OBSERVATIONES CIRCA DIVISIONEM QVADRATORVM PER NVMEROS PRIMOS.

Hypothesis.

Si numerorum a, b, c, d, etc. quadrata a^2, b^2, c^2, d^2, etc. per numerum quempiam primum P diuidantur, residua in diuisione relicta litteris cognominibus graecis α, β, γ, δ, etc. indicemus.

Corollarium 1.

§. 2. Cum ergo quadratum aa per numerum P diuisum relinquat residuum α; posito quoto $= A$ erit $aa = AP + \alpha$, ideoque $aa - \alpha$ diuisibile erit per P; similique modo hae expressiones: $bb - \beta$, $cc - \gamma$, $dd - \delta$, etc. diuisibiles erunt per eundem diuisorem P.

Corollarium 2.

§. 3. Quadrata $(a + P)^2$, $(a + 2P)^2$, $(a + 3P)^2$, et in genere $(a + nP)^2$ idem residuum α relinquent, si per numerum propositum P diuidantur. Vnde patet, numerorum, diuisore P maiorum, quadrata eadem praebere residua, quae ex quadratis numerorum, diuisore P minorum, nascuntur.

ORVM
b^2, c^2, d^2, diuidantur, graecis
numerum P $= A$ erit per P; si- γ, $dd - \delta$,
$a + 3P)^2$, inquent, si patet, nu- mero-

Corollarium 3.

§. 4. Cum deinde quadratum $(P - a)^2$ per P diuisum idem praebeat residuum, quod quadratum a^2, patet si fuerit $a > \frac{1}{2}P$, fore $P - a < \frac{1}{2}P$. Vnde manifestum est, omnia residua diuersa ex quadratis numerorum, qui semisse diuisoris P sint minores, resultare.

Corollarium 4.

§. 5. Quare si omnia residua desiderentur, quae ex diuisione quadratorum per datum diuisorem P proueniunt, sufficiet ea tantum quadrata considerasse, quorum radices semissem ipsius P non superent.

Corollarium 5.

§. 6. Hinc si diuisor sit $P = 2p + 1$, si per eum omnes numeri quadrati 1, 4, 9, 16, 25, etc. diuidantur, plura residua diuersa inde prodire nequeunt, quam vnitates in numero p continentur; eaque resultant ex quadratis numerorum 1, 2, 3, 4, ... p: sequentium enim numerorum $p + 1$, $p + 2$, $p + 3$, etc. quadrata eadem residua ordine retrogrado reproducunt.

Scholion.

§. 7. Manifestum hoc inde est, quod haec duo quadrata: p^2 et $(p + 1)^2$, per numerum $2p + 1$ diuisa, idem

idem praebent reſiduum; ſiquidem eorum differentia per $2p+1$ eſt diuiſibilis. Generatim enim, quorumcunque numerorum differentia $M-N$ per $2p+1$, eſt diuiſibilis, neceſſe eſt vt vterque M et N, ſeorſim diuiſus, idem reſiduum relinquat. Hinc etiam cum ſit $(p+2)^2-(p-1)^2 = 3(2p+1)$, vtrumque quadratum ſeorſim, $(p+2)^2$ et $(p-1)^2$, idem reſiduum praebere debet, et in genere quadratum $(p+n+1)^2$ idem reſiduum dabit, quod quadratum $(p-n)^2$. Hoc igitur oſtenſo perſpicuum eſt plura reſidua reſultare non poſſe, quam in numero p vnitates continentur: vtrum autem haec reſidua omnia ſint diuerſa, an quaepiam inter ſe conueniant? hinc non definitur; atque adeo, ſi diuiſores quicunque admittantur, vtrumque euenire poteſt. Sin autem diuiſor $2p+1$, fuerit numerus primus, omnia illa reſidua erunt inter ſe diuerſa quod ſequenti modo demonſtro.

Theorema I.

§. 8. Si diuiſor $P = 2p+1$ fuerit numerus primus, per eumque omnia quadrata $1, 4, 9, 16, \ldots\ldots$ vsque ad p^2 diuidantur, omnia reſidua hinc reſultantia inter ſe erunt diuerſa, eorumque adeo multitudo $= p$.

Demonſtratio.

Sint a et b duo numeri quicunque ipſo p minores, vel ſaltem non maiores; ac demonſtrandum eſt, ſi eorum quadrata a^2 et b^2 per numerum primum $2p+1$ diuidantur, reſidua certe diuerſa eſſe proditura. Si enim idem praeberent reſiduum, eorum differentia $aa-bb$ per $2p+1$, foret diuiſibilis, ideoque ob $2p+1$ numerum primum

ferentia per orumcunque t diuiſibilis, idem reſi- $-(p-1)^2$ $(p+2)^2$ et genere qua- od quadra- eſt plura p vnitates ſint diuer- definitur; vtrumque fuerit nu- ſe diuerſa

numerus $16, \ldots\ldots$ ltantia in- $=p$.

p mino- m eſt, ſi $2p+1$ Si enim $-bb$ per numerum primum

primum et $aa-bb = (a+b)(a-b)$, alter horum factorum per $2p+1$ diuiſibilis eſſe deberet. Cum autem ſit tam $a<p$ quam $b<p$, ſaltem non $a>p$, ſumma $a+b$, multoque magis differentia $a-b$ diuiſore $2p+1$ eſt minor; indeque neutra per $2p+1$ diuiſibilis eſſe poteſt. Ex quo manifeſto ſequitur: omnia quadrata, quorum radices non ſint ipſo p maiores, per numerum primum $2p+1$ diuiſa, certe diuerſa reſidua eſſe relictura.

Corollarium 1.

§. 9. Quodſi ergo omnia quadrata $1, 4, 9, 16$, etc. per numerum primum $2p+1$ diuidantur, omniaque reſidua diuerſa notentur, eorum numerus neque maior erit neque minor quam p, ſed huic numero p praeciſe aequalis.

Corollarium 2.

§. 10. Omnia vero haec reſidua diuerſa numero p, oriuntur ex totidem quadratis in ſerie naturali primum occurrentibus, ſcilicet $1, 4, 9, 16, \ldots\ldots pp$; neque ex ſequentibus maioribus vlla noua reſidua eliciuntur.

Corollarium 3.

§. 11. Non omnes ergo numeri ipſo diuiſore $2p+1$ minores inter reſidua occurrent, ſed tantum tot eorum, quot vnitates continentur in diuiſoris minori ſemiſſe p. Quare cum numerorum, diuiſore $2p+1$ minorum, multitudo ſit $= 2p$, horum alter ſemiſſis tantum in ordine reſiduorum reperietur, alter vero inde penitus excluditur.

I 2 Scholi-

Scholion.

§. 12. Numeros hos diuisore primo $2p+1$ minores, qui ex ordine residuorum excluduntur, nomine *non-residuorum* indicabo, quorum ergo multitudo semper numero residuorum est aequalis. Hoc discrimen inter residua et non-residua probe perpendisse iuuabit, quare pro diuisoribus aliquot primis minoribus tam residua quam non-residua hic exhibebo.

Div. 3; $p=1$		Div. 5; $p=2$			Div. 7; $p=3$			
quadr.	1	quadr.	1,	4	quadr.	1.	4.	9
residuum	1	resid.	1.	4	residuum	1.	4.	2
non-res.	2	non-res.	2,	3	non-res.	3.	5.	6

Diuisor 11; $p=5$					
Quadrata	1,	4,	9,	16,	25
Residua	1,	4,	9,	5,	3
non-resid.	2,	6,	7,	8,	10

Diuisor 13; $p=6$						
Quadrata	1,	4,	9,	16,	25,	36
Residua	1,	4,	9,	3,	12,	10
non-resid.	2,	5,	6,	7,	8,	11

Diuisor 17; $p=8$								
Quadrata	1,	4,	9,	16,	25,	36,	49,	64
Residua	1,	4,	9,	16,	8.	2,	15,	13
non-resid.	3,	5,	6,	7,	10,	11,	12,	14

Diuisor 19; $p=9$									
Quadrata	1,	4,	9,	16,	25,	36,	49,	64,	81
Residua	1,	4,	9,	16,	6,	17,	11,	7,	5
non-residua	2,	3,	8,	10,	12,	13,	14,	15,	18

$+1$ mi-
, nomine
do semper
1 inter re-
quare pro
dua quam
= 3
4. 9
4. 2
5. 6
6
16, 25, 36
3, 12, 10
7, 8, 11
Circa

Circa haec residua et non-residua pro quouis diuisore primo tam memorabiles proprietates obseruantur, quas eo maiori studio perpendisse operae est pretium, quod inde non contemnenda incrementa in numerorum Theoriam redundare videntur.

Theorema II.

§. 13. Si in ordine residuorum ex diuisore P ortorum occurrant numeri α et β, ibidem quoque occurret eorum productum $\alpha\beta$, siquidem minus fuerit diuisore P; sin autem sit maius eius loco capi conuenit $\alpha\beta-P$, vel $\alpha\beta-2P$, vel generatim $\alpha\beta-nP$, donec infra P deprimatur.

Demonstratio.

Oriantur residua α et β ex diuisione quadratorum aa et bb per diuisorem P facta, ita vt sit

$$aa = AP+\alpha \text{ et } bb = BP+\beta.$$

Hinc erit

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Quare si quadratum $aabb$ per diuisorem P diuidatur, residuum relinquetur $\alpha\beta$, vel si $\alpha\beta$ superet diuisorem P, eius loco sumi debet residuum, quod ex diuisione ipsius $\alpha\beta$ per P facta relinquetur, quod proinde erit vel $\alpha\beta-P$, vel $\alpha\beta-2P$ vel $\alpha\beta-3P$, vel generatim $\alpha\beta-nP$, ita vt sit $\alpha\beta-nP < P$.

Corollarium 1.

§. 14. Si ergo inter residua occurrat numerus α, ibidem quoque occurret $\alpha\alpha$, item α^3, α^4, etc. omnesque adeo eius potestates, siquidem a singulis eiusmodi multiplum diuisoris P subtrahatur, vt residuum minus fiat diuisore P.

Corollarium 2.

§. 15. Cum igitur existente diuisore P numero primo $2p+1$, residuorum numerus sit $=p$; si unius cuiuspiam residui α omnes potestates α^0, α^1, α^2, α^3, α^4, etc. per eundem diuisorem P diuidantur, inde non plura quam p residua diuersa resultare possunt.

Corollarium 3.

§. 16. Hinc sequitur, potestatem α^p, per $P=2p+1$ diuisam, idem praebere residuum quod $\alpha^0=1$, seu residuum fore vnitatem, vti alibi ostendi, siquidem diuisor $2p+1$ fuerit numerus primus.

Scholion.

§. 17. Eximiis proprietatibus, quae hinc deduci possunt, hic vberius euoluendis non immoror, cum hoc iam olim a me sit factum. Ea hic tantum principia breuiter repetere constitui, quibus indigeo ad nouas quasdam residuorum affectiones explicandas, vnde insignes nonnullas numerorum proprietates multo expeditius demonstrare liceat. Hunc in finem animaduerto, quod quidem per se est perspicuum, quemadmodum residuo $\alpha\beta$ aequiualent numeri

nerus α, mnesque li multi- fiat di- numero inius cu- α^4, etc. a quam $=2p+1$ residuum $2p+1$ deduci um hoc ipia bre- quasdam onnullas trare li- per se lent nu- meri

meri $\alpha\beta-P$, $\alpha\beta-2P$, et in genere $\alpha\beta-nP$, existente P diuisore, ita etiam omnes numeros per P diuisos, idem residuum relinquentes, in hoc negotio tanquam hoc ipsum residuum spectari posse. Ita in ordine residuorum, pro quocunque diuisore P, omnes plane numeri quadrati ipsi occurrere sunt censendi, cum quilibet aa huiusmodi forma $AP+\alpha$ exhiberi queat, ideoque vero residuo α aequiualere sit existimandus. Hinc etiam inter residua numeri negatiui admitti poterunt, cum residuo α aequiualeat $\alpha-P$, hocque pacto omnia residua ad numeros semissi diuisoris P minores reuocare licebit.

Theorema III.

§. 18. Si in ordine residuorum, ex diuisore P ortorum, occurrant bina residua α et β, in eo quoque occurret residuum $\frac{\alpha+nP}{\beta}$, numero n ita assumto, vt $\frac{\alpha+nP}{\beta}$ fiat numerus integer, id quod semper fieri licet.

Demonstratio.

Sint aa et bb ea quadrata, quae per P diuisa relinquunt residua α et β, vt sit $aa=AP+\alpha$ et $bb=BP+\beta$. Iam quaeratur c, vt sit $c=\frac{a+mP}{b}$ numerus integer, eritque

$$cc=\frac{aa+2amP+mmPP}{bb}=\frac{\alpha+(A+2am+mmP)P}{\beta+BP}=\text{num.}$$

integro. Cum nunc numerator tanquam ipsum residuum α, denominator vero tanquam residuum β spectari possit, patet, si cc per P diuiditur, residuum ad formam propositam reductum iri. Posito enim breuitatis gratia $A+2am+mmP=D$, vt sit $cc=\frac{\alpha+DP}{\beta+BP}$; tum vero $\frac{\alpha+nP}{\beta}=\gamma$, osten-

ostendi oportet, fore $cc = CP + \gamma$, vt residuum ex diuisione quadrati cc per numerum P natum prodeat $= \gamma$. Cum autem sit $\alpha = \beta\gamma - nP$ vtique fieri poterit:

$$cc = \frac{\beta\gamma + (D-n)P}{\beta + BP} = CP + \gamma,$$

quoniam inde sequitur:

$$(D-n)P = (\beta C + \gamma B + BCP)P, \text{ seu}$$
$$D - n = \beta C + \gamma B + BCP$$

cuiusmodi relatio inter coefficientes ipsius P omnino necessaria est, vt numeri integri prodeant.

Aliter.

Loco residui α aliud aequiualens accipiatur $\alpha + nP$, vt sit $\alpha + nP = \beta\gamma$; et cum omnia quadrata huius formae $(a + mP)^2$ idem praebeant residuum α, quod ex quadrato aa nasci assumitur, sumatur m ita, vt fiat $a + mP = bc$, et quia quadratum $bbcc$ per P diuisum relinquit residuum α, vel $\beta\gamma$, quadratum vero bb residuum b: necesse est vt quadratum cc relinquat residuum $\gamma = \frac{\alpha + nP}{\beta}$. Sit enim $bbcc = EP + \beta\gamma$ et $bb = BP + \beta$; tum vero si neges quadratum cc praebiturum esse residuum γ, praebeat diuersum x, vt sit $cc = CP + x$; erit ergo

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x)$$
$$= \beta x + (\beta C + Bx + BCP)P.$$

Iam multiplis diuisoris P vtrinque omissis, quemadmodum in aestimatione residuorum fieri solet, siquidem in minima forma desiderentur, habebitur $\beta x = \beta\gamma$, ideoque $x = \gamma$.

Corol-

ex di-
at $= \gamma$.
ino ne-
$+ nP$,
ius for-
uod ex
$a+mP$
elinquit
b: ne-
$\frac{\alpha+nP}{\beta}$.
; tum
uum γ,
rgo
x)
modum
minima
$= \gamma$.
Corol-

Corollarium 1.

§. 19. Cum igitur vnitas semper sit residuum, si pro diuisore P fuerit aliquod residuum α, tum etiam $\frac{1+nP}{\alpha}$ inter residua occurret, quod si vocetur β, erit $\alpha\beta = 1 + nP$, seu inter residua productum $\alpha\beta$ vnitati aequiualebit.

Corollarium 2.

§. 20. Pro quolibet ergo residuo α aliud quasi eius reciprocum β assignari potest, vt $\alpha\beta$ vnitati aequiualeat, sumendo scilicet $\beta = \frac{1+nP}{\alpha}$; atque haec duo residua reciproca α et β inter se erunt diuersa, nisi ambo fuerint vel $+1$ vel -1. Si enim sit $\beta = \alpha$ et

$$\alpha\alpha = 1 + nP = 1 + 2mP + mmPP,$$

erit $\alpha = \pm(1 + mP)$ et multiplum diuisoris mP omittendo, $\alpha = \pm 1$.

Corollarium 3.

§. 21. Dum igitur in ordine residuorum cuilibet residuo suum reciprocum adiungitur, hoc modo bina copulabuntur; semper autem vnitas solitaria relinquetur, tum vero etiam residuum -1, seu $P - 1$, quoties quidem inter residua occurrit.

Scholion.

§. 22. Idea haec binorum residuorum reciprocorum maximi est momenti, et ad demonstrationem facilem Theorematis pulcerrimi nos manuducet, quod alias per satis multas ambages demonstraueram: scilicet quod numerus primus formae $4q + 1$ semper sit summa duorum qua-

 dra-

draturum. Ceterum hic meminisse iuuabit, si pro quopiam diuisore P residua sint α, β, γ, δ, etc. non-residua vero $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. tum residuorum omnia producta mutua $\alpha\beta$, $\alpha\gamma$, etc. etiam inter residua reperiri, eorum autem producta per quodpiam non-residuum, veluti $\alpha\mathfrak{A}$, inter non-residua esse referenda. At producta ex binis non-residuis, vti $\mathfrak{A}\mathfrak{B}$, in ordinem residuorum transeunt.

Theorema IV.

§. 23. Si diuisor P fuerit numerus primus formae $4q+3$, tum -1, seu $P-1$ certe in ordine non-residuorum reperitur.

Demonstratio.

Cum posito diuisore $P=2p+1$, hic sit $p=2q+1$, ideoque numerus impar, numerus omnium residuorum erit impar. At si -1 in ordine residuorum occurreret, cuilibet residuo α responderet aliud residuum $-\alpha$, vnde ordo residuorum ita se esset habiturus:

$$\begin{matrix} +1; & +\alpha; & +\beta; & +\gamma; & +\delta \\ -1; & -\alpha; & -\beta; & -\gamma; & -\delta \end{matrix} \text{ etc.}$$

foretque ergo numerus residuorum par. Cum igitur numerus residuorum certo sit impar, fieri nequit, vt in ordine residuorum occurrat -1, seu $P-1$, consequenter in ordine non-residuorum necessario reperiri debet.

Corollarium 1.

§. 24. Quodsi ergo pro diuisore primo $P=4q+3$ inter residua occurrat numerus α, tum numerus $-\alpha$, seu $P-$

o quo-
residua
roducta
autem
er non-
esiduis,
formae
esiduo-
$2q+1$,
im erit
, cui-
c ordo
ur nu-
in or-
iter in
$4q+3$
α, seu
P -

$P-\alpha$ certe inter non-residua reperietur; similique modo, si $-\beta$ fuerit residuum, tum $+\beta$ erit non-residuum.

Corollarium 2.

§. 25. Si quadratum aa per diuisorem $P=4q+3$ diuisum relinquat residuum α, quia nullum datur quadratum xx, quod praebeat residuum $-\alpha$, fieri omnino nequit, vt vlla summa duorum quadratorum $aa+xx$, per numerum illum $4q+3$ diuisibilis, existat.

Corollarium 3.

§. 26. Oriatur praeterea residuum β ex quadrato bb, et quia forma βaa residuum dat $\alpha\beta$, forma vero αbb residuum $\alpha\beta$, haec forma $\beta aa-\alpha bb$ per diuisorem $P=4q+3$ erit diuisibilis.

Corollarium 4.

§. 27. Cum autem nullum detur quadratum xx, quod residuum praebeat $-\beta$, nulla datur forma αxx residuum praebens $-\alpha\beta$, nulla huiusmodi forma $\beta aa+\alpha xx$ per numerum $P=4q+3$ erit diuisibilis, siquidem α et β sint residua, et α residuum quadrato aa respondens.

Corollarium 5.

§. 28. Cum autem neque haec forma $\beta aacc+\alpha ccxx$ per diuisorem $P=4q+3$ sit diuisibilis, nisi quadratum cc diuisionem admittat, qui casus sponte excluditur, quadrato $aacc$ quodcunque aliud residuum praeter α respondere potest; vnde, loco $aacc$ et $ccxx$ scribendo

dd

dd et yy, nulla huiusmodi forma $\beta dd + \alpha yy$ exhiberi potest per numerum $P = 4q + 3$ diuisibilis, dum α et β sint residua.

Scholion.

§. 29. Quo haec clarius perspiciantur, percurramus quosdam numeros primos formae $4q + 3$, ac residua eius semisse maiora, subtrahendo inde $4q + 3$, negatiue repraesentemus, vt infra semissem reuocentur, indeque pateat, nullius residui α negatiuum $-\alpha$ simul in ordine residuorum occurrere:

Diuisor	residua
3	1
7	1, −3, +2
11	1, +4, −2, + 5, +3
19	1, +4, +9, − 3, +6, − 2, − 8, +7, +5
23	1, +4, +9, − 7, +2, −10, + 3, −5, −11, +8, +6
31	1, +4, +9, −15, −6, + 5, −13, +2, −12, +7, −3, −11, +14, +10, +8

Hic euidens est, inter residua omnes numeros semisse diuisoris non maiores occurrere vel signo + vel − affectus, nullum autem bis vtroque signo affectum occurrere. Hinc si singulorum horum residuorum signa mutentur, ordo nonresiduorum complebitur. Hinc pro diuisore 31 sequentes formae exhiberi possunt nunquam per 31 diuisibiles: $aa+bb$; $aa-15bb$; $aa-6bb$; $aa+5bb$; $aa-13bb$; $aa+2bb$; $aa+7bb$; $aa-3bb$; $aa-11bb$; $aa+14bb$; $aa+10bb$. Atque in genere, si α et β sint duo quaecunque residua, nulla huiusmodi forma: $\alpha aa + \beta bb$, per numerum 31 diuisionem admittet.

Theo-

exhiberi
α et β
ercurra-
residua
tiue re-
: patear,
residuo-
+6
−3,
+8
e diui-
ffectus,
. Hinc
lo non-
quentes
ı+bb;
-2bb;
10 bb.
esidua,
ım 31
Theo-

Theorema V.

§. 30. Si diuisor P fuerit numerus primus formae $4q + 1$, tum numerus -1 seu $P - 1$ certe in ordine residuorum reperitur.

Demonstratio.

Sit α residuum quodcunque, eritque etiam eius reciprocum $\frac{1}{\alpha}$ seu $\frac{1+nP}{\alpha}$ residuum (19), quod, nisi sit vel $\alpha = +1$ vel $\alpha = -1$, ab α erit diuersum, ita vt exceptis his duobus casibus cuilibet residuo α respondeat suum reciprocum, quod sit α', ab α diuersum; vbi notetur ipsius α' reciprocum vicissim esse α. Quare si -1 inter residua non reperiretur, omnia residua ita repraesentari possent, binis reciprocis coniungendis:

$$\begin{array}{l} 1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \text{etc.} \\ \quad \alpha',\ \beta',\ \gamma',\ \delta',\ \text{etc.} \end{array}$$

sicque cum omnia sint diuersa, numerus omnium residuorum foret impar. Cum autem diuisor sit numerus primus formae $4q + 1$, numerus omnium residuorum est $2q$, ideoque par; vnde necessario sequitur, inter residua quoque numerum -1, seu $P - 1$ occurrere, quia alioquin numerus residuorum foret impar.

Corollarium 1.

§. 31. Cum ergo pro diuisore primo $P = 4q + 1$ numerus -1 certe inter residua reperiatur, si aliud residuum quodcunque fuerit α, inter residua etiam occurret $-\alpha$.

Corol.

Corollarium 2.

§. 32. Si igitur quadratum aa per diuiforem primum $4q+1$ diuifum relinquat refiduum α, aliud dabitur quadratum bb, quod refiduum praebebit $-\alpha$, vnde horum quadratorum fumma $aa+bb$ certe erit per numerum primum $4q+1$ diuifibilis;

Corollarium 3.

§. 33. Quoniam omnia refidua ex quadratis, quorum radices femiffem diuiforis non fuperant, nafcuntur, quadrato quocunque propofito aa aliud femper bb non maius quam $4qq$ exhiberi poteft, vt fumma $aa+bb$ prodeat diuifibilis per $4q+1$.

Corollarium 4.

§. 34. Si $1+aa$ diuifionem per $4q+1$ admittat, tum etiam $bb+aabb$, ac proinde quoque $bb+(ab-(4q+1)n)^2$ diuifionem admittet, ficque altero quadrato bb pro lubitu affumto alterum $(ab-(4q+1)n)^2$ facile reperitur.

Corollarium 5.

§. 35. Si haec duorum quadratorum fumma $aa+bb$ per diuiforem $4q+1$ fuerit diuifibilis, tum etiam $aaxx+bbxx$, ac proinde quoque haec forma:

$$(ax-(4q+1)m)^2+(bx-(4q+1)n)^2$$

diuifionem admittet. Semper autem x ita affumere licet, vt alterius radix $ax-(4q+1)m$ dato numero c aequetur, fumendo $x=\frac{c+(4q+1)m}{a}$, quod femper in integris fieri poteft.

Scho-

iuiforem pri-
alind dabi-
-α, vnde ho-
t per nume-
adratis, quo-
, nafcuntur,
per bb non
a aa+bb
4q+1 ad-
ade quoque
tet, ficque
-(4q+1)n)²
um fumma
ibilis, tum
aec forma:
1)n)²
unere licet,
ero c aeque-
in integris
Scho-

Scholion 1.

§. 36. Pro quouis diuifore primo, fiue fit formae $4q+1$, fiue $4q+3$, numerorum reciprocorum confideratio omnem attentionem meretur, cum inde tam facile hanc infignem veritatem elicuerimus, quod, propofito numero primo quocunque formae $4q+1$, femper fummae binorum quadratorum exhiberi queant per illum diuifibiles. Cum igitur demonftrari praeterea poffit, fummam duorum quadratorum alios non admittere diuifores, nifi qui ipfi fint fummae duorum quadratorum, hoc modo Theorematis Fermatiani, quod omnes numeri primi formae $4q+1$ fint duorum quadratorum aggregata, demonftratio multo expeditius abfoluitur, quam quidem olim a me eft factum. Quemadmodum autem numeri reciproci pro quouis diuifore P fe habeant, dum cuiusuis numeri a reciprocus eft $\frac{1+nP}{a}$, ex fubiunctis exemplis clarius intelligetur:

Diuifor

Diuifor	Reciprocorum paria
3	- - -
5	2 3
7	2,3 4,5
11	2,3,5,7 6,4,9,8
13	2,3, 4,5, 6 7,9,10,8,11
17	2,3, 4,5, 8,10,11 9,6,13,7,15,12,14
19	2, 3,4, 6, 7, 8, 9,14 10,13,5,16,11,12,17,15
23	2,3,4, 5, 7, 9,11,13,15,17 12,8,6,14,10,18,21,16,20,19
29	2, 3, 4,5, 7, 8, 9,12,14,16,18,19,23 15,10,22,6,25,11,13,17,27,20,21,26,24

Singula haec paria reciproca ita inter se sunt connexa, vt quilibet numerus vnicum tantum recipiat reciprocum, diuisore scilicet minorem, prorsus vti in Theoremate assumsimus.

§. 37.

8,19,23
1,26,24
sunt connexa,
t reciprocum,
heoremate as-
§. 37.

Scholion 2.

§. 37. Quodsi ergo diuisor primus fuerit formae $4q+1$, videamus quomodo residua secundum hanc legem reciprocorum disposita se sint habitura:

Diuisor	Residua
5	1,4 1,(−1)
13	1,4,9,3,12,10 1, 4,9,12 10,3,(−1)
17	1,4,9,16,8,2,15,13 1, 4,9, 8,16 13,2,15,(−1)
29	1,4,9,16,25,7,20,6,23,13,5,28,24,22 1, 4, 9,16,25,6,23,28 22,13 20, 7,5,24,(−1)
37	1,4.9,16.25.36,12,27.7.26.10,33.21,11.3,34.30.28 1, 4, 9,16,25,12,27,26,21,36 28,33, 7, 3,34,11,10,30,(−1)

Ex his exemplis perspicuum est, cum vnitas sit solitaria, et reliquorum residuorum quodque suum reciprocum habeat adiunctum, numerum residuorum futurum esse imparem, nisi praeter vnitatem aliud residuum solitarium accederet, quod sibi ipsi esset reciprocum. Quoniam igitur his casibus, quibus diuisor est numerus primus formae $4q+1$, numerus reſiduorum certo eſt par $= 2q$, neceſſe eſt vt praeter vnitatem, reſiduum $4q$ vel -1 occurrat, cuius quippe reciprocum ipſi eſt aequale. Vnde veritas inſignis iſtius Theorematis, cuius demonſtratio alioquin maxime erat difficilis, admodum fit perſpicua: quod ſcilicet, quoties diuiſor ſit numerus primus formae $4q+1$, inter reſidua ſemper occurrat numerus $4q$ vel -1.

Scholion 3.

§. 38. Quemadmodum hinc patet numerum -1 inter reſidua reperiri, quoties diuiſor fuerit numerus primus formae $4q+1$, ita pro quouis alio numero primo s, diuiſorum primorum forma aſſignari, at nondum demonſtrari poteſt, vt iſte numerus s in reſiduis reperiatur. Cuiusmodi eſt hoc Theorema:

Si diuiſor primus fuerit formae $4ns+(2x+1)^2$, existente s numero primo, tum in reſiduis occurrent numeri $+s$ et $-s$.

alterumque huic ſimile:

Si diuiſor primus fuerit formae $4ns-(2x+1)^2$ existente s numero primo, tum in reſiduis occurret numerus $+s$; at $-s$ erit in non-reſiduis

Quando autem viciſſim $-s$ occurrat in reſiduis, at $+s$ in non-reſiduis, ita in genere definiri nequit. Pro caſibus autem particularibus res ita ſe habere deprehenditur,

vt ſit diuiſor primus debet eſſe

$\left.\begin{matrix}-2 \text{ reſiduum}\\ +2 \text{ non-reſiduum}\end{matrix}\right\} P = 8n+3$

ceſſe eſt vt
rrat, cuius
itas inſignis
in maxime
cet, quoties
ater reſidua

nerum -1
merus pri-
o primo s,
m demon-
tiatur. Cu-

$+1)^2$, exis-
occurrent

$+1)^2$ exis-
ccurret nu-

; at $+s$
Pro caſibus
litur,

-3

$\left.\begin{matrix}-3 \text{ reſiduum}\\ +3 \text{ non-reſiduum}\end{matrix}\right\} P = 12n+7$

$\left.\begin{matrix}-5 \text{ reſiduum}\\ +5 \text{ non-reſiduum}\end{matrix}\right\} P = 20n+3, 7$

$\left.\begin{matrix}-7 \text{ reſiduum}\\ +7 \text{ non-reſiduum}\end{matrix}\right\} P = 28n+11, 15, 23$

$\left.\begin{matrix}-11 \text{ reſiduum}\\ +11 \text{ non-reſiduum}\end{matrix}\right\} P = 44n+3, 15, 23, 27, 31$

$\left.\begin{matrix}-13 \text{ reſiduum}\\ +13 \text{ non-reſiduum}\end{matrix}\right\} P = 52n+7, 11, 19, 15, 31, 47$

$\left.\begin{matrix}-17 \text{ reſiduum}\\ +17 \text{ non-reſiduum}\end{matrix}\right\} P = 68n+3, 7, 11, 23, 27, 31, 39, 63$

$\left.\begin{matrix}-19 \text{ reſiduum}\\ +19 \text{ non-reſiduum}\end{matrix}\right\} P = 76n+7, 11, 19, 23, 35, 39, 43, 47, 55, 63$

$\left.\begin{matrix}-23 \text{ reſiduum}\\ +23 \text{ non-reſiduum}\end{matrix}\right\} P = 92n+3, 23, 27, 31, 35, 39, 47, 55, 59, 71, 75, 87$

Quorum caſuum contemplatio hoc ſuppeditat Theorema:

Si diuiſor primus fuerit formae $4ns-4z-1$, excludendo omnes valores in forma $4ns-(2x+1)^2$ contentos, exiſtente s numero primo, tum in reſiduis occurret $-s$, at $+s$ erit non-reſiduum.

Quibus Theorematibus inſuper hoc adiungi poteſt.

Si diuiſor primus fuerit formae $4ns+4z+1$, excludendo omnes valores in forma $4ns+(2x+1)^2$ contentos, exiſtente s numero primo, tum tam $+s$ quam $-s$ in non-reſiduis occurret.

Theoremata haec ideo ſubiungo, vt qui huiusmodi ſpeculalationibus delectantur, in eorum demonstrationem inquirant, cum nullum sit dubium, quin inde Theoria numerorum insignia incrementa sit adeptura.

Conclusio.

§. 39. Quatuor haec Theoremata postrema, quorum demonstratio adhuc desideratur, sequenti modo concinnius exhiberi possunt:

Existente s numero quocunque primo, diuidantur tantum quadrata imparia 1, 9, 25, 49, etc. per diuisorem 4s, notenturque residua, quae omnia erunt formae $4q+1$, quorum quoduis littera α indicetur, reliquorum autem numerorum, formae $4q+1$, qui inter residua non occurrunt, quilibet littera $\mathfrak{A}$ indicetur, quo facto si fuerit

diuisor numerus primus formae	tum est
$4ns+\alpha$	$+s$ residuum et $-s$ residuum
$4ns-\alpha$	$+s$ residuum et $-s$ non-residuum
$4ns+\mathfrak{A}$	$+s$ non-residuum et $-s$ non-residuum
$4ns-\mathfrak{A}$	$+s$ non-residuum et $-s$ residuum.

OBSER-

onem inqui-
heoria nume-
strema, quo-
i modo con-
ntur tantum
per diuisorem
erunt formae
licetur, reli-
$+1$, qui in-
ra $\mathfrak{A}$ indice-
n
siduum
on-residuum
siduum.
OBSER-

OBSERVATIONES ANALYTICAE.

§. 1.

Inter alia, quae passim de fractionibus continuis sum commentatus, notatu digna videtur haec forma:

$$1+\cfrac{n}{2+\cfrac{n+1}{3+\cfrac{n+2}{4+\cfrac{n+3}{5+\cfrac{n+4}{6+\text{etc.}}}}}}$$

cuius valor, quoties n est numerus integer, sequenti modo exhiberi potest, denotante e numerum, cuius logarithmus est vnitas, vt sit $e = 2,718281828459045$

$$1+\cfrac{1}{2+\cfrac{2}{3+\cfrac{3}{4+\cfrac{4}{5+\text{etc.}}}}} = \frac{1}{e-2};$$

$$1+\cfrac{2}{2+\cfrac{3}{3+\cfrac{4}{4+\cfrac{5}{5+\text{etc.}}}}} = e-1;$$

L 3

1+