THEORIA
RESIDUORUM BIQUADRATICORUM

AVCTORE
CAROLO FRIDERICO GAUSS.

COMMENTATIO PRIMA

SOCIETATI REGIAE TRADITA 1825, APR. 5.

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, vt 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 vsitata ad theoriam generalem stabiliendam neutiquam sufficere, quin potius hanc necessario postulare, vt campus Arithmeticae Sublimioris infinities quasi promoueatur, quod quomodo intelligendum sit, in continuatione harum disquisitionum clarissime elucebit. Quamprimum hunc campum nouum ingressi sumus, aditus ad cognitionem theorematum simplicissimorum totam theoriam exhaurientium per inductionem statim patuit: sed ipsorum demonstrationes tam profunde latuerunt, vt 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 absoluere licuit, quae illuc viam quasi sternunt, simulque theoriae diuisionis circuli quaedam noua incrementa adiungunt.

2.

Notionem residui biquadratici in *Disquisitionibus Arithmeticis* p. 113 introduximus: scilicet numerus integer a, positiuus seu negatiuus, 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, vbi contrarium expressis verbis non monetur, modulum p esse numerum primum (imparem positiuum) supponemus, atque a per p non diuisibilem, 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 conuertere licet, quoties p est numerus primus formae $4n+3$. Nam si in hoc casu a est residuum quadraticum ipsius p, statuamus $a \equiv bb$ (mod. p), vbi b vel residuum quadraticum ipsius p erit vel non-residuum: in casu priori statuemus $b \equiv cc$, vnde $a \equiv c^4$, i. e. a erit residuum biquadraticum ipsius p; in casu posteriori $-b$ fiet residuum quadraticum ipsius p (quoniam -1 est non-residuum cuiusuis numeri primi formae $4n + 3$), faciendoque $-b \equiv cc$, erit vt antea $a \equiv c^4$, atque a residuum biquadraticum ipsius p. Simul facile perspicietur, alias solutiones congruentiae $x^4 \equiv a$ (mod. 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, siue hanc ad modulos primos formae $4n + 1$ limitabimus.

4.

Existente itaque p numero primo formae $4n + 1$, propositionem art. praec. conuertere non licet: nempe exstare possunt residua quadratica, quae non sunt simul residua biquadratica, quod euenit, quoties residuum quadraticum congruum est quadrato non-residui quadratici. Statuendo enim $a \equiv bb$, existente b non-residuo quadratico ipsius p, si congruentiae $x^4 \equiv a$ satisfieri posset, per valorem $x \equiv c$, foret $c^4 \equiv bb$, siue productum $(cc - b)(cc + b)$ per p diuisibile, vnde p vel factorem $cc - b$ vel alterum $cc + b$ metiri deberet, i. e. vel $+b$ vel $-b$ foret residuum quadraticum ipsius p, et proin vterque (quoniam -1 est residuum quadraticum), contra hyp:

Omnes itaque numeri integri per p non diuisibiles 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 $1, 2, 3 \ldots\ldots p - 1$ 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 positiuorum e productis eA secundum modulum p oriundorum, et perinde C, D resp. complexus residuorum minimorum positiuorum e productis eeA, e^3A secundum modulum p prodeuntium. His ita factis facile perspicitur, singulos numeros B inter se diuersos 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 vt certe complexus A, C nullum numerum cum complexu B vel D communem habere possint. Sed etiam neque A cum C, neque B cum D vllum numerum communem habere potest. Supponamus enim

I. numerum aliquem ex A, e. g. a etiam in C inueniri, vbi 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, vt fiat $\Theta\alpha' \equiv 1$. His ita factis erit

$$ee\alpha'^4 \equiv \alpha^4, \text{ adeoque multiplicando per } \Theta^4,$$

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

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 $ea \equiv e^3a'$ sequaeretur $a \equiv eea'$, adeoque haberetur numerus, qui e producto eea' oriundus ad C simulque ad A pertineret, quod impossibile esse modo demonstrauimus.

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 inuenitur.

II. Residuum quadraticum h, (ipso p minus), quod simul est non residuum biquadraticum, statuatur $\equiv gg$, vbi g erit non-residuum quadraticum. Accipiatur integer γ talis, vt 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 inueniatur 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, vt habeatur $eg \equiv h$. Erit itaque g residuum quadraticum, et proin vel in A vel in C contentus: in casu priori h manifesto inter numeros B, in posteriori autem inter numeros D inuenietur.

Ex his omnibus colligitur, cunctos numeros $1, 2, 3 \ldots p-1$ inter quatuor series A, B, C, D ita distribui, vt quiuis illorum in vna harum reperiatur, vnde 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, $-1 \equiv ff$ (mod. p), vnde 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 $\alpha, f\alpha, -\alpha, -f\alpha$, quas inter se incongruas esse facile perspicitur. Hinc patet, si colligantur residua minima positiua biquadratorum $1, 16, 81, 256 \ldots (p-1)^4$, quaterna semper aequalia fore, ita vt $\frac{1}{4}(p-1)$ residua biquadratica diuersa habeantur complexum $\mathfrak{A}$ formantia. Si residua minima biquadratorum vsque ad $(\frac{1}{2}p - \frac{1}{2})^4$ tantum colliguntur, singula bis aderunt.

7.

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

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

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

Simul facile iam diiudicari potest, ad quamnam classem referendum sit productum e pluribus factoribus. Scilicet tribuendo classi $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ 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 euoluere, qua in auxilium vocata omnia adhuc multo facilius demonstrare licet.

Sit g radix primitiua pro modulo p, i. e. numerus talis, vt in serie potestatum g, gg, g^3 .... nulla ante hanc g^{p-1} vnitati secundum modulum p congrua euadat. Tunc residua minima positiua numerorum 1, g, gg, g^3 .... g^{p-2} praeter ordinem cum his $1, 2, 3 \ldots . p-1$ conuenient, et in quatuor classes sequenti modo distribuentur:

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

Hinc omnes propositiones praecedentes sponte demanant.

Ceterum sicuti hic numeri $1, 2, 3 \ldots p-1$ in quatuor classes distributi sunt, quarum complexus per A, B, C, D designamus, ita *quemuis* integrum per p non diuisibilem, 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, vnde quum fiat $ff \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ (*Disquiss. Arithm.* p. 59), patet, characterem f hic idem significare, quod in art. 6. Potestas $g^{\frac{1}{4}\lambda(p-1)}$ itaque, denotante λ integrum positiuum, congrua erit secundum modulum p numero $1, f, -1, -f$, prout λ formae $4m$, $4m+1$, $4m+2$, $4m+3$ resp., siue 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 diuisibilis 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 euadit.

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* p. 114 docuimus, facile adornari potest.

10.

Quum *omnes* radices primitiuae 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 primitiua e complexu B pro basi accipitur, classificatio eadem manebit; si vero radix primitiua 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, vtram radicem congruentiae $xx \equiv -1$ (mod. 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 primitiuam pro singulis minimam adoptauimus.

$p = 5$

$g = 2,\ f = 2$

A	1
B	2
C	3
D	4

$p = 13$

$g = 2,\ f = 8$

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

$p = 17$

$g = 3,\ f = 13$

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

$p = 29$

$g = 2,\ f = 12$

A	1, 7, 16, 20, 23, 24, 25
B	2, 3, 11, 14, 17, 19, 21
C	4, 5, 6, 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 inuenietur. 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, inuenimus 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 vnico tantum modo, sub formam $aa+2bb$ (*Disquiss. Arithm.* p. 220); radices a, b positiue accipi supponemus. Manifesto a impar erit, b vero par; statuemus autem $b=2^\lambda c$, ita vt c sit impar. Iam obseruamus

I. quum habeatur $p\equiv aa$ (mod. c) ipsum p esse residuum quadraticum ipsius c, et proin etiam singulorum factorum primorum, in quos c resoluitur: 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 inuenitur numerus 2; quare quum $aa\equiv-2bb$, manifestum est, 2 vel in classe A, vel in classe C inueniri, prout a sit vel residuum quadraticum ipsius p, vel non-residuum qradraticum.

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 $p\equiv 2bb$ (mod. 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 vt 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 inuenietur.

Quod confirmatur per exempla in art. praec. enumerata; priores enim moduli ita discerpuntur: $73 = 1 + 2\cdot36$, $89 = 81 + 2\cdot4$, $113 = 81 + 2\cdot16$, $233 = 225 + 2\cdot4$, $257 = 225 + 2\cdot16$, $281 = 81 + 2\cdot100$, $337 = 49 + 2\cdot144$, $353 = 225 + 2\cdot64$; posteriores vero ita: $17 = 9 + 2\cdot4$, $41 = 9 + 2\cdot16$, $97 = 25 + 2\cdot36$, $137 = 9 + 2\cdot64$, $193 = 121 + 2\cdot36$, $241 = 169 + 2\cdot36$, $313 = 25 + 2\cdot144$, $401 = 9 + 2\cdot196$, $409 = 121 + 2\cdot144$, $433 = 361 + 2\cdot36$, $449 = 441 + 2\cdot4$, $457 = 169 + 2\cdot144$.

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 obseruamus, 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 veró 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 inuicem sequuntur, spectantes.

15.

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)

$$\begin{array}{llll} (00), & (01), & (02), & (03) \\ (10), & (11), & (12), & (13) \\ (20), & (21), & (22), & (23) \\ (30), & (31), & (32), & (33) \end{array}$$

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

$p = 5$	$p = 37$	$p = 73$
0, 1, 0, 0	2, 1, 2, 4	5, 6, 4, 2
0, 0, 0, 1	2, 2, 4, 1	6, 2, 5, 5
0, 0, 0, 0	2, 2, 2, 2	4, 5, 4, 5
0, 0, 1, 0	2, 4, 1, 2	2, 5, 5, 6
$p = 13$	$p = 41$	$p = 89$
0, 1, 2, 0	0, 4, 3, 2	3, 8, 6, 4
1, 1, 0, 1	4, 2, 2, 2	8, 4, 5, 5
0, 1, 0, 1	3, 2, 3, 2	6, 5, 6, 5
1, 0, 1, 1	2, 2, 2, 4	4, 5, 5, 8
$p = 17$	$p = 53$	$p = 97$
0, 2, 1, 0	2, 3, 6, 2	2, 6, 7, 8
2, 0, 1, 1	4, 4, 2, 3	6, 8, 5, 5
1, 1, 1, 1	2, 4, 2, 4	7, 5, 7, 5
0, 1, 1, 2	4, 2, 3, 4	8, 5, 5, 6
$p = 29$	$p = 61$	
2, 3, 0, 2	4, 3, 2, 6	
1, 1, 2, 3	3, 3, 6, 3	
2, 1, 2, 1	4, 3, 4, 3	
1, 2, 3, 1	3, 6, 3, 3	

Quum moduli formae $8n+1$ et $8n+5$ diuerso modo se habeant, vtrosque scorsim tractare oportet: a prioribus initium faciemus.

16.

Character (00) indicat, quot modis diuersis 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 diuersorum, aequationi $1+\alpha+\alpha'=p$, satisfaciendi: manifesto huius aequationis vice etiam congruentia $1+\alpha+\alpha'\equiv 0$ (mod. p) fungi potest.

Perinde (01) indicat multitudinem solutionum congruentiae $1+\alpha+\beta\equiv 0$ (mod. 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 quauis 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, vt fiat $\beta\delta\equiv 1$, simulque statuitur $\alpha\equiv\beta\delta'$. Hinc concludimus, vtramque congruentiam aequali solutionum multitudine gaudere, siue 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 vt fiat $\gamma\gamma'\equiv 1$, atque γ'' ex eodem complexu congruus producto $\alpha\gamma'$. Vnde facile colligimus, has duas congruentias aequalem solutionum multitudinem admittere, siue esse $(02)=(22)$.

Perinde e congruentia $1+\alpha+\delta\equiv 0$ deducimus $\beta+\beta'+1\equiv 0$, accipiendo β, β' ita vt 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 $\gamma'+\delta'+1\equiv 0$ deriuamus, atque hinc concludimus $(12)=(13)=(23)$.

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

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

Facile vero tres nouae aequationes conditionales adiiciuntur. Quum enim quemuis numerum complexus A, excepto vltimo $p-1$, 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.

Vt vero determinationem completam nanciscamur, inuestigare conueniet multitudinem solutionum congruentiae

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

disignantibus 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 quouis autem valore *dato* ipsius $1+\alpha$ ad A pertinente, puta pro $1+\alpha=\alpha^\circ$, congruentia $\alpha^\circ+\beta+\gamma\equiv 0$ totidem solutiones admittet, quot congruentia $1+\beta'+\gamma'\equiv 0$ (statuendo scilicet $\beta\equiv\alpha^\circ\beta'$, $\gamma\equiv\alpha^\circ\gamma'$), i. e. solutiones $(12)=m$. Perinde pro quouis valore dato ipsius $1+\alpha$ ad B pertinente, puta pro $1+\alpha=\beta^\circ$, congruentia $\beta^\circ+\beta+\gamma\equiv 0$ totidem solutiones habebit, quot haec $1+\alpha'+\beta'\equiv 0$ (scilicet statuendo $\beta\equiv\beta^\circ\alpha'$, $\gamma\equiv\beta^\circ\beta'$), i. e. solutiones $(01)=i$. Similiter pro quolibet valore dato ipsius $1+\alpha$ ad C pertinente, puta pro $1+\alpha=\gamma^\circ$, congruentia $\gamma^\circ+\beta+\gamma\equiv 0$ totidem modis diuersis solui poterit, quot haec $1+\delta+\alpha'\equiv 0$ (nempe statuendo $\beta\equiv\gamma^\circ\delta$, $\gamma\equiv\gamma^\circ\alpha'$), i. e. solutionum multitudo erit $(03)=l$. Denique pro quouis valore dato ipsius $1+\alpha$ ad D pertinente, puta pro $1+\alpha=\delta^\circ$, congruentia $\delta^\circ+\beta+\gamma\equiv 0$ totidem solutiones habebit, quot haec $1+\gamma'+\delta'\equiv 0$ (statuendo $\beta\equiv\delta^\circ\gamma'$, $\gamma\equiv\delta^\circ\delta'$), i. e. $(23)=m$ solutiones. Omnibus itaque collectis, patet, congruentiam $1+\alpha+\beta+\gamma\equiv 0$ admittere

$$hm+ii+kl+lm$$

solutiones diuersas.

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

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

Ad eundem valorem perducimur, si euolutionem 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 vltimae 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

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

siue

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

Statuendo itaque

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

habebimus

$$p = aa + bb$$

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

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

$$\begin{aligned} 8h &= 4n - 3a - 5 \\ 8i &= 4n + a - 2b - 1 \\ 8k &= 4n + a - 1 \\ 8l &= 4n + a + 2b - 1 \\ 8m &= 4n - a + 1 \end{aligned}$$

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

$$\begin{array}{l|l|l|l} p-6a-11 & p+2a-4b-3 & p+2a-3 & p+2a+4b-3 \\ p+2a-4b-3 & p+2a+4b-3 & p-2a+1 & p-2a+1 \\ p+2a-3 & p-2a+1 & p+2a-3 & p-2a+1 \\ p+2a+4b-3 & p-2a+1 & p-2a+1 & p+2a-4b-3 \end{array}$$

19.

Superest, vt 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, praeuidere licet, nexum inter signum ipsius b atque numerum f exstare debere. Quem vt cognoscamus, ante omnia obseruamus, si, denotante μ integrum non negatiuum, pro z accipiantur omnes numeri $1, 2, 3 \ldots p-1$, fieri secundum modulum p, vel $\sum z^\mu \equiv 0$, vel

$\Sigma z^\mu \equiv -1$, prout μ vel non-diuisibilis sit per $p-1$, vel diuisibilis. Pars posterior theorematis inde patet, quod pro valore ipsius μ per $p-1$ diuisibili, habetur $z^\mu \equiv 1$: partem priorem vero ita demonstramus. Denotante g radicem primitiuam, omnes z conuenient 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

$$\Sigma g^{\mu y} = \frac{g^{\mu(p-1)}-1}{g^\mu - 1}, \text{ adeoque}$$

$$(g^\mu - 1)\,\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0.$$

Hinc vero sequitur, quoniam pro valore ipsius μ per $p-1$ nondiuisibili g^μ ipsi 1 congruus siue $g^\mu - 1$ per p diuisibilis esse nequit, $\Sigma z^\mu \equiv 0$. *Q. E. D.*

Iam si potestas $(z^4+1)^{\frac{1}{4}(p-1)}$ secundum theorema binomiale euoluitur, 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

$4(00)$ ad A
$4(01)$ ad B
$4(02)$ ad C
$4(03)$ 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

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

siue substitutis pro (00), (01) etc. valoribus in art. praec. inuentis,

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

Hinc itaque colligimus, semper fieri debere $a + bf \equiv 0$, siue, 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, inseruit.

20.

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

Quum pro tali modulo -1 ad classem C pertineat, complementa numerorum complexuum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ 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)	$1+\delta+\beta \equiv 0$

vnde

vnde statim habentur sex aequationes:

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

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

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

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

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

Porro habemus aequationes

$$\begin{aligned} (00) + (01) + (02) + (03) &= 2n+1 \\ (10) + (11) + (12) + (13) &= 2n+1 \\ (20) + (21) + (22) + (23) &= 2n \\ (30) + (31) + (32) + (33) &= 2n+1 \end{aligned}$$

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

$$\begin{aligned} h + i + k + l &= 2n+1 \\ 2m + i + l &= 2n+1 \\ h + m &= n \end{aligned}$$

quarum itaque adiumento incognitas nostras iam ad duas reducere licet.

Aequationes reliquas e consideratione multitudinis solutionum congruentiae $1 + \alpha + \beta + \gamma \equiv 0$ deriuabimus (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 quouis 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 quouis valore *dato* ipsius β in his quatuor casibus exstent solutiones h, m, h, m, multitudo omnium solutionum erit

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

vnde deriuamus 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 $l + i = 1 + 2h$, vnde

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

Quibus valoribus in aequatione praecedente substitutis, prodit:

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

Quodsi tandem pro $4m$ hic substituimus $2(h + m) - 2(h - m)$ siue, propter aequationem vltimam 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

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

fiet

$$p = aa + bb.$$

Iam quum in hoc quoque casu p vnico 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, vt fiat $a \equiv 1$ (mod. 4), signumque ipsius b ita, vt habeatur $b \equiv af$ (mod. p), vti per ratiocinia iis quibus in art. praec. vsi sumus prorsus similia facile demonstratur.

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

$$\begin{aligned}
8h &= 4n + a - 1\\
8i &= 4n + a + 2b + 3\\
8k &= 4n - 3a + 3\\
8l &= 4n + a - 2b + 3\\
8m &= 4n - a + 1
\end{aligned}$$

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 soluimus, ad disquisitionem principalem reuertimur, determinationem completam complexus, ad quem numerus 2 pertinet, iam aggressuri.

I. Quoties p est formae $8n+1$, iam constat, numerum 2 ve in complexu A vel in complexu C inueniri. In casu priori facil 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, siue, 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

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

siue 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 inuentum.

II. Sed etiam casum alterum, vbi p est formae $8n+5$, aeque complete absoluere 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 vnus eorum sibi ipse associatus est, i. e. vbi $\frac{1}{2}(p-1)$ 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

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

siue 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: vnde colligimus, 2 pertinere ad B, quoties b sit formae $8m + 2$, ad D vero, quoties b sit formae $8m + 6$.

Summa harum inuestigationum 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 diuisionis circuli, atque solutionis aequationis $x^p - 1 = 0$ explicauimus, interque alia docuimus, si μ sit diuisor numeri $p - 1$, functionem $\frac{x^p - 1}{x - 1}$ in μ factores ordinis $\frac{p - 1}{\mu}$ resolui posse adiumento aequationis auxiliaris ordinis μ. Praeter theoriam generalem huius resolutionis simul casus speciales, vbi $\mu = 2$ vel $\mu = 3$, in illo opere p. 356-358 seorsim considerauimus, aequationemque auxiliarem a priori assignare docuimus, i. e. absque euolutione schematis residuorum minimorum potestatum alicuius radicis primitiuae pro modulo p. Iam vel nobis non monentibus lectores attenti facile percipient nexum arctissimum casus proximi istius theoriae, puta pro $\mu = 4$, cum inuestigationibus hic in artt. 15-20 explicatis, quarum adiumento ille quoque sine difficultate complete absolui poterit. Sed hanc tractationem ad aliam occasionem nobis reseruamus, 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 noua pure arithmetica, cum argumento hactenus pertractato arctissime coniuncta, adiiciemus.

23.

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

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

denotando per P coëfficientem medium

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

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 $\frac{1}{2}(p-1)$ euecti 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. 17, 19 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

$$1 \cdot 2 \cdot 3 \ldots\ldots \tfrac{1}{4}(p-1)$$
$$\tfrac{1}{4}(p+3) \cdot \tfrac{1}{4}(p+7) \cdot \tfrac{1}{4}(p+11) \ldots\ldots \tfrac{1}{2}(p-1)$$
$$\tfrac{1}{2}(p+1) \cdot \tfrac{1}{2}(p+3) \cdot \tfrac{1}{2}(p+5) \ldots\ldots \tfrac{3}{4}(p-1)$$
$$\tfrac{1}{4}(3p+1) \cdot \tfrac{1}{4}(3p+5) \cdot \tfrac{1}{4}(3p+9) \ldots\ldots (p-1)$$

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

$$2a \equiv \frac{r}{q} \text{ (mod. } p)$$

Quum quilibet factorum ipsius q complementum suum ad p habeat in t, erit $q \equiv t$ (mod. p), quoties multitudo factorum par est, i. e. quoties p est formae $8n+1$, contra $q \equiv -t$, quoties multitudo factorum impar est, siue p formae $8n+5$. Perinde in casu priori erit $r \equiv s$, in posteriori $r \equiv -s$. In vtroque casu erit $qr \equiv st$, et quum constet, haberi $qrst \equiv -1$, erit $qqrr \equiv -1$, adeoque $qr \equiv \pm f$ (mod. p). Combinando hanc congruentiam cum theoremate modo inuento obtinemus $rr \equiv \pm 2af$, et proin, per artt. 19. 20

$$2b \equiv \pm rr \text{ (mod. } p)$$

Valde memorabile est, discerptionem numeri p in duo quadrata per operationes prorsus directas inueniri 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:

$$\frac{6.\ 10.\ 14.\ 18 \ldots\ldots (p-3)}{2.\ 3.\ 4\ \ 5. \ldots\ldots \frac{1}{4}(p-1)}$$

Sed quum insuper nouerimus, quonam signo affecta prodeat ex hac formula radix quadrati imparis, eo scilicet, vt semper fiat formae $4m+1$, attentione perdignum est, quod simile criterium generale respectu signi radicis quadrati paris hactenus inueniri non potuerit. Quale si quis inueniat, 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.

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