Mathem.

872 ^a/₂

Der Königl. öffentlichen Bibliothek in Dresden
durch letztwillige Verfügung
geschenkt

von

Professor Dr. Paul Hohlfeld
gest. am 21. Juli 1910 in Dresden

97776
Bibl. zu Göttingen 228

THEOREMATIS FUNDAMENTALIS
IN
DOCTRINA DE RESIDUIS
QUADRATICIS DEMONSTRATIONES

ET
AMPLIATIONES NOVAE

AUCTORE

CAROLO FRIDERICO GAUSS,

ORDINIS GUELPHORUM ATQUE ORDINIS DANNEBROG EQUITE, BRITANNIARUM HANNOVERAEQUE REGI A CONSILIIS AULAE, OBSERVATORII REGII GOTTINGENSIS DIRECTORE, ASTRONOMIAE IN UNIVERSITATE GOTTINGENSI PROFESSORE, SOCIETATUM REGIARUM GOTTINGENSIS ET LONDINENSIS, ACADEMIAE BEROLINENSIS, SOCIETATIS ITALICAE ALIARUMQUE SODALI.

GOTTINGAE

APUD HENRICUM DIETERICH.

MDCCCXVIII.

IV (1911) 3622

THEOREMATIS FUNDAMENTALIS
IN
DOCTRINA DE RESIDUIS QUADRATICIS
DEMONSTRATIONES ET AMPLIATIONES
NOVAE

AUCTORE
CAROLO FRIDERICO GAUSS
SOC. REG. SCIENT. TRADITAE 1817. FEBR. 10.

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, quam primum una inuenta est via, ut *plures* subinde patefiant ad eandem metam perducentes, aliae brevius et magis directe, aliae quasi ex obliquo et a principiis longe diversis exorssae, 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.

A 2

Etfi

Et si igitur theorema arithmeticum, de quo hic agetur, per curas anteriores, quae quatuor demonstrationes inter se prorsus diversas *) suppeditaverunt, plene absolutum videri possit, tamen denuo ad idem argumentum revertor, duasque alias demonstrationes adjungo, quae novam certe lucem huic rei affundent. Prior quidem tertiae quodammodo affinis est, quod ab eodem lemme 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 adjungitur algorithmus novus persimplex ad dijudicandum, utrum numerus integer datus, numeri primi dati residuum quadraticum sit an non residuum.

Alia adhuc affuit ratio, quae ut novas demonstrationes, novem jam abhinc annos promissas, nunc potissimum promulgarem, effecit. Scilicet quum inde ab anno 1805 theoriā 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 exhaustiunt, et in quibus mira analogia cum theorematibus ad residua quadratica pertinentibus eminet, per inductionem detecta fuerunt, quamprimum 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

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

tionibus jam 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.

Theorematibus fundamentalibus in theoria residuorum quadraticorum demonstratio quinta.

I.

In introductione jam declaravimus, demonstrationem quintam et tertiam ab eodem lemmate proficisci, quod commoditatis causa, in huius 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

$$M, 2M, 3M, 4M, \dots, \frac{1}{2}(m-1)M$$

secundum modulum m , quae partim erunt minora quam $\frac{1}{2}m$, partim majora: posteriorum multitudo sit $= n$. Tunc erit M residuum quadraticum ipsius m , vel non residuum, 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, majora 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, quam-

quamobrem cum his simul sumpta, ordine quidem mutato, identica erunt cum omnibus numeris $1, 2, 3, 4 \dots \frac{1}{2}(m-1)$. Statuendo itaque productum

$$1. 2. 3. 4. \dots \frac{1}{2}(m-1) = P$$

erit

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

adeoque

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

Porro fit, secundum modulum m ,

$$\begin{aligned} P M^{\frac{1}{2}(m-1)} &\equiv a b c d \dots \times a' b' c' d' \dots \\ &\equiv a b c d \dots \times (a'-m) (b'-m) (c'-m) (d'-m) \dots \end{aligned}$$

adeoque

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

Hinc $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, accepto signo superiori vel inferiori, prout n par est vel impar, unde adjumento 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 $M, 2M, 3M \dots \frac{1}{2}(m-1)M$ secundum modulum m , quae sunt majora quam $\frac{1}{2}m$; ac perinde N multitudo eorum e residuis minimis positivis numerorum $m, 2m, 3m \dots \frac{1}{2}(M-1)m$ secundum modulum M , quae sunt majora 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 $1, 2, 3 \dots \frac{1}{2}(m-1)$

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

per F complexum numerorum $1, 2, 3 \dots \frac{1}{2}(M-1)$

per

per F' complexum numerorum $M-1, M-2, M-3 \dots \frac{1}{2}(M+1)$.
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 $1, 2, 3 \dots \frac{1}{2}(mM-1)$

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

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 $= \xi$.
- 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.

Mani-

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. Jam patet, si omnes numeri primae classis associantur 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

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

similique ratione etiam erit

$$\xi + \gamma = \frac{1}{4}(m-1)(M-1)$$

Junctis 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:

$F', M + F', 2M + F', 3M + F' \dots \frac{1}{2}(m-1)M + F'$
unde omnium multitudo erit $= \frac{1}{4}(m-1)(M-1)$, sive habebimus

$$\xi + \delta + N = \frac{1}{4}(m-1)(M-1)$$

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

$$\gamma + \delta$$

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

Ex his quatuor aequationibus oriuntur sequentes:

$$2\alpha = \frac{1}{4} (m-1) (M-1) + n + N$$

$$2\beta = \frac{1}{4} (m-1) (M-1) + n - N$$

$$2\gamma = \frac{1}{4} (m-1) (M-1) - n + N$$

$$2\delta = \frac{1}{4} (m-1) (M-1) - n - N$$

quarum quaelibet theorematis veritatem monstrat.

3.

Quodsi jam supponimus, m et M esse numeros primos, e combinatione theorematis praecedentis cum lemmate art. 1 theoremata 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.

I.

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

DEMONSTR. Accipiat integer positivus g ita ut fiat $g^n \equiv 1 \pmod{p}$, fiataturque $g^n = 1 + hp$. Tunc erit

$$B \quad 1 + x^n$$

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

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

$$1, \alpha, \alpha\alpha, \alpha^3, \dots, \alpha^{p-2}$$

secundum modulum p sine respectu ordinis cum numeris $1, 2, 3, 4, \dots, p-1$ identici fiant. Designando porro per $f(x)$ functionem

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

patet, $f(x) - 1 - x - xx - x^3 - \text{etc.} - x^{p-1}$ 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 $f(x)$ 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.

3.

THEOREMA. Statuendo

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

erit $\xi\xi = p$ 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

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

etc. usque ad

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

primam fieri $= 0$, singulas reliquas autem per $1-x^p$ divisibiles.

Quare per $1-x^p$ etiam divisibilis erit omnium summa, quae colligitur =

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

Erit itaque haec expressio Ω etiam divisibilis per $\frac{1-x^p}{1-x}$. Jam

inter exponentes $2, 2+1, 2^2+1, 2^3+1, \dots, 2^{p-2}+1$ unus tantum erit divisibilis per p , puta $2^{\frac{1}{2}(p-1)}+1$, unde per art. praec. singulae partes expressionis Ω hae

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

excepto solo termino $f(x^{2^{\frac{1}{2}(p-1)}+1})$, 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

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

B 2

ubi

ubi signum superius vel inferius valebit, prout p est formae $4k+1$ vel formae $4k+3$. Et quum insuper $f(x^{\frac{1}{2}(p-1)+1}) - p$ divisibilis sit per $\frac{1-x}{1-x^p}$, 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

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

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.

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

$$\xi^q - (x^q - x^{q^2} + x^{q^3} - x^{q^4} + \text{etc.} - x^{q^{p-2}})$$

divisibilem fieri per q , sive formae qX , ita ut X sit functio integra ipsius x etiam respectu coefficientium 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 $q, q\alpha, q\alpha^2, q\alpha^3, \dots, q\alpha^{p-2}$ secundum modum

modulum p resp. congrui numeris $\alpha^\mu, \alpha^{\mu+1}, \alpha^{\mu+2}, \dots, \alpha^{p-2}, 1, \alpha, \alpha\alpha, \dots, \alpha^{\mu-1}$, adeoque

$$x^q = x^{\alpha^\mu}$$

$$x^{q^2} = x^{\alpha^{\mu+1}}$$

$$x^{q^3} = x^{\alpha^{\mu+2}}$$

$$x^{q^4} = x^{\alpha^{\mu+3}}$$

.

.

.

.

$$x^{q^{p-\mu-2}} = x^{\alpha^{p-2}}$$

$$x^{q^{p-\mu-1}} = x$$

$$x^{q^{p-\mu}} = x^\alpha$$

$$x^{q^{p-\mu+1}} = x^{\alpha\alpha}$$

.

.

.

.

$$x^{q^{p-2}} = x^{\alpha^{\mu-1}}$$

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

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

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

$$x^q - x^{q^2} + x^{q^3} - x^{q^4} + \text{etc.} - x^{q^{p-2}} = \gamma \xi = (1 - x^p)W$$

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

$$q \xi X$$

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

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

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

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

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

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

- I. Quoties vel uterque p , q , vel alteruter tantum est formae $4k+1$, adeoque $\delta = +1$, erit $\xi = \gamma$, 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 $\xi = -\gamma$, 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.

Algo-

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

I.

Antequam solutionem novam hujus problematis exponamus, solutionem in *Disquisitionibus Arithmeticis* traditam hic breviter repetemus, quae satis quidem expedite perficitur adjumento theorematum notorum sequentium:

- I. Relatio numeri a ad numerum b (quatenus ille hujus 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 $\alpha, \beta, \gamma, \delta$ 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 cujusvis numeri primi formae $8m + 1$ vel $8m + 7$, non residuum vero cujusvis numeri primi formae $8m + 3$ vel $8m + 5$.

Proposito itaque numero a , cujus relatio ad numerum primum b quaeritur: pro a , si major est quam b , ante omnia substituetur ejus residuum minimum positivum secundum modulum b , quo residuo in factores suos primos resoluta, 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

relatio reliquorum, per theorema fundamentale, pendet a relatione ipsius b ad singulos. Hoc itaque modo loco unius relationis numeri dati ad numerum primum b jam investigandae sunt aliquae relationes numeri b ad alios primos impares ipso b minores, quae problemata eodem modo ad minores modulos deprimuntur, manifestoque hae depressiones successivae tandem exhaustae erunt.

2.

Ut exemplo haec solutio illustretur, quaerenda sit relatio numeri 103 ad 379. Quum 103 jam 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 jam hanc analysin in synthesin transmutare placet, quaestionis decisio ad quatuordecim momenta referetur, quae complete hic apponimus, ut major 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.

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 6).
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 causa 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 $[\frac{1}{2}a] = a'$, invenire aggregatum

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

C

Sol.

Sor. Designemus brevitatis caussa hujusmodi 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 hujus propositionis ad eum quoque casum extenditur, ubi alteruter numerorum a, b est impar, uti illic jam addigitavimus. Dividatur, ad instar methodi, per quam duorum integrorum divisor communis maximus investigatur, a per b , sitque ξ quotiens atque c residuum; dein dividatur b per c et sic porro, ita ut habeantur aequationes

$$a = \xi b + c$$

$$b = \gamma c + d$$

$$c = \delta d + e$$

$$d = \varepsilon e + f \text{ etc.}$$

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

$$k = \lambda l + 1.$$

Quum manifestum habeatur

$$\left[\frac{a}{b}\right] = \left[\xi + \frac{c}{b}\right] = \xi + \left[\frac{c}{b}\right]$$

$$\left[\frac{2a}{b}\right] = \left[2\xi + \frac{2c}{b}\right] = 2\xi + \left[\frac{2c}{b}\right]$$

$$\left[\frac{3a}{b}\right] = \left[3\xi + \frac{3c}{b}\right] = 3\xi + \left[\frac{3c}{b}\right]$$

etc., erit

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

et proin

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

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

$$\varphi(b, c) = b'c' - \frac{1}{2}\gamma(c'c' + c') - \varphi(c, d)$$

$$\varphi(c, d) = c'd' - \frac{1}{2}\delta(d'd' + d') - \varphi(d, e)$$

$$\varphi(d, e) = d'e' - \frac{1}{2}\varepsilon(e'e' + e') - \varphi(e, f)$$

etc. usque ad

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

Hinc,

Hinc, quoniam manifesto est $\Phi(l, 1) = 0$, colligimus formulam
 $\Phi(a, b) = a' b' - b' c' + c' d' - d' e' + \text{etc.} \pm k' l'$
 $- \frac{1}{2} \xi(b' b' + b') + \frac{1}{2} \gamma(c' c' + c') - \frac{1}{2} \delta(d' d' + d') + \frac{1}{2} \varepsilon(e' e' + e')$
 $- \text{etc.} \mp \lambda(l' l' + l')$

4.

Facile jam ex iis, quae in demonstratione tertia exposita sunt, colligitur, relationem numeri b ad a , quoties a sit numerus primus, sponte cognosci e valore aggregati $\Phi(a, 2b)$. 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 $\Phi(a, b)$ 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 $\Phi(a, b)$ 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 $\Phi(a, b)$ est impar, non residuum vero, si $\Phi(a, b)$ est par.

Haec omnia ex art. 3 demonstrationis tertiae facillime derivantur.

5.

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

$a = 379$	$a' = 189$	$\xi = 3$
$b = 103$	$b' = 51$	$\gamma = 1$
$c = 70$	$c' = 35$	$\delta = 2$
$d = 33$	$d' = 16$	$\varepsilon = 3$
$e = 4$	$e' = 2$	

hinc $\Phi(379, 103) = 9639 - 1785 + 560 - 32$
 $- 3978 + 630 - 272 + 24$
 $= 4786$, unde 103 erit residuum quadraticum numeri 379. Si ad eundem finem aggregatum $(379, 206)$ adhibere malumus, habemus hocce paradigma:

379

379	189	
206	103	1
173	86	1
33	16	5
8	4	4

unde deducimus

$$\begin{aligned}\varphi(379, 206) &= 19467 - 8858 + 1376 - 64 \\ &\quad - 5356 + 3741 - 680 + 40 \\ &= 9666, \text{ quapropter } 103 \text{ est residuum quadraticum} \\ &\text{numeri } 379.\end{aligned}$$

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 $a = \xi b + c$, $b = \gamma c + d$, $c = \delta d + e$ etc., donec in serie numerorum a, b, c, d, e etc. ad unitatem perventum sit. Statuatur $[\frac{1}{2}a] = a'$, $[\frac{1}{2}b] = b'$, $[\frac{1}{2}c] = c'$ 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 ξ, 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 $\xi', \gamma', \delta', \varepsilon'$, 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.

Datum der Entleihung bitte hier einstempeln!

(204) TG 162/14/79		

(204) JG 162/14/79

Wash. 872 ⁰—