamen hic non immoramur, quum theorema ipsum sit tantummodo casus specialis theorematis generalioris, summam theoriae residuorum biquadraticorum quasi exhaurientis. Ad hanc igitur iam transeamus.

61.

Quae in art. 2 prioris commentationis de notione residui et non-residui biquadratici prolata sunt, etiam ad arithmeticam numerorum complexorum extendimus, et perinde ut illic etiam hic disquisitionem ad modulos tales, qui sunt numeri primi, restringimus: simul plerumque tacite subintelligendum erit, modulum ita accipi, ut sit inter associatos primarius, puta $\equiv 1$ secundum modulum $2+2i$, nec non numeros, de quorum charactere (quatenus sint residua biquadratica vel non-residua) agitur, per modulum non esse divisibiles.

Pro modulo itaque dato numeri per eum non divisibiles in tres classes dispertiri possent, quarum prima contineret residua biquadratica, secunda non-residua biquadratica ea, quae sunt residua quadratica, tertia non-residua quadratica.

Sed hic quoque praestat, loco tertiae classis binas stabilire, ut omnino habeantur quaternae.

Assumta radice quacunque primitiva pro basi, residua biquadratica habebunt indices per 4 divisibiles sive formae $4n$; non-residua ea, quae sunt residua quadratica, habebunt indices formae $4n+2$; denique non-residuorum quadraticorum indices erunt partim formae $4n+1$, partim formae $4n+3$. Hoc modo classes quaternae quidem oriuntur, at distinctio inter binas posteriores non esset absoluta, sed ab electione radicis primitivae pro basi assumtae dependens; facile enim perspicitur, semissem radicum primitivarum non-residuo quadratico dato conciliare indicem formae $4n+1$, semissem alteram vero indicem formae $4n+3$. Quam ambiguitatem ut tollamus, supponemus semper talem radicem primitivam adoptari, pro qua index $\frac{1}{4}(p-1)$ competat numero $+i$ (conf. art. 55, VI). Hoc pacto classificatio oritur, quam concinnius independenter a radicibus primitivis ita enunciare possumus.

Classis *prima* contineat numeros k eos, pro quibus fit $k^{\frac{1}{4}(p-1)} \equiv 1$; hi numeri sunt moduli residua biquadratica.

Classis *secunda* contineat eos, pro quibus $k^{\frac{1}{4}(p-1)} \equiv i$.

Classis *tertia* eos, pro quibus $k^{\frac{1}{4}(p-1)} \equiv -1$.

Classis *quart* denique eos, pro quibus $k^{\frac{1}{4}(p-1)} \equiv -i$.

Classis tertia comprehendet non-residua biquadratica ea, quae sunt residua quadratica; inter secundam et quartam non-residua quadratica distributa erunt.

Numeris harum classium tribuemus resp. *characteres biquadraticos* 0, 1, 2, 3. Si characterem λ numeri k secundum modulum m ita definimus, ut sit exponens eius potestatis ipsius i, cui numerus $k^{\frac{1}{2}(p-1)}$ congruus est, manifesto characteres secundum modulum 4 congrui pro aequivalentibus habendi sunt. Ceterum haec notio tantisper ad modulos eos limitatur, qui sunt numeri primi: in continuatione harum disquisitionum ostendemus, quomodo etiam modulis compositis adaptari possit.

62.

Quo facilius inductio copiosa circa numerorum characteres adstrui possit, tabulam compendiosam hic adiungimus, cuius auxilio character cuiusvis numeri propositi respectu moduli, cuius norma valorem 157 non transscendit, levi opera obtinetur, dummodo ad observationes sequentes attendatur.

Quum character numeri compositi aequalis sit (sive secundum modulum 4 congruus) aggregato characterum singulorum factorum, sufficit, si pro modulo dato characteres numerorum primorum assignare possumus. Porro quum characteres unitatum -1, i, $-i$ manifesto sint congrui numeris $\frac{1}{2}(p-1)$, $\frac{1}{4}(p-1)$, $\frac{3}{4}(p-1)$ secundum modulum 4, etiam sufficiet, characteres numerorum inter associatos primariorum exhibuisse. Denique quam moduli secundum modulum m congrui eundem characterem habeant, sufficit, characteres talium numerorum in tabulam recipere, qui continentur in systemate residuorum absolute minimorum. Praeterea per ratiocinium simile ut in art. 58 demonstratur, si pro modulo $a+bi$ character numeri $A+Bi$ sit λ, pro modulo $a-bi$ autem λ' sit character numeri $A-Bi$, semper esse $\lambda \equiv -\lambda' \pmod 4$, sive $\lambda+\lambda'$ per 4 divisibilem: quapropter sufficit, in tabulam recipere modulos, in quibus b est vel 0 vel positivus.

Ita e.g. si quaeritur character numeri $11-6i$ respectu moduli $-5-6i$, substituimus loco horum numerorum hosce $11+6i$, $-5+6i$; dein determinamus (art. 43) residuum absolute minimum numeri $11+6i$ secundum modulum $-5+6i$, quod fit $-1-4i = -1 \times (1+4i)$; quare quum pro modulo $-5+6i$ character ipsius -1 sit 30, character numeri $1+4i$ autem, ex tabula, 2, erit 32 sive 0 character numeri $11+6i$ pro modulo $-5+6i$, et proin per observationem ultimam etiam character numeri $11-6i$ pro modulo $-5-6i$. Perinde si quaeritur character numeri $-5+6i$ respectu moduli $11+6i$, illius residuum absolute minimum $1-5i$ resolvitur in factores $-i$, $1+i$, $3-2i$, quibus respondent characteres 117, 0, 1, unde character quaesitus erit 118 sive 2; idem character etiam numero $-5-6i$ respectu moduli $11-6i$ tribuendus est.

Modulus.	Character.	Numeri.
-3	3	$1+i$
$+3+2i$	3	$1+i$
$+1+4i$	1	$-1+2i$
	3	$1+i$
$-5+2i$	0	$-1-2i$
	1	$1+i$
	2	$-1+2i$
$-1+6i$	0	-3
	1	$1+i$, $-1+2i$

Modulus.	Character.	Numeri.
$-1+6i$	2	$-1-2i$
$+5+4i$	0	$1+i$
	1	-3
	3	$-1+2i,\ -1-2i$
-7	0	-3
	1	$-1+2i,\ -3-2i$
	2	$1+i$
	3	$-1-2i$
$+7+2i$	0	$1+i,\ 3+2i,\ 3-2i,\ 1-4i$
	1	-3
	2	$-1-2i,\ 1+4i$
	3	$-1+2i$
$-5+6i$	0	$1+i,\ -3,\ 3+2i,\ 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\ -1-2i$
$-3+8i$	0	$-1+2i,\ 3-2i,\ 1-4i$
	1	$1+i,\ 3+2i$
	2	-3
	3	$-1-2i,\ 1+4i,\ -5+2i$
$+5+8i$	0	$-1-2i$
	1	$-5-2i,\ -1+6i$
	2	$-1+2i,\ 3-2i$
	3	$1+i,\ -3,\ 3+2i,\ 1+4i,\ 1-4i$
$+9+4i$	0	$-1+2i,\ 3+2i$
	1	$1+i,\ -1-2i,\ 3-2i$
	2	$-3,\ 1+4i$
	3	$1-4i,\ -5+2i$
$-1+10i$	0	$1+i,\ -1+2i,\ -1-2i,\ 3+2i$
	1	-3
	2	$3-2i,\ -5+2i,\ 5-4i$
	3	$1+4i,\ 1-4i$

Modulus.	Character.	Numeri.
$+3+10i$	1	$1+i,\ -1-2i,\ 1-4i$
	2	$-3,\ 3+2i,\ 1+4i,\ -5-2i$
	3	$-1+2i,\ 3-2i$
$-7+8i$	0	$1+i,\ -7$
	1	$3+2i,\ 3-2i,\ 1-4i,\ -5-2i$
	2	$-1-2i,\ 1+4i,\ -5+2i,\ -1-6i$
	3	$-1+2i,\ -3,\ -1+6i$
-11	0	-3
	1	$1+i,\ 3-2i,\ 1+4i,\ -5+2i,\ 5+4i$
	2	$-1+2i,\ -1-2i$
	3	$3+2i,\ 1-4i,\ -5-2i,\ 5-4i$
$-11+4i$	0	$1+i,\ -1+2i,\ 3+2i,\ 5+4i$
	1	$-1-2i,\ -1+6i$
	2	$-5+2i$
	3	$-3,\ 3-2i,\ 1+4i,\ 1-4i,\ -5-2i$
$+7+10i$	0	$1+4i,\ 1-4i,\ -1+6i,\ -1-6i$
	1	$-1+2i,\ 3+2i,\ -5+2i$
	2	$1+i,\ 3-2i$
	3	$-1-2i,\ -3,\ -5-2i$
$+11+6i$	0	$1+i,\ -1+2i,\ -3,\ 1+4i,\ 1-4i,\ -7$
	1	$-1-2i,\ 3+2i,\ 3-2i$
	2	$-5-2i,\ -1+6i,\ -5-4i$
	3	$-5+2i,\ 5+4i,\ 7-2i$

63.

Operam nunc dabimus, ut criteria communia modulorum, pro quibus numerus primus datus characterem eundem habet, per inductionem detegamus. Modulos semper supponimus primarios inter associatos, puta tales $a+bi$, pro quibus vel $a \equiv 1$, $b \equiv 0$, vel $a \equiv 3,\ b \equiv 2 \pmod 4$.

Respectu numeri $1+i$, a quo initium facimus, inductionis lex facilius arripitur, si modulos prioris generis (pro quibus $a \equiv 1,\ b \equiv 0$) a modulis posterioris generis (pro quibus $a \equiv 3,\ b \equiv 2$) separamus. Adiumento tabulae art. praec. invenimus respondere

characterem	modulis primi generis.
0	$5+4i,\ -7+8i,\ -7-8i,\ -11+4i$
1	$1-4i,\ -3+8i,\ -3-8i,\ 9+4i,\ -11$
2	$5-4i,\ -7,\ -11-4i$
3	$-3,\ 1+4i,\ 5+8i,\ 5-8i,\ 9-4i$

Si haec septemdecim exempla attente consideramus, in omnibus invenimus characterem $\equiv \frac{1}{4}(a-b-1) \pmod 4$.

Perinde respondet

character	modulis secundi generis.
0	$3-2i,\ -1-6i,\ 7+2i,\ -5+6i,\ -1+10i,\ 11+6i$
1	$-5+2i,\ -1+6i,\ 7-2i,\ -1-10i,\ 3+10i$
2	$-1+2i,\ -5-2i,\ 3-10i,\ 7+10i$
3	$-1-2i,\ 3+2i,\ -5-6i,\ 7-10i,\ 11-6i$

In omnibus his viginti exemplis, levi attentione adhibita, invenitur character $\equiv \frac{1}{4}(a-b-5) \pmod 4$.

Facile has duas regulas in unam pro utroque modulorum genere valentem contrahere licet, si perpendimus, $\frac{1}{4}bb$ esse pro modulis prioris generis $\equiv 0$, pro modulis posterioris generis $\equiv 1 \pmod 4$. Est itaque character numeri $1+i$ respectu moduli cuiusvis primi inter associatos primarii $\equiv \frac{1}{4}(a-b-1-bb) \pmod 4$.

Obiter hic annotare convenit, quum $(b+1)^2$ semper sit formae $8n+1$, sive $\frac{1}{4}(2b+bb)$ par, characterem istum semper parem vel imparem fieri, prout $\frac{1}{4}(a+b-1)$ par sit vel impar, quod quadrat cum regula pro charactere quadratico in art. 58 prolata.

Quum $\frac{1}{4}(a-b-1)$, $\frac{1}{4}(a-b+3)$ sint integri, quorum alter par, alter impar, ipsorum productum par erit, sive $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod 4$. Hinc loco expressionis allatae pro charactere biquadratico haec quoque adoptari potest

$$\tfrac{1}{4}(a-b-1-bb) - \tfrac{1}{8}(a-b-1)(a-b+3) = \tfrac{1}{8}(-aa+2ab-3bb+1)$$

quae forma eo quoque nomine se commendat, quod non restringitur ad modulos primarios, sed tantummodo supponit; a esse imparem, b parem: manifesto enim in hac suppositione vel $a+bi$, vel $-a-bi$ erit numerus inter associatos primarius, valorque istius formulae pro utroque modulo idem.

64.

Proficiscendo a regula ultima in art. praec. eruta invenimus esse

numeri	characterem $\equiv$
$-1+i$	$\frac{1}{8}(aa+2ab-bb-1)$
$-1-i$	$\frac{1}{8}(-aa+2ab+bb+1)$
$+1-i$	$\frac{1}{8}(aa+2ab+3bb-1)$

Hoc statim inde sequitur, quod character ipsius i est $\frac{1}{4}(aa+bb-1)$, character ipsius -1 autem $\frac{1}{2}(aa+bb-1) \equiv \frac{1}{2}bb$, quum $aa-1$ semper sit formae $8n$. Manifesto hae quatuor regulae, etiamsi hactenus ab inductione mutuatae sint, ita inter se sunt nexae, ut quamprimum unius demonstratio absoluta fuerit, tres reliquae simul sint demonstratae. Vix opus est monere, etiam in his regulis tantummodo supponi a imparem, b parem.

Si formulas ad modulos primarios restrictas adhibere non displicet, hac forma uti possumus. Est

numeri	characterem $\equiv$
$-1+i$	$\frac{1}{4}(-a-b+1-bb)$
$-1-i$	$\frac{1}{4}(a-b-1+bb)$
$+1-i$	$\frac{1}{4}(-a-b+1+bb)$

Formulae simplicissimae prodeunt, si, ut initio inductionis nostrae feceramus, modulos primi et secundi generis distinguimus. Est scilicet character

numeri	pro modulis primi generis	pro modulis secundi generis
$-1+i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b-3)$
$-1-i$	$\frac{1}{4}(a-b-1)$	$\frac{1}{4}(a-b+3)$
$+1-i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b+5)$

65.

Pro numero $-1+2i$, ad quem iam progredimur, eandem distinctionem inter modulos $a+bi$ eos, pro quibus $a \equiv 1$, $b \equiv 0$, atque eos, pro quibus $a \equiv 3$, $b \equiv 2$ quoque adhibebimus. Tabula art. 62 docet, respectu illius numeri respondere

characterem	modulis primi generis
0	$-3+8i,\ +5-8i,\ +9+4i,\ -11+4i$
1	$+1+4i,\ +5-4i,\ -7,\ -3-8i$
2	$+1-4i,\ +5+8i,\ -7-8i,\ -11$
3	$-3,\ +5+4i,\ +9-4i,\ -7+8i,\ -11-4i$

Revocatis singulis his modulis ad residua absolute minima secundum modulum $-1+2i$, animadvertimus, omnes, quibus respondet character 0, esse $\equiv 1$; eos, quibus character 1 respondet, $\equiv i$; eos, quorum character est 2, fieri $\equiv -1$; denique omnes, quorum character est 3, fieri $\equiv -i$. At characteres numerorum 1, i, -1, $-i$ pro modulo $-1+2i$ ipsi sunt 0, 1, 2, 3 resp.; quapropter in omnibus his 17 exemplis character numeri $-1+2i$ respectu moduli prioris generis $a+bi$, cum charactere huius numeri respectu moduli $-1+2i$ identicus est.

Perinde adiumento tabulae invenitur, respondere

characterem	modulis secundi generis
0	$+3+2i,\ -5-2i,\ -1+10i,\ -1-10i,\ +11+6i$
1	$+3-2i,\ -1+6i,\ -5-6i,\ +7+10i,\ +7-10i$
2	$-5+2i,\ -1-6i,\ +7-2i$
3	$-1-2i,\ +7+2i,\ -5+6i,\ +3+10i,\ +3-10i,\ +11-6i$

Revocatis his modulis ad residua minima secundum modulum $-1+2i$, omnia, quibus resp. characteres 0, 1, 2, 3 respondent, congrua inveniuntur numeris -1, $-i$, $+1$, $+i$; his vero ipsis numeris, si vice versa $-1+2i$ pro modulo adoptatur, competunt characteres 2, 3, 0, 1 resp. Quapropter in omnibus his 19 exemplis character numeri $-1+2i$ respectu moduli secundi generis duabus unitatibus differt a charactere huius numeri respectu numeri $-1+2i$ pro modulo habiti.

Ceterum nullo negotio perspicitur, prorsus similia respectu numeri $-1-2i$ locum habitura esse.

66.

Pro numero -3 distinctionem inter modulos primi generis et secundi omittimus, quum eventus doceat, illam hic superfluam esse. Respondet itaque

character	modulis
0	$-1+6i,\ -1-6i,\ -7,\ -5+6i,\ -5-6i,\ -11,\ 11+6i,\ 11-6i$
1	$-1-2i,\ 1-4i,\ -5+2i,\ 5+4i,\ 7+2i,\ 5-8i,\ -1+10i,\ -7-8i,$ $-11-4i,\ 7-10i$
2	$3+2i,\ 3-2i,\ -3+8i,\ -3-8i,\ 9+4i,\ 3+10i,\ 3-10i$
3	$-1+2i,\ 1+4i,\ -5-2i,\ 5-4i,\ 7-2i,\ 5+8i,\ -1-10i,\ -7+8i,$ $-11+4i,\ 7+10i$

Revocatis his modulis ad residua minima secundum modulum 3, videmus, eos, quibus respondet character 0, esse partim $\equiv 1$, partim $\equiv -1$; eos, quorum character est 1, fieri vel $\equiv 1-i$, vel $\equiv -1+i$: eos, quorum character est 2, fieri vel $\equiv i$, vel $\equiv -i$; denique eos, quibus competit character 3, esse vel $\equiv 1+i$, vel $\equiv -1-i$. Ex hac itaque inductione colligimus, characterem numeri -3 pro modulo, qui est numerus primus inter associatos primarius, identicum esse cum charactere huius ipsius numeri, dum 3, sive, quod eodem redit, -3 tamquam modulus consideratur.

67.

Simili inductione circa alios numeros primos instituta, invenimus, numeros $3 \pm 2i$, $-1 \pm 6i$, $7 \pm 2i$, $-5 \pm 6i$ etc. suppeditare theoremata ei similia, ad quod in art. 65 respectu numeri $-1+2i$ pervenimus; contra numeros $1 \pm 4i$, $5 \pm 4i$, $-3 \pm 8i$, $5 \pm 8i$, $9 \pm 4i$ etc. perinde se habere ut numerum -3. Inductio itaque perducit ad elegantissimum theorema, quod ad instar theoriae residuorum quadraticorum in arithmetica numerorum realium THEOREMA FUNDAMENTALE theoriae residuorum biquadraticorum nuncupare liceat, scilicet:

Denotantibus $a+bi$, $a'+b'i$ numeros primos diversos inter associatos suos primarios, i.e. secundum modulum $2+2i$ unitati congruos, character biquadraticus numeri $a+bi$ respectu moduli $a'+b'i$ identicus erit cum charactere numeri $a'+b'i$ respectu moduli $a+bi$, si vel uterque numerorum $a+bi$, $a'+b'i$, vel alteruter saltem, ad primum genus refertur, i.e. secundum modulum 4 unitati congruus est: contra characteres illi duabus unitatibus inter se different, si neuter numerorum $a+bi$, $a'+b'i$ ad primum genus refertur, i.e. si uterque secundum modulum 4 congruus est numero $3+2i$.

At non obstante summa huius theorematis simplicitate, ipsius demonstratio inter mysteria arithmeticae sublimioris maxime recondita referenda est, ita ut, saltem ut nunc res est, per subtilissimas tantummodo investigationes enodari possit, quae limites praesentis commentationis longe transgrederentur. Quamobrem promulgationem huius demonstrationis, nec non evolutionem nexus inter hoc theorema atque ea, quae in initio huius commentationis per inductionem stabilire coeperamus, ad commentationem tertiam nobis reservamus. Coronidis tamen loco iam hic trademus, quae ad demonstrationem theorematum in artt. 63, 64 propositorum requiruntur.

68.

Initium facimus a numeris primis $a+bi$ talibus, pro quibus $b=0$ (tertia specie art. 34), ubi itaque (ut numerus inter associatos primarius sit) a debet esse numerus primus realis negativus formae $-(4n+3)$, pro quo scribemus $-q$, quales sunt -3, -7, -11, -19 etc. Denotando per λ characterem numeri $1+i$, illo numero pro modulo accepto, esse debet

$$i^{\lambda} \equiv (1+i)^{\frac{1}{4}(qq-1)} \equiv 2^{\frac{1}{8}(qq-1)} \cdot i^{\frac{1}{8}(qq-1)} \pmod{q}$$

Sed constat, 2 esse residuum quadraticum, vel non-residuum quadraticum ipsius q, prout q sit formae $8n+7$, vel formae $8n+3$, unde colligimus, esse generaliter

$$2^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{4}(q+1)} \equiv i^{\frac{1}{2}(q+1)} \pmod{q}$$

adeoque evehendo ad potestatem exponentis $\frac{1}{4}(q+1)$

$$2^{\frac{1}{8}(qq-1)} \equiv i^{\frac{1}{8}(q+1)^2} \pmod{q}$$

Aequatio itaque praecedens hanc formam induit

$$i^{\lambda} \equiv i^{\frac{1}{8}(q+1)^2+\frac{1}{8}(qq-1)} \equiv i^{\frac{1}{4}(qq+q)} \pmod{q}$$

unde sequitur

$$\lambda \equiv \tfrac{1}{4}(qq+q) \equiv \tfrac{1}{4}(q+1)^2 - \tfrac{1}{4}(q+1) \pmod{4}$$

sive quum habeatur $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$, $\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(a-1) \pmod{4}$. Quod est ipsum theorema art. 63 pro casu $b=0$.

69.

Longe vero difficilius absolvuntur moduli $a+bi$ tales, pro quibus non est $b=0$ (numeri quartae speciei art. 34), pluresque disquisitiones erunt praemittendae. Normam $aa+bb$, quae erit numerus primus realis formae $4n+1$, designabimus per p.

Denotetur per S complexus omnium residuorum simpliciter minimorum pro modulo $a+bi=m$, exclusa cifra, ita ut multitudo numerorum in S contentorum sit $=p-1$. Designet $x+yi$ indefinite numerum huius systematis, statuaturque $ax+by=\xi$, $ay-bx=\eta$. Erunt itaque ξ, η integri inter limites 0 et p *exclusive* contenti: in casu praesente enim, ubi a, b inter se primi sunt, formulae art. 45, puta $\eta \equiv k\xi$, $\xi \equiv -k\eta \pmod{p}$ docent, neutrum numerorum ξ, η esse posse $=0$, nisi alter simul evanescat, adeoque fiat $x=0$, $y=0$, quam combinationem iam eiecimus. Criterium itaque numeri $x+yi$ in S contenti, consistit in eo, ut quatuor numeri ξ, η, $p-\xi$, $p-\eta$ sint positivi.

Praeterea observamus pro nullo tali numero esse posse $\xi=\eta$; hinc enim sequeretur $p(x+y)=a(\xi+\eta)+b(\xi-\eta)=2a\xi$, quod est absurdum, quum nullus factorum 2, a, ξ per p divisibilis sit. Simili ratione aequatio $p(x-y+a+b)=2a\xi+(a+b)(p-\xi-\eta)$ docet, esse non posse $\xi+\eta=p$. Quapropter quum numeri $\xi-\eta$, $p-\xi-\eta$ esse debeant vel positivi vel negativi, hinc petimus subdivisionem systematis S in quatuor complexus C, C', C'', C''', puta ut coniiciantur

in complexum	numeri pro quibus
C	$\xi-\eta$ positivus, $p-\xi-\eta$ positivus
C'	$\xi-\eta$ positivus, $p-\xi-\eta$ negativus
C''	$\xi-\eta$ negativus, $p-\xi-\eta$ negativus
C'''	$\xi-\eta$ negativus, $p-\xi-\eta$ positivus

Criterium itaque numeri complexus C proprie sextuplex est, puta sex numeri ξ, η, $p-\xi$, $p-\eta$, $\xi-\eta$, $p-\xi-\eta$ positivi esse debent; sed manifesto conditiones 2, 5 et 6 iam sponte implicant reliquas. Similia circa complexus C', C'', C''' valent, ita ut criteria completa sint triplicia, puta

pro complexu	positivi esse debent numeri		
C	$\eta,$	$\xi-\eta,$	$p-\xi-\eta$
C'	$p-\xi$	$\xi-\eta,$	$\xi+\eta-p$
C''	$p-\eta$	$\eta-\xi,$	$\xi+\eta-p$
C'''	$\xi,$	$\eta-\xi,$	$p-\xi-\eta$

Ceterum vel nobis non monentibus quisque facile intelliget, in repraesentatione figurata numerorum complexorum (vid. art. 39) numeros systematis S intra quadratum contineri, cuius latera iungant puncta numeros 0, $a+bi$, $(1+i)(a+bi)$, $i(a+bi)$ repraesentantia, et subdivisionem systematis S respondere partitioni quadrati per rectas diagonales. Sed hocce loco ratiocinationibus pure arithmeticis uti maluimus, illustrationem per intuitionem figuratam lectori perito brevitatis caussa linquentes.

70.

Si quatuor numeri complexi $r=x+yi$, $r'=x'+y'i$, $r''=x''+y''i$, $r'''=x'''+y'''i$ ita inter se nexi sunt, ut habeatur $r'=m+ir$, $r''=m+ir'=(1+i)m-r$, $r'''=m+ir''=im-ir$, atque primus r ad complexum C pertinere supponitur, reliqui r', r'', r''' resp. ad complexus C', C'', C''' pertinebunt. Statuendo enim $\xi=ax+by$, $\eta=ay-bx$, $\xi'=ax'+by'$, $\eta'=ay'-bx'$, $\xi''=ax''+by''$, $\eta''=ay''-bx''$, $\xi'''=ax'''+by'''$, $\eta'''=ay'''-bx'''$, invenitur

$$\eta=p-\xi'=p-\eta''=\xi'''$$
$$\xi-\eta=\xi'+\eta'-p=\eta''-\xi''=p-\xi'''-\eta'''$$
$$p-\xi-\eta=\xi'-\eta'=\xi''+\eta''-p=\eta'''-\xi'''$$

unde adiumento criteriorum theorematis veritas sponte demanat. Et quum rursus fiat $r=m+ir'''$, facile perspicietur, si r supponatur pertinere ad C', numeros r', r'', r''' pertinere resp. ad C'', C''', C; si ille ad C'', hos ad C''', C, C'; denique si ille ad C''', hos ad C, C', C''.

Simul hinc colligitur, in singulis complexibus C, C', C'', C''' aeque multos numeros reperiri, puta $\frac{1}{4}(p-1)$.

71.

THEOREMA. *Si denotante k integrum per m non divisibilem singuli numeri complexus C per k multiplicantur, productorumque residuis simpliciter minimis secundum modulum m inter complexus C, C', C'', C''' distributis, multitudo eorum,*

quae ad singulos hos complexus pertinent, resp. per c, c′, c″, c‴ denotatur: character numeri k respectu moduli m erit $\equiv c' + 2c'' + 3c'''$ *(mod.* 4*).*

Demonstr. Sint illa c residua minima ad C pertinentia α, β, γ, δ etc.; dein c' residua ad C' pertinentia haec $m+i\alpha'$, $m+i\beta'$, $m+i\gamma'$, $m+i\delta'$ etc.; porro c'' residua ad C'' pertinentia haec $(1+i)m-\alpha''$, $(1+i)m-\beta''$, $(1+i)m-\gamma''$, $(1+i)m-\delta''$ etc.; denique c''' residua ad C''' pertinentia haec $im-i\alpha'''$, $im-i\beta'''$, $im-i\gamma'''$, $im-i\delta'''$ etc. Iam consideremus quatuor producta, scilicet

1) productum ex omnibus $\frac{1}{4}(p-1)$ numeris complexum C constituentibus:
2) productum productorum, quae e multiplicatione singulorum horum numerorum per k orta erant;
3) productum e residuis minimis horum productorum, puta e numeris α, β, γ, δ etc., $m+i\alpha'$, $m+i\beta'$ etc. etc.
4) productum ex omnibus $c+c'+c''+c'''$ numeris α, β, γ, δ etc., α', β', γ', δ' etc., α'', β'', γ'', δ'' etc., α''', β''', γ''', δ''' etc.

Denotando haec quatuor producta ordine suo per P, P', P'', P''', manifesto erit

$$P' = k^{\frac{1}{4}(p-1)}P, \quad P' \equiv P'', \quad P'' \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

et proin

$$Pk^{\frac{1}{4}(p-1)} \equiv P'''i^{c'+2c''+3c''} \pmod{m}$$

At facile perspicietur, numeros α', β', γ', δ' etc., α'', β'', γ'', δ'' etc., α''', β''', γ''', δ''' etc. omnes ad complexum C pertinere, atque tum inter se tum a numeris α, β, γ, δ etc. diversos esse, sicuti hi ipsi inter se diversi sint. Omnes itaque hi numeri simul sumti, et abstrahendo ab ordine, prorsus identici esse debent cum omnibus numeris complexum C constituentibus, unde colligimus $P = P'''$, adeoque

$$Pk^{\frac{1}{4}(p-1)} \equiv Pi^{c'+2c''+3c'''} \pmod{m}$$

Denique quum singuli factores producti P per m non sint divisibiles, hinc concluditur

$$k^{\frac{1}{4}(p-1)} \equiv i^{c'+2c''+3c'''} \pmod{m}$$

unde $c' + 2c'' + 3c'''$ erit character numeri k respectu moduli m. Q. E. D.

72.

Quo theorema generale art. praec. ad numerum $1+i$ applicari possit, complexum C denuo in duos complexus minores G et G' subdividere oportet, et quidem referemus in complexum G numeros eos $x+yi$, pro quibus $ax+by=\xi$ minor est quam $\frac{1}{2}p$, in alterum G' eos, pro quibus ξ est maior quam $\frac{1}{2}p$; multitudinem numerorum in complexibus G, G' contentorum resp. per g, g' denotabimus, unde erit $g+g'=\frac{1}{4}(p-1)$.

Criterium completum numerorum ad G pertinentium itaque erit, ut tres numeri η, $\xi-\eta$, $p-2\xi$ sint positivi: nam conditio tertia pro complexu C, secundum quam $p-\xi-\eta$ positivus esse debet, sub illis implicite iam continetur, quum sit $p-\xi-\eta=(\xi-\eta)+(p-2\xi)$. Perinde criterium completum numerorum ad G' pertinentium consistet in valoribus positivis trium numerorum η, $p-\xi-\eta$, $2\xi-p$.

Hinc facile concluditur, productum cuiusvis numeri complexus G per numerum $1+i$ pertinere ad complexum C'''; si enim statuitur

$$(x+yi)(1+i)=x'+y'i, \text{ atque } ax'+by'=\xi', ay'-bx'=\eta', \text{ invenitur}$$
$$\xi'=\xi-\eta, \eta'-\xi'=2\eta, p-\xi'-\eta'=p-2\xi$$

i.e. criterium pro numero $x+yi$ complexui G subdito identicum est cum criterio pro numero $x'+y'i$ ad complexum C''' pertinente.

Prorsus simili modo ostenditur, productum cuiusvis numeri complexus G' per $1+i$ pertinere ad complexum C''.

Erit itaque, si in art. praec. ipsi k valorem $1+i$ tribuimus, $c=0$, $c'=0$, $c''=g'$, $c'''=g$, et proin character numeri $1+i$ fiet $3g+2g'=\frac{1}{2}(p-1)+g$. Et quum characteres numerorum i, -1, sint $\frac{1}{4}(p-1)$, $\frac{1}{2}(p-1)$, characteres numerorum $-1+i$, $-1-i$, $1-i$ resp. erunt $\frac{3}{4}(p-1)+g$, g, $\frac{1}{4}(p-1)+g$. Totus igitur rei cardo iam in investigatione numeri g vertitur.

73.

Quae in artt. 69-72 exposuimus, proprie independentia sunt a suppositione, m esse numerum primarium: abhinc vero saltem supponemus, a imparem, b parem esse, praetereaque a, b et $a-b$ esse numeros positivos. Ante omnia limites valorum ipsius x in complexu G stabilire oportet.

Statuendo $ay - bx = \eta$, $(a+b)x - (a-b)y = \zeta$, $p - 2ax - 2by = \theta$, criterium numerorum $x + yi$ ad complexum G pertinentium consistit in tribus conditionibus, ut η, ζ, θ sint numeri positivi. Quum fiat $px = (a-b)\eta + a\zeta$, $p(a-2x) = a\theta + 2b\eta$, manifestum est, x et $2a - x$ esse debere numeros positivos, sive x alicui numerorum 1, 2, $3 \ldots \frac{1}{2}(a-1)$ aequalem. Porro quum sit $(a-b)\theta = 2b\zeta + p(a-b-2x)$, patet, quamdiu x minor sit quam $\frac{1}{2}(a-b)$, conditionem secundam (iuxta quam ζ positivus esse debet) iam implicare tertiam (quod θ debet esse positivus); contra quoties x sit maior quam $\frac{1}{2}(a-b)$, conditionem secundam iam contineri sub tertia. Quamobrem pro valoribus ipsius x his 1, 2, $3 \ldots \frac{1}{2}(a-b-1)$ tantummodo prospiciendum est, ut η et ζ positivi evadant, sive ut y maior sit quam $\frac{bx}{a}$ et minor quam $\frac{(a+b)x}{a-b}$: pro valore itaque tali dato ipsius x aderunt numeri $x + yi$ omnino

$$\left[\tfrac{(a+b)x}{a-b}\right] - \left[\tfrac{bx}{a}\right]$$

si uncis in eadem significatione utimur, qua iam alibi passim usi sumus (Conf. *Theorematis arithm. dem. nova* art. 4 et *Theorematis fund. in doctr. de residuis quadr. etc. Algorithm. nov.* art. 3). Contra pro valoribus ipsius x his $\frac{1}{2}(a-b+1)$, $\frac{1}{2}(a-b+3) \ldots \frac{1}{2}(a-1)$ sufficiet, ut ipsis η et θ valores positivi concilientur, sive ut y maior sit quam $\frac{bx}{a}$ et minor quam $\frac{p-2ax}{2b}$ sive $\frac{1}{2}b + \frac{aa-2ax}{2b}$: quare pro valore tali dato ipsius x aderunt numeri $x + yi$ omnino

$$\left[\tfrac{1}{2}b + \tfrac{aa-2ax}{2b}\right] - \left[\tfrac{bx}{a}\right]$$

Hinc itaque colligimus, multitudinem numerorum complexus G esse

$$g = \Sigma\left[\tfrac{(a+b)x}{a-b}\right] + \Sigma\left[\tfrac{1}{2}b + \tfrac{aa-2ax}{2b}\right] - \Sigma\left[\tfrac{bx}{a}\right]$$

ubi in termino primo summatio extendenda est per omnes valores integros ipsius x ab 1 usque ad $\frac{1}{2}(a-b-1)$, in secundo ab $\frac{1}{2}(a-b+1)$ usque ad $\frac{1}{2}(a-1)$, in tertio ab 1 usque ad $\frac{1}{2}(a-1)$.

Si characteristica φ in eadem significatione utimur, ut loco citato (*Theorematis fund.* etc. *Algor. nov.* art. 3), puta ut sit

$$\varphi(t,u) = \left[\tfrac{u}{t}\right] + \left[\tfrac{2u}{t}\right] + \left[\tfrac{3u}{t}\right] \ldots + \left[\tfrac{t'u}{t}\right]$$

denotantibus t, u numeros positivos quoscunque, atque t' numerum $\left[\frac{1}{2}t\right]$, terminus ille primus fit $= \varphi(a-b, a+b)$, tertius $= -\varphi(a,b)$; secundus vero fit

$$= \tfrac{1}{4}bb + \sum \left[\tfrac{aa-2ax}{2b}\right]$$

Sed fit, scribendo terminos inverso ordine,

$$\Sigma \left[\tfrac{aa-2ax}{2b}\right] = \left[\tfrac{a}{2b}\right] + \left[\tfrac{3a}{2b}\right] + \left[\tfrac{5a}{2b}\right] + \ldots + \left[\tfrac{(b-1)a}{2b}\right] = \varphi(2b,a) - \varphi(b,a)$$

Formula itaque nostra sequentem induit formam:

$$g = \varphi(a-b,a+b) + \varphi(2b.a) - \varphi(a,b) - \varphi(b,a) + \tfrac{1}{4}bb$$

Consideremus primo terminum $\varphi(a-b,a+b)$, qui protinus transmutatur in $\varphi(a-b,2b) + 1 + 2 + 3 + \text{etc.} + \tfrac{1}{2}(a-b-1)$ sive in

$$\varphi(a-b,2b) + \tfrac{1}{8}((a-b)^2 - 1)$$

Dein quum per theorema generale fiat $\varphi(t,u) + \varphi(u,t) = \left[\tfrac{1}{2}t\right] \cdot \left[\tfrac{1}{2}u\right]$, dum t,u sunt integri positivi inter se primi, habemus

$$\varphi(a-b,2b) = \tfrac{1}{2}b(a-b-1) - \varphi(2b,a-b)$$

adeoque

$$\varphi(a-b,a+b) = \tfrac{1}{8}(aa + 2ab - 3bb - 4b - 1) - \varphi(2b,a-b)$$

Disponamus partes ipsius $\varphi(2b,a-b)$ sequenti modo

$$\begin{aligned} &\left[\tfrac{a-b}{2b}\right] + \left[\tfrac{3(a-b)}{2b}\right] + \left[\tfrac{5(a-b)}{2b}\right] + \text{etc.} + \left[\tfrac{(b-1)(a-b)}{2b}\right] \\ +&\left[\tfrac{a-b}{b}\right] + \left[\tfrac{2(a-b)}{b}\right] + \left[\tfrac{3(a-b)}{b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}b(a-b)}{b}\right] \end{aligned}$$

Series secunda manifesto fit

$$= \varphi(b,a-b) = \varphi(b,a) - 1 - 2 - 3 - \text{etc.} - \tfrac{1}{2}b = \varphi(b,a) - \tfrac{1}{8}(bb+2b)d$$

seriem primam ordine terminorum inverso ita exhibemus:

$$\left[\tfrac{1}{2}(a+1-b) - \tfrac{a}{2b}\right] + \left[\tfrac{1}{2}(a+3-b) - \tfrac{3a}{2b}\right] + \left[\tfrac{1}{2}(a+5-b) - \tfrac{5a}{2b}\right] + \text{etc.} + \left[\tfrac{1}{2}(a-1) - \tfrac{(b-1)a}{2b}\right]$$

quae expressio, quum denotante t numerum integrum, u fractum, generaliter sit $[t-u] = t-1-[u]$, mutatur in sequentem

$$\begin{aligned} &\tfrac{1}{8}b(2a-4-b) - \left[\tfrac{a}{2b}\right] - \left[\tfrac{3a}{2b}\right] - \left[\tfrac{5a}{2b}\right] - \text{etc.} - \left[\tfrac{(b-1)a}{2b}\right] \\ =&\tfrac{1}{8}b(2a-4-b) - \varphi(2b,a) + \varphi(b,a) \end{aligned}$$

Hinc fit

$$\varphi(2b, a-b) = 2\varphi(b,a) - \varphi(2b,a) + \tfrac{1}{4}b(a-3-b)$$

et proin

$$\varphi(a-b, a+b) = \varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}(aa - bb + 2b - 1)$$

Substituendo hunc valorem in formula pro g supra tradita, insuperque $\varphi(a,b) + \varphi(b,a) = \tfrac{1}{4}b(a-1)$, obtinemus

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}(aa - 2ab + bb + 4b - 1)$$

74.

Per ratiocinia prorsus similia absolvitur casus is, ubi manentibus a, b positivis $a-b$ est negativus sive $b-a$ positivus. Aequationes $p(a-2x) = 2b\eta + a\theta$, $p(b-a+2x) = 2b\zeta + (b-a)\theta$ docent, $\tfrac{1}{2}a - x$ atque $x + \tfrac{1}{2}(b-a)$ positivos, et proin x alicui numerorum $-\tfrac{1}{2}(b-a-1)$, $-\tfrac{1}{2}(b-a-3)$, $-\tfrac{1}{2}(b-a-5) \ldots + \tfrac{1}{2}(a-1)$ aequalem esse debere. Porro ex aequatione $px + (b-a)\eta = a\zeta$ sequitur, pro valoribus negativis ipsius x conditionem, ex qua η debet esse positivus, iam contineri sub conditione, ex qua ζ debet esse positivus, contrarium vero evenire, quoties ipsi x valor positivus tribuatur. Hinc valores ipsius y pro valore determinato negativo ipsius x inter $\frac{(a+b)x}{a-b}$ et $\frac{p-2ax}{2b}$, contra pro valore positivo ipsius x inter $\frac{bx}{a}$ et $\frac{p-2ax}{2b}$ contenti esse debent: manifesto pro $x = 0$ hi limites sunt 0 et $\frac{p-2ax}{2b}$, valore $y = 0$ ipso excluso. Hinc colligitur

$$g = -\sum \left[\tfrac{(a+b)x}{a-b}\right] + \sum \left[\tfrac{1}{2}b + \tfrac{aa-2ax}{2b}\right] - \sum \left[\tfrac{bx}{a}\right]$$

ubi in termino primo summatio extendenda est per omnes valores negativos ipsius x inde a -1 usque ad $-\tfrac{1}{2}(b-a-1)$; in secunda per omnes valores ipsius x inde a $-\tfrac{1}{2}(b-a-1)$ usque ad $\tfrac{1}{2}(a-1)$; in tertia per omnes valores positivos ipsius x inde a $+1$ usque ad $\tfrac{1}{2}(a-1)$: hoc pacto e summatione prima prodit $-\varphi(b-a, b+a)$, e secunda perinde ut in art. praec. $\tfrac{1}{4}bb + \varphi(2b,a) - \varphi(b,a)$, denique e tertia $-\varphi(a,b)$, sive habetur

$$g = -\varphi(b-a, b+a) + \varphi(2b,a) - \varphi(b,a) - \varphi(a,b) + \tfrac{1}{4}bb$$

Iam simili modo ut in art. praec. evolvitur

$$\varphi(b-a,b+a) = \varphi(b-a,2b) - \tfrac{1}{8}((b-a)^2-1)$$
$$= \tfrac{1}{8}(3bb-2ab-aa-4b+1) - \varphi(2b,b-a)$$

nec non

$$\varphi(2b,b-a) = \varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{4}b(b-1-a)$$

adeoque

$$\varphi(b-a,b+a) = 2\varphi(b,a) - \varphi(2b,a) + \tfrac{1}{8}(bb-aa-2b+1)$$

tandemque

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}(aa-2ab+bb+4b-1)$$

Evictum est itaque, eandem formulam pro g valere, sive sit $a-b$ positivus sive negativus, dummodo a, b sint positivi.

75.

Ut reductionem ulteriorem assequamur, statuemus

$$L = \left[\tfrac{a}{2b}\right] + \left[\tfrac{2a}{2b}\right] + \left[\tfrac{3a}{2b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}ba}{2b}\right]$$
$$M = \left[\tfrac{(\frac{1}{2}b+1)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+2)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+3)a}{2b}\right] + \text{etc.} + \left[\tfrac{ba}{2b}\right]$$
$$N = \left[\tfrac{a+b}{2b}\right] + \left[\tfrac{2a+b}{2b}\right] + \left[\tfrac{3a+b}{2b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}ba+b}{2b}\right]$$

Quum facile perspiciatur, haberi generaliter $[u] + \left[u+\frac{1}{2}\right] = [2u]$, quamcunque quantitatem realem denotet u, fit $L+N = \varphi(b,a)$, et quum manifesto sit $L+M = \varphi(2b,a)$, erit

$$\varphi(2b,a) - \varphi(b,a) = M - N$$

Porro autem obvium est, aggregatum termini primi seriei N cum penultimo termino seriei M, puta $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right]$ fieri $= \frac{1}{2}(a-1)$, atque eandem summam effici e termino secundo seriei N cum antepenultimo seriei M, et sic porro: quare quum etiam terminus ultimus seriei M fiat $= \frac{1}{2}(a-1)$, ultimus vero terminus seriei N sit $= \left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$, valente signo superiori vel inferiori, prout a est formae $4n+1$ vel $4n-1$: erit

$$M + N = \tfrac{1}{4}(a-1)b + \tfrac{1}{4}(a \mp 1)$$

et proin

$$\varphi(2b,a) - \varphi(b,a) = \tfrac{1}{4}(a-1)b + \tfrac{1}{4}(a \mp 1) - 2N$$

Formula itaque pro g in artt. 73 et 74 inventa, transit in sequentem

$$g = \tfrac{1}{8}((a+b)^2 - 1) + 2n - 4N$$

statuendo $a \mp 1 = 4n$, ubi n erit integer. Sed quum hinc habeatur $1 = 16nn - 8an + aa$, formula haec etiam sequenti modo exhiberi potest:

$$g = \tfrac{1}{8}(-aa + 2ab + bb + 1) + 4(\tfrac{1}{2}(a+1)n - nn - N)$$

Quapropter quum g sit character numeri $-1-i$ pro modulo $a+bi$, hic character fit $\equiv \tfrac{1}{8}(-aa+2ab+bb+1) \pmod 4$, quod est ipsum theorema supra (art.64) per inductionem erutum, sponteque inde demanant theoremata circa characteres numerorum $1+i$, $1-i$, $-1+i$. Quamobrem haec quatuor theoremata, pro casu eo, ubi a et b sunt positivi, iam rigorose sunt demonstrata.

76.

Si manente a positivo b est negativus, statuatur $b = -b'$, ut fiat b' positivus. Quum iam evictum sit, ita pro modulo $a + b'i$ characterem numeri $-1 - i$ esse $\equiv \tfrac{1}{8}(-aa + 2ab' + b'b' + 1) \pmod 4$, character numeri $-1 + i$ pro modulo $a - b'i$ per theorema in art. 62 prolatum erit $\equiv \tfrac{1}{8}(aa - 2ab' - b'b' - 1)$, i.e. character numeri $-1 + i$ pro modulo $a + bi$ fit $\equiv \tfrac{1}{8}(aa + 2ab - bb - 1)$: hoc vero est ipsum theorema in art. 64 allatum, unde tria reliqua circa characteres numerorum $1 + i$, $1 - i$, $-1 - i$ sponte demanant. Quapropter ista theoremata etiam pro casu, ubi b negativus est, demonstrata sunt, scilicet pro omnibus casibus, ubi a est positivus.

Denique si a est negativus, statuatur $a = -a', b = -b'$. Quum itaque per iam demonstrata character numeri $1 + i$ respectu moduli $a' + b'i$ sit $\equiv \tfrac{1}{8}(-a'a' + 2a'b' - 3b'b' + 1) \pmod 4$, nihilque intersit, utrum numerum $a' + b'i$ an oppositum $-a' - b'i$ moduli loco habeamus; manifesto character numeri $1 + i$ respectu moduli $a + bi$ est $\equiv \tfrac{1}{8}(-aa + 2ab - 3bb + 1)$, et similia valent circa characteres numerorum $1 - i$, $-1 + i$, $-1 - i$.

Ex his itaque colligitur, demonstrationem theorematum circa characteres numerorum $1+i$, $1-i$, $-1+i$, $-1-i$ (artt. 63. 64) nulli amplius limitationi obnoxiam esse.