1783

Disquitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta

Leonhard Euler

tem eſt dubium, quin ea patefacta multa praeclara incrementa Analyſeos expectare liceat. Cum igitur prior forma finita euadat, ſi fuerit $g = (\alpha - i\gamma)(\beta + (i+1)\delta)$, intelligimus etiam poſterioris valorem rationaliter exprimi poſſe, quoties fuerit

$$f = (\alpha - i\gamma)(\beta + (i+1)\delta) - \alpha(\beta + \delta)$$

ſeu

$$f = i(\alpha\delta - \beta\gamma - (i+1)\gamma\delta),$$

denotante i numerum integrum quemcunque.

DIS-

lara incre-
rior forma
1) δ), intel-
r exprimi
IEX
S
mc
dit
prc
idq
red
ma
gat
be
na
dit
Eu
DIS-

DISQVISITIO ACCVRATIOR CIRCA RESIDVA EX DIVISIONE QVADRATORVM ALTIORVMQVE POTESTATVM PER NVMEROS PRIMOS RELICTA.

§. 1.

Si numerus quadratus aa per numerum primum p diuidatur, reſiduum relictum littera α indicetur; ſimilique modo litterae β, γ, δ, etc. mihi denotabunt reſidua in diuiſione quadratorum bb, cc, dd, etc. relicta.

§. 2. Erit ergo $\alpha = aa - np$, quia reſiduum α prodit, ſi a quadrato aa multiplum numeri p auferatur, idque maximum, vt reſiduum α ipſo diuiſore p minus reddatur. Nihil autem impedit, quominus multiplum np maius accipiatur quadrato aa, vnde reſiduum α prodit negatiuum, ſicque eius valor infra $\frac{1}{2}p$ deprimi poteſt.

§. 3. Idem igitur reſiduum α multis modis exhiberi poteſt, quoniam cunctae hae formae $\alpha \pm mp$ eandem naturam continent. Perinde ſcilicet eſt, ſiue reſiduum ex diuiſione quadrati aa per numerum p ortum dicatur eſſe α, ſiue

$\alpha \pm p$, siue $\alpha \pm m p$, denotante littera m numerum integrum quemcunque.

§. 4. Innumera autem quadrata $a a$, per numerum p diuisa, idem relinquunt residuum α, quae omnia ex cognito vno $a a$ facile inueniuntur. Cuncta haec quadrata ista forma $(a \pm m p)^2$ vel $(m p \pm a)^2$ contineri euidens est; sicque sufficit residuum ex harum forma minima, cuius radix non excedet $\frac{1}{2} p$, notasse: omnia scilicet haec quadrata $(m p \pm a)^2$ respectu numeri p eiusdem indolis sunt censenda.

§. 5. Quadratis secundum ordinem naturalem dispositis, residua per diuisorem p orta ita se habebunt:

Quadrata: $1, 2^2, 3^2, 4^2, \ldots (p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2$
Residua: $1, 4, 9, 16, \ldots 16, \quad 9, \quad 4, \quad 1.$

Quadratis ergo ad $(p-1)^2$ continuatis, singula residua bis occurrunt; et quia p est numerus primus, eorum numerus est par, et bina quadrata media $(\frac{p-1}{2})^2$ et $(\frac{p+1}{2})^2$, idem dabunt residuum $\frac{pp-2p+1}{4}$.

§. 6. Omnia ergo residua, quae quidem ex diuisione numerorum quadratorum per numerum primum p resultare possunt, nascuntur ex his quadratis:

Quadr.	$1,$	$2^2,$	$3^2,$	$4^2,$	$- - - -$	$(\frac{p-1}{2})^2$
Resid.	$1,$	$4,$	$9,$	$16,$	$- - - -$	$\frac{pp-2p+1}{4}$

quorum numerus est $= \frac{p-1}{2}$. Neque ergo omnes numeri diuisore p minores, quorum multitudo est $p-1$, inter residua occurrunt, sed eorum semissis inde certe excluditur.

§. 7.

merum integrum
e numerum
mnia ex co-
ec quadrata
eri euidens
minima, cu-
t haec qua-
ndolis sunt
uralem di-
bunt:
$2)^2, (p-1)^2$
1.
esidua bis
numerus
$)^2$, idem
ex diui-
rimum p
$)^2$
$2p+1$
mes nu-
-1, in-
erte ex-
§. 7.

§. 7. Continuatis autem quadratis ad $(\frac{p-1}{2})^2$, residua inde orta omnia sunt diuersa: neque enim vllum vsque ad hunc terminum bis occurrere potest, siquidem diuisor p sit numerus primus. Namque si bina quadrata $a a$ et $b b$, neutro quadratum $(\frac{p-1}{2})^2$ excedente, idem darent residuum r, differentia eorum $a a - b b$, ideoque vel $a - b$ vel $a + b$, per p diuidi posset. Cum autem neque a neque b superet $\frac{p-1}{2}$, etiam summa $a + b$ minor erit quam p, ideoque fieri omnino nequit, vt ea summa, ac multo minus differentia $a - b$, diuisionem per numerum p admittat.

§. 8. Proposito ergo numero primo p omnia residua ex his quadratis $1, 2^2, 3^2, 4^2 \ldots (\frac{p-1}{2})^2$ obtinentur, quorum numerus cum sit $= \frac{p-1}{2}$, et residua omnia inter se differant, numerorum ipso p minorum, quorum multitudo est $p-1$, semissis certe inter residua occurrit; semissis vero inde excluditur, et classem non-residuorum constituit. Pro quolibet ergo numero primo p residua a non-residuis probe sunt discernenda.

§. 9. Si enim α inter residua occurrat, pronunciare possumus, innumerabilia quadrata dari, quae in hac forma $n p + \alpha$ contineantur, ac minimi eorum radicem non excedere numerum $\frac{p-1}{2}$. Sin autem numerus $\mathfrak{A}$ inter residua non reperiatur, pronunciabimus nullum numerum quadratum in forma $n p + \mathfrak{A}$ contineri. Quouis autem casu tam residuorum α quam non-residuorum $\mathfrak{A}$ multitudo est $= \frac{p-1}{2}$.

§. 10.

§. 10. Quodſi reſidua, ex diuiſione quadratorum per numerum primum p oriunda, ſecundum hunc ordinem naturalem diſponantur, primo occurrent numeri quadrati 1, 4, 9, 16, etc: donec diuiſione per numerum p ad minores numeros redigi poſſunt: poſtremum vero eorum erit $\frac{pp-2p+1}{4}$, vnde numerum p, quoties fieri poteſt, auferri oportet.

§. 11. Ad hoc poſtremum reſiduum agnoſcendum duos caſus contemplari conuenit, prout numerus primus p fuerit formae vel $4q+1$, vel $4q+3$. Sit primo $p=4q+1$, ideoque $\frac{p-1}{2}=2q$, et vltimum reſiduum $4qq$, quod ſubtractione multipli $qp=4qq+q$ reducitur ad $-q$, ſeu ad $3q+1$. Altero vero caſu $p=4q+3$, ſeu $\frac{p-1}{2}=2q+1$, vltimum reſiduum $4qq+4q+1$ ablatione multipli $qp=4qq+3q$ reducitur ad $q+1$.

§. 12. Simili modo penultimum reſiduum, ex quadrato $(\frac{p-3}{2})^2$ ortum, reperitur:

Pro caſu $p=4q+1$; $4qq-4q+1$, ſeu $-5q+1$, ſeu $-q+2$:

Pro caſu $p=4q+3$; $4qq+1$, ſeu $-3q$; ſeu $q+3$.

At antepenultimum, ex $(\frac{p-5}{2})^2$ ortum, ita prodit:

Pro caſu $p=4q+1$; $4qq-8q+4$, ſeu $-9q+4$, ſeu $-q+6$

Pro caſu $p=4q+3$; $4qq-4q+1$, ſeu $-7q+1$, ſeu $q+7$.

Quod vero antepenultimum praecedit, hoc modo:

Pro caſu $p=4q+1$; $4qq-12q+9$, ſeu $-13q+9$, ſeu $-q+12$

Pro caſu $p=4q+3$; $4qq-8q+4$, ſeu $-11q-4$, ſeu $q+13$.

adratorum ordinem quadrati p ad mi- orum erit 1, auferri

oſcendum primus p it primo reſiduum 7 reduci- $4q+3$, $4q+1$ $q+1$.

ex qua- u $-q+2$ $+3$. t: u $-q+6$ u $q+7$. $-q+12$ $q+13$.

§. 13.

§. 13. Hos igitur binos caſus diſtinguendo, reſidua ſequenti modo ſe habebunt:

Caſu $p=4q+1$.

Quadr. $1;\ 2^2,\ 3^2,\ 4^2 \ldots (2q-3)^2;\ (2q-2)^2;\ (2q-1)^2;\ (2q)^2$

Reſidua: $1,\ 4;\ 9,\ 16 \ldots -q+12;\ -q+6,\ -q+2,\ -q$

ſeu $3q+13,\ 3q+7;\ 3q+3;\ 3q+1$.

Caſu $p=4q+3$.

Quadr. $1;\ 2^2,\ 3^2,\ 4^2 \ldots (2q-2)^2,\ (2q-1)^2,\ (2q)^2,\ (2q+1)^2$

Reſidua: $1,\ 4,\ 9,\ 16 \ldots q+13;\ q+7,\ q+3,\ q+1$.

Priori ſcilicet caſu in genere occurrit reſiduum $-q+nn+n$ ſeu $3q+nn+1$, poſteriori vero $q+nn+n+1$.

§. 14. Quo hic reſiduorum ordo clarius perſpiciatur, exempla ſpectanda proponam, et primo quidem pro numeris primis formae $p=4q+1$.

$$\begin{matrix} p=5 \\ q=1 \end{matrix}\left\{\begin{matrix} 1; & 2^2 \\ 1, & 4 \\ \text{ſeu } 1; & -1 \end{matrix}\right.$$

$$\begin{matrix} p=13 \\ q=3 \end{matrix}\left\{\begin{matrix} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2 \\ 1; & 4, & 9, & 3, & 12, & 10 \\ \text{ſeu } 1; & 4, & -4, & 3, & -1, & -3 \end{matrix}\right.$$

$$\begin{matrix} p=17 \\ q=4 \end{matrix}\left\{\begin{matrix} 1; & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2 \\ 1, & 4, & 9, & 16, & 8, & 2, & 15, & 13 \\ \text{ſeu } 1, & 4, & -8, & -1, & 8, & 2, & -2, & -4 \end{matrix}\right.$$

$$\begin{matrix} p=29 \\ q=7 \end{matrix}\left\{\begin{matrix} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2, & 9^2, & 10^2, & 11^2, & 12^2, & 13^2, & 14^2 \\ 1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22 \\ \text{ſeu } 1, & 4, & 9, & -13, & -4, & 7, & -9, & 6, & -6, & 13, & 5, & -1, & -5, & -7 \end{matrix}\right.$$

$p=37 \left.\right\}$ $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2$
$q=9 \left.\right\{$ $1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28$
seu $1, 4, 9, 16, -12, -1, 12, -10, 7, -11, 10, -4, -16, 11, 3, -3, -7, -9$

$p=41 \left.\right\}$ $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2, 19^2, 20^2$
$q=10 \left.\right\{$ $1, 4, 9, 16, 25, 36, 8, 23, 40, 18, 39, 21, 5, 32, 20, 10, 2, 37, 33, 31$
seu $1, 4, 9, 16, -16, -5, 8, -18, -1, 18, -2, -20, 5, -9, 20, 10, 2, -4, -8, -10$

vbi obferuare licet, in refiduis per negatiua ad minimam formam reductis, fingulos numeros bis, politiue fcilicet et negatiue occurrere.

§. 15. Sequentia exempla pertinent ad numeros primos formae $p = 4q + 3$.

$p=3 \left\{ 1 \right.$ | $p=7 \left\{ 1, 2^2, 3^2 \right.$
$q=0 \left\{ 1 \right.$ | $q=1 \left\{ 1, 4, 2 \right.$
seu $1, -3, 2$

$p=11 \left\{ 1, 2^2, 3^2, 4^2, 5^2 \right.$
$q=2 \left\{ 1, 4, 9, 5, 3 \right.$
seu $1, 4, -2, 5, 3$

$p=19 \left\{ 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2 \right.$
$q=4 \left\{ 1, 4, 9, 16, 6, 17, 11, 7, 5 \right.$
seu $1, 4, 9, -3, 6, -2, -8, 7, 5$

$p=23 \left\{ 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2 \right.$
$q=5 \left\{ 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 \right.$
seu $1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6$

$p=31 \left\{ 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2 \right.$
$q=7 \left\{ 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8 \right.$
seu $1, 4, 9, -15, -6, 5, -13, 2, -12, 7, -3, -11, 14, 10, 8$

$p=$

$p=43 \left\{ 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2, 19^2, 20^2 \right.$
$q=10 \left\{ 1, 4, 9, 16, 25, 36, 6, 21, 38, 14, 35, 15, 40, 24, 10, 41, 31, 23, 17, 13 \right.$
seu $1, 4, 9, 16, -18, -7, 6, 21, -5, 14, -8, 15, -3, -19, -10, -2, -12, -20, 17, 13$.

In iftis refiduis ad minimam formam reductis omnes plane numeri ab vnitate vsque ad $2q+1$ occurrunt, alii figno pofitionis, alii negationis affecti. Verum has proprietates obferuatas demonftrari oportet.

§. 16. Iam fupra, p. 69. demonftraui, fi inter refidua, ex diuifione quadratorum per numerum p orta, occurrant numeri α et β, ibidem quoque reperiri productum $\alpha\beta$, ac proinde quoque hanc formam latius patentem $\alpha^m \beta^n$. Oriantur enim haec refidua ex quadratis aa et bb, ita vt fit $aa = mp + \alpha$ et $bb = np + \beta$, atque manifeftum eft ex horum quadratorum producto

$$aabb = mnpp + (m\beta + n\alpha)p + \alpha\beta,$$

cuius forma eft $Mp + \alpha\beta$, nafci refiduum $\alpha\beta$; fimilique modo ex quadrato $a^{2m} b^{2n}$ prouenire refiduum $\alpha^m \beta^n$, feu $\alpha^m \beta^n - Mp$, vt ad minimam formam reducatur. Quin etiam notari conuenit, hoc ipfum refiduum $\alpha^m \beta^n$ nafci ex omnibus his quadratis: $(a^m b^n \pm Np)^2$ feu $(Np \pm a^m b^n)^2$, ideoque ex quadrato, cuius latus $a^m b^n - Np$ feu $Np - a^m b^n$ minus erit quam $\frac{1}{2}p$.

§. 17. Denotent litterae $a, b, c, d, \ldots\ldots l$ omnes numeros diuiforis p femiffe $\frac{1}{2}p$ minores, quorum ergo multitudo eft $= \frac{p-1}{2}$, fintque $\alpha, \beta, \gamma, \delta, \ldots\ldots \lambda$ refidua ex eorum quadratorum $a^2, b^2, c^2, d^2, \ldots\ldots l^2$ per numerum p diuifione relicta, quorum multitudo itidem eft $= \frac{p-1}{2}$, ita vt ex omnibus numeris diuifore p mi-

minoribus, quorum multitudo est $p-1$, totidem ex residuorum ordine excludantur, quos nomine non-residuorum complexos litteris $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \ldots \mathfrak{L}$ indicabo. Notatu ergo maxime dignum est, in ordine residuorum $\alpha, \beta, \gamma, \delta, \ldots \lambda$, etiamsi eorum multitudo tantum est $= \frac{p-1}{2}$, tamen omnia eorumdem producta ex binis pluribusque, atque etiam singulorum potestates omnes occurrere; siquidem auferendo inde, quoties fieri potest, diuisorem p, ad minimam formam reuocentur.

§. 18. Quo magis haec illustrentur, animaduerti oportet, ratione cuiusque diuisoris p omnes numeros in totidem species distribui; scilicet ratione diuisoris 2 duae habentur species numerorum parium et imparium formulis $2x$ et $2x+1$ contentorum. Diuisor autem 3 tres praebet numerorum species $3x$, $3x+1$ et $3x+2$, et diuisor 4 has quatuor $4x$, $4x+1$, $4x+2$ et $4x+3$, quae diuersae species in numerorum doctrina sollicite distingui solent. Simili ergo modo ratione diuisoris cuiusque p, hae diuersae numerorum species constituuntur:

$$px;\ px+1;\ px+2;\ px+3;\ \ldots\ldots px+p-1$$

quarum multitudo est p. Omissa ergo prima specie px multipla diuisoris p continente, reliquarum multitudo est $p-1$; ac si p fuerit numerus primus, has species in duas classes diuidi conuenit, vtraque $\frac{p-1}{2}$ species complectente:

$$px+\alpha,\ px+\beta,\ px+\gamma,\ px+\delta,\ \ldots\ldots px+\lambda$$
$$px+\mathfrak{A},\ px+\mathfrak{B},\ px+\mathfrak{C},\ px+\mathfrak{D},\ \ldots\ldots px+\mathfrak{L}$$

ita vt omnes numeri quadrati in priori classe contineantur, posterior vero classis naturae quadratorum prorsus aduersetur.

tidem ex resi-
on-residuorum
indicabo. No-
siduorum α, β,
o tantum est
ex binis plu-
omnes occur-
potest, diuiso-

, animaduerti
s numeros in
uisoris 2 duae
rium formulis
m 3 tres prae-
$x+2$, et di-
et $4x+3$,
a sollicite di-
uisoris cuius-
tituuntur:
$px+p-1$
a specie px
multitudo est
in duas
complectente:
$\ldots px+\lambda$
$\ldots px+\mathfrak{L}$
contineantur,
rorsus aduer-

§. 19.

§. 19. Pro quolibet ergo diuisore primo p his duabus classibus constitutis, quarum vtraque $\frac{p-1}{2}$ species continet, et quae ambae coniunctim omnes plane numeros continent, exceptis multiplis ipsius p, quippe quorum iudicium est in promtu, omnes numeri in priori classe contenti hac gaudent proprietate, vt producta ex binis in eadem classe contineantur, in qua ergo simul non solum potestates singulorum quaecunque, sed etiam producta ex binis pluribusque harum potestatum occurrunt. Prior igitur classis, quam voco residuorum, numeris $\alpha, \beta, \gamma, \delta, \ldots\ldots \lambda$ determinatur, dum altera classis non-residuorum numeris $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \ldots\ldots \mathfrak{L}$ definitur.

§. 20. Demonstraui deinde etiam, si in classe residuorum occurrant duo numeri r et rs, quorum ille r huius rs sit factor, tum etiam huius alterum factorem in eadem classe reperiri. Cum enim dentur duo quadrata aa et bb, vt formae $aa-r$ et $bb-rs$ fiat per numerum primum p diuisibiles, existentibus numeris a et b ipso p minoribus, etiam forma $aas-rs$ per p est diuisibilis, hincque etiam differentia $bb-aas$, et $(b+np)^2-aas$. Cum autem a et b sint ipso p minores, semper n ita assumere licet, vt fiat $b+np=ma$. Ex quo talis forma $mmaa-aas$ dabitur per p diuisibilis, adeoque et haec, $mm-s$, ita vt sit $s=mm-np$, ac propterea numerus s inter residua reperiatur. Hinc sequitur, si r fuerit residuum, at s non-residuum, tum productum rs certe fore non-residuum; seu producta ex quouis residuo per non-residuum facta, veluti $\alpha\mathfrak{A}$, $\alpha\mathfrak{B}$, $\beta\mathfrak{A}$ inter non-residua reperiuntur.

§. 21. Si igitur $\mathfrak{A}$ fuerit non-reſiduum, omnia haec producta: $\alpha\mathfrak{A}$, $\beta\mathfrak{A}$, $\gamma\mathfrak{A}$, $\delta\mathfrak{A}$, - - - - $\lambda\mathfrak{A}$, erunt non-reſidua, quae cum ſint diuerſa inter ſe, etiam reductione ad minimam formam facta, eorumque numerus $= \frac{p-1}{2}$, in iis adeo omnia non-reſidua continentur. Ex quo iam perſpicuum eſt producta ex binis non-reſiduis, veluti $\alpha\beta\mathfrak{A}\mathfrak{A}$, ad claſſem reſiduorum eſſe referenda, quoniam $\alpha\beta$ eſt reſiduum, et $\mathfrak{A}\mathfrak{A}$, vtpote numerus quadratus, per ſe inter reſidua occurrit. Simul vero patet producta ex ternis non-reſiduis, vti $\mathfrak{A}\mathfrak{B}\mathfrak{C}$, iterum in claſſem non-reſiduorum cadere, producta vero ex quaternis inter ipſa reſidua reperiri, et ita porro.

§. 22. Praeterea vero etiam obſeruo ex datis binis reſiduis α et β per diuiſionem nouum reſiduum oriri, et fractionem $\frac{\alpha}{\beta}$ inter reſidua eſſe referendam. Etſi enim fractiones ex hac ratione prorſus excluduntur, tamen, quia numerus α aequiualens cenſetur huic formae generali, $\alpha + np$, vniuerſam ſpeciem continente, numerum n vtique ita accipere licet, vt $\frac{\alpha+np}{\beta}$ fiat numerus integer, de quo effatum eſt intelligendum, quod ſcilicet inter reſidua reperiatur. Hinc ergo omnes termini huius progreſſionis geometricae:

$$\alpha,\ \beta,\ \frac{\beta^2}{\alpha},\ \frac{\beta^3}{\alpha^2},\ \frac{\beta^4}{\alpha^3},\ \text{etc.}$$

ex binis reſiduis α et β continuatae, in claſſe reſiduorum continentur, ſi ſcilicet ſinguli ad formas integras reuocentur. Quodſi enim fractio $\frac{\beta}{\alpha}$ aequiualeat numero integro r, ſtatim ſequentes numeri integri obtinentur: α, β, βr, βr^2, βr^3, βr^4, etc. qui ad minimam formam reducti non plures quam $\frac{p-1}{2}$ numeros diuerſos praebere poſſunt.

§. 23.

§. 23. Conſideremus ergo hanc progreſſionem geometricam: α, β, βr, βr^2, βr^3, βr^4, etc. et cum omnes termini diuerſi eſſe nequeant, praebeant hi termini βr^m et βr^{m+n} per p diuiſi idem reſiduum, ita vt differentia $\beta r^{m+n} - \beta r^m$, ac propterea $r^n - 1$ per p fiat diuiſibilis. Tum ergo etiam termini β et βr^n, atque etiam α et βr^{n-1} ratione reſidui conuenient; ex quo patet, plura reſidua diuerſa prodire non poſſe, quam quae oriuntur ex his terminis initialibus: α, β, βr, βr^2, - - - - βr^{n-2}, quoniam ex ſequentibus βr^{n-1}, βr^n, βr^{n+1}, etc. eadem reſidua eodem ordine recurrunt; quorum ergo reſiduorum, ſiquidem fuerint diuerſa, multitudo maior eſſe nequit quam $\frac{p-1}{2}$; quod euenit ſi r^n ſit minima poteſtas ipſius r, quae vnitate minuta per p diuiſionem admittat. Hinc patet numerum n certe non ſuperare $\frac{p-1}{2}$; ac ſi fuerit $n = \frac{p-1}{2}$, omnia plane reſidua obtinentur.

§. 24. Sin autem ex terminis α, β, βr, βr^2, - - - - βr^{n-2}, non omnia reſidua prodeant, ſed quaedam omittantur, facile oſtenditur, ad minimum totidem omitti, quot adſunt. Si enim reſiduum γ inter ea non occurrat, quod etiam per $\alpha\delta$ repraeſentare licet, quoniam $\gamma + mp$ ſemper ad formam $\alpha\delta$ reuocari poteſt, tum etiam neque $\beta\delta$, neque $\beta\delta r$, neque $\beta\delta r^2$, etc. inter ea reſidua reperietur, quae cum ſint diuerſa, excluſo vno ſimul n excluduntur, vnde $2n$ numerum omnium $\frac{p-1}{2}$ ſuperare nequit. Erit ergo vel $2n = \frac{p-1}{2}$ vel $2n < \frac{p-1}{2}$, et poſteriori caſu adhuc de nouo ad minimum n reſidua excluduntur. Quare cum termini progreſſionis geometricae α, β, βr, βr^2, - - - βr^{n-2}, quorum numerus eſt n,

R 2 vel

vel omnia residua contineant ex quadratis orta, quorum multitudo est $= \frac{p-1}{2}$, vel inde exclusorum numerus fit $= n$, vel $= 2n$; vel $= 3n$, etc. euidens est numerum n necessario partem aliquotam ipsius $\frac{p-1}{2}$ esse debere, ideoque minimum exponentem n, quo potestas r^n vnitate minuta per p divisibilis reddatur, vel ipsi numero $\frac{p-1}{2}$, vel eiusdem parti cuipiam aliquotae esse aequalem.

§. 25. Siue autem fit $n = \frac{p-1}{2}$, siue eius parti cuidam aliquotae aequetur, semper forma $r^{\frac{1}{2}(p-1)} - 1$ diuisionem admittet per numerum primum p. Ponamus $p = 2q + 1$, vt fit $\frac{p-1}{2} = q$; ac si ex binis quadratorum residuis quibuscunque α et β, sumendo $r = \frac{\beta + ip}{\alpha}$, formetur haec progressio geometrica:

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \text{- - - - -}\ \beta r^{q-2},$$

terminorum numero existente $= q$, tum hinc vel omnia residua quadratorum, α, β, γ, δ, ε, - - - - - - λ, resultabunt, vel eorum tantum semissis, vel pars tertia vel pars quarta aliaue aliquota: simulque perspicitur, quot ab initio diuersa prodierint, eadem deinceps eodem ordine continuo repetitum iri. Semper autem termini sequentes βr^{q-1}, βr^q, βr^{q+1}, etc. eadem residua reproducent α, β, βr, quae initio habentur.

§. 26. Quoties ergo q est numerus primus, existente $p = 2q + 1$, tum progressio geometrica ex binis quadratorum residuis quibusque α et β formata et ad q terminos continuata:

ta, quorum multi-
is fit $= n$, vel $= 2n$;
necessario par-
ideoque minimum-
minuta per p di-
vel eiusdem parti
, siue eius parti
ma $r^{\frac{1}{2}(p-1)} - 1$
m p. Ponamus
nis quadratorum
$= \frac{\beta + ip}{\alpha}$, forme-
r^{q-2},
hinc vel omnia
- - - λ, resulta-
rs tertia vel pars
r, quot ab initio
em ordine conti-
rmini sequentes
reproducent α,
erus primus, ex-
metrica ex binis
formata et ad q
α,

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \text{- - - - -}\ \beta r^{q-2},$$

omnia plane quadratorum residua exhibebit, nullo neque excluso neque repetito. Omnia ergo reliqua residua γ, δ, ε, - - - - λ, cum tali quopiam termino βr^n, vt fit $n < q - 1$, conuenient. Sin autem numerus q fuerit compositus, puta $q = mn$ et $p = 2mn + 1$, tum euenire potest, vt non omnia residua quadratorum sic prodeant, sed tantum einsmodi pars aliquota ipsius q, qualem eius indoles admittit. Quod si vsu venit, tota progressio geometrica, q terminis constans, quasi sponte in duo pluraue membra distinguitur, in quibus eadem residua recurrunt.

§. 27. Cum sit $\frac{\beta}{\alpha} = r$, ideoque $\beta = \alpha r$, nostra progressio geometrica hoc modo expressa magis fit perspicua:

$$\alpha,\ \alpha r,\ \alpha r^2,\ \alpha r^3,\ \text{- - - - -}\ \alpha r^{q-1},$$

cuius omnes termini quia sunt per α multiplicati, hoc factore communi praetermisso, progressio simplicius ita exhiberi potest. Proposito scilicet diuisore primo $p = 2q + 1$, si residuum quodcunque fuerit α, singuli termini huius progressionis geometricae:

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \text{- - - - -}\ \alpha^{q-1}$$

quorum numerus est $= q$, inter residua quadratorum reperiuntur; ac si omnes ad diuersas species pertineant, etiam vniuersam residuorum classem implent. Fieri autem potest, vti vidimus, vt non omnia residua hoc modo prodeant, sed totius classis tantum pars aliquota, dum eadem post certam periodum iterum repetuntur, reliqua vero hinc prorsus excluduntur.

§. 28. Siue autem omnia quadratorum residua ex hac progressione geometrica nascantur, siue quaedam tantum pars aliquota, ea, quae terminis istius progressionis continentur, tam insignibus proprietatibus sunt praedita, vt operae omnino pretium sit eas accuratius euoluere. Primum igitur obseruo, si haec progressio geometrica vlterius continuetur, terminos sequentes α^q, α^{q+1}, α^{q+2}, etc. aequiualere primis 1, α, α^2, etc. propterea quod $\alpha^q - 1$ diuidi certe potest per diuisorem primum $p = 2q + 1$. Adiecto ergo termino sequente α^q vnitati aequiualente, ita vt habeamus

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ - - - -\ \alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1$$

quia productum ex primo termino in vltimum est $= 1$, ex natura progressionis geometricae sequitur, etiam producta ex secundo α in penultimum α^{q-1}, item ex tertio α^2 in ante-penultimum α^{q-2}, et in genere ex binis ab extremis aequidistantibus α^m et α^{q-m} ad vnitatem reduci.

§. 29. Dato ergo quocunque residuo α inter reliqua vnum reperietur β, ita vt productum $\alpha\beta$ vnitati aequiualeat, seu sit $\beta = \frac{1+np}{\alpha}$, vnde id facile inuenitur. Quia igitur haec duo residua α et β tali vinculo inter se colligantur, ea *sociata* nominabo; ex quo superioris progressionis geometricae bini termini ab extremis aequidistantes huiusmodi bina residua *sociata* suppeditant. Terminus scilicet penultimus α^{q-1} aequiualet ipsi β, antepenultimus α^{q-2} ipsi β^2 et ita porro, vnde si sociata subscribantur hoc modo:

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ - - - -\ \alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1$$
$$1,\ \beta,\ \beta^2,\ \beta^3,\ - - - -\ \beta^{q-3},\ \beta^{q-2},\ \beta^{q-1},\ 1$$

inse-

inferior series congruit cum superiori retro scripta. Semper autem residuum vnitati associatum quoque est vnitas.

§. 30. Consideratio horum residuorum sociatorum aperit nobis viam ad insignes proprietates detegendas. Cum enim, posito diuisore primo $p = 2q + 1$, sit numerus omnium residuorum $= q$, quorum cuilibet, praeter vnitatem, conuenit suum sociatum, vnitate exclusa reliqua, quorum numerus est $= q - 1$, secundum hanc sociationem in paria distribui possunt, binis sociatis inuicem iungendis. Hinc si $q - 1$ fuerit numerus impar, ac propterea q par, necesse est vt in hac distributione idem residuum, puta δ, bis occurrat. Verum idem residuum δ duobus diuersis residuis associari nequit: si enim esset $\alpha\delta = p$ et $\beta\delta = 1$, residua α et β non discreparent. Quare nihil aliud relinquitur, nisi vt idem residuum δ secum ipsum associetur, sitque idcirco $\delta\delta = 1$, vnde fit vel $\delta = 1$ vel $\delta = -1$; sed quia vnitas iam est seposita, necesse est hoc casu, quo q est numerus par, inter residua reperiri -1 vel $p - 1$.

§. 31. En ergo egregiam demonstrationem veritatis supra iam obseruatae, quod si diuisor primus sit $p = 4m + 1$, ideoque $q = 2m$, inter residua necessario occurrat -1, seu semper exhiberi queat quadratum aa, vt $aa + 1$ per illum numerum primum $p = 4m + 1$ diuidi possit. Hinc simul patet, si inter residua sit numerus α, ibidem quoque productum $-1 \cdot \alpha$, nempe $-\alpha$ occurrere, hincque omnia residua ad minimam formam reducta tam positiue quam negatiue adesse, omnino vti in exemplis §. 14. allatis perspicitur. Simul vero etiam patet,

patet, si fuerit $p = 4m + 3$, ideoque residuorum multitudo impar, ibi -1 locum habere non posse, quia tum singula residua vtroque signo $+$ et $-$ occurrerent, ideoque eorum numerus impar esse non posset. Ex quo sequitur, per huiusmodi numerum primum $p = 4m + 3$ nullam binorum quadratorum summam diuidi posse.

§. 32. Pro diuisoribus autem primis formae $p = 4m + 1$, si quadratum aa det residuum a, aliud semper dabitur quadratum bb, praebens residuum $-a$; sicque horum quadratorum summa $aa + bb$ per illum numerum primum erit diuisibilis, ita vt nec a nec b superet $2m$. Operae pretium ergo erit his casibus bina residua signo discrepantia iunctim exhibere, simulque quadrata, vnde nascuntur, adscribere.

$$p=5\begin{cases}\begin{array}{c}1^2\\ +1\\ -1\\ 2^2\end{array}\end{cases}\quad p=13\begin{cases}\begin{array}{ccc}1^2&2^2&4^2\\ +1;&+4;&+3\\ -1;&-4;&-3\\ 5^2&3^2&6^2\end{array}\end{cases}\quad p=17\begin{cases}\begin{array}{cccc}1^2&6^2&2^2&5^2\\ +1;&+2;&+4;&+8\\ -1;&-2;&-4;&-8\\ 4^2&7^2&8^2&3^2\end{array}\end{cases}$$

$$p=29\begin{cases}\begin{array}{ccccccc}1^2&2^2&11^2&8^2&6^2&3^2&10^2\\ +1;&+4;&+5;&+6;&+7;&+9;&+13\\ -1;&-4;&-5;&-6;&-7;&-9;&-13\\ 12^2&5^2&13^2&9^2&14^2&7^2&4^2\end{array}\end{cases}$$

$$p=37\begin{cases}\begin{array}{ccccccccc}1^2&15^2&2^2&9^2&3^2&11^2&14^2&7^2&4^2\\ +1;&+3;&+4;&+7;&+9;&+10;&+11;&+12;&+16\\ -1;&-3;&-4;&-7;&-9;&-10;&-11;&-12;&-16\\ 6^2&16^2&12^2&17^2&18^2&8^2&10^2&5^2&13^2\end{array}\end{cases}$$

$p =$

residuorum multi- 1 posse, quia tum currerent, ideoque Ex quo sequitur, $m + 3$ nullam bi- se.
m primis formae residuum a, aliud residuum $-a$; sic- bb per illum nu- t nec a nec b su- is casibus bina re- re, simulque qua-
$p =$

$$p=41\begin{cases}\begin{array}{cccccccccc}1^2&17^2&2^2&13^2&7^2&3^2&16^2&4^2&10^2&15^2\\ +1;&+2;&+4;&+5;&+8;&+9;&+10;&+16;&+18;&+20\\ -1;&-2;&-4;&-5;&-8;&-9;&-10;&-16;&-18;&-20\\ 9^2&11^2&18^2&6^2&19^2&14^2&20^2&5^2&8^2&12^2\end{array}\end{cases}$$

§. 33. Hinc euidens est, pro diuisore primo $p = 4m + 1$ tot modis, quot m continet vnitates, bina quadrata, radices limitem $2m$ non superantes habentia, assignari posse, quorum summa sit diuisibilis per numerum p. In his autem binis quadratis nulla lex, qua inter se cohaereant, perspicitur, aliorumque summa modo maior reperitur modo minor, ac minima quidem vbique ipsi numero p est aequalis. Num autem semper talis binorum quadratorum summa diuisori p aequalis detur, hinc non facile demonstrari posse videtur. Cum autem ex alio fonte demonstrauerim, binorum quadratorum summam alios non admittere diuisores, nisi qui ipsi sint binorum quadratorum summae, quoniam hic euictum est semper dari binorum quadratorum summas, quae sint per numerum primum $p = 4m + 1$ diuisibiles, iam certo constat omnes numeros primos formae $4m + 1$ esse summam duorum quadratorum. Praesens autem supplementum demonstrationem huius propositionis mirifice contrahit. Olim enim, nonnisi per multas ambages ostendi, dari semper eiusmodi binorum quadratorum summas, quae sint per quemlibet numerum primum formae $4m + 1$ diuisibiles, id quod hic in aprico est positum.

§. 34. Data autem duorum quadratorum summa $aa + bb$ per numerum primum p diuisibili, alias inde bino-

binorum quadratorum summas idem praestantes facile reperire licet.

1°. Si numeri a et b communem habeant diuisorem, vt sit $a = n c$ et $b = n d$, etiam summa quadratorum $cc + dd$ per p erit diuisibilis.

2°. Si numeri a et b ambo sint impares, ideoque $\frac{a+b}{2}$ et $\frac{a-b}{2}$ numeri integri, etiam horum quadratorum summa per p diuisionem admittet: semissis autem ea est praecedentis.

3°. Tum vero etiam hae quadratorum summae: $(p-a)^2 + (p-b)^2$, vel $a^2 + (p-b)^2$ per p erunt diuisibiles; vnde si radices communem sortiantur diuisorem, eo ad formam minorem redigi possunt.

4°. Si ergo sint ambo impares $a = 2c+1$ et $b = 2d+1$, ob $p = 4m+1$, horum quadratorum summa, $(2m-c)^2 + (2m-d)^2$, erit diuisibilis; et si alter par $a = 2c$, alter impar $b = 2d+1$, haec summa, $cc + (2m-d)^2$, erit per p diuisibilis; hocque modo continuo plures huiusmodi binorum quadratorum summas inuenire licet.

§. 35. Exemplo haec fient clariora. Sumto igitur diuisore $p = 41$, inuenta sit summa duorum quadratorum $17^2 + 11^2$ per eum diuisibilis, vt sit $a = 17$ et $b = 11$, atque per has regulas sequentes valores alii pro a et b reperientur:

$$p = 41;\ \begin{array}{l|l|l|l} a = 17 \;--\; 24 & 4 & 1 \;--\; 40 & 5 \\ b = 11 \;--\; 30 & 5 \;--\; 36 & 9 \;--\; 32 & 4 \end{array}$$

Tum

Tum vero porro ex casu quo alterutrer numerorum est $= 1$, alteri valor quicunque tribui, alterque ita definiri potest, vt infra $\frac{1}{2}p$ subsistat. Scilicet inuento casu $a = 1$ et $b = 9$, satisfacit quoque $a = m$ et $b = 9m$, vbi loco b sumi potest $9m - np$, seu $np - 9m$, ita vt b infra $\frac{1}{2}p$ deprimatur; sicque pro a omnes numeros accipere licebit.

$a=1$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$b=9$	18	14	5	4	13	19	10	1	8	17	15	6	3	12	20

etc.

Desideratur ergo methodus, inter omnes hos binos valores litterarum a et b eos inueniendi, quorum quadratorum summa sit minima, vt deinceps demonstretur, hanc summam ipsi diuisori 41 certe fore aequalem: quod quidem praesenti casu euenit, si litterarum a et b valores sint 4 et 5.

§. 36. Reuertor autem ad eam residuorum ex quadratis oriundorum dispositionem, qua ea secundum progressionem geometricam disponi posse obseruaui. Sit igitur diuisor primus $p = 2q + 1$, et residua inde ex quadratis orta ordine quocunque scripta $1, \alpha, \beta, \gamma, \delta \ldots \lambda$, quorum multitudo est $= q$, atque sequentes progressiones geometricae omnes in his residuis continebuntur:

$$\begin{array}{l} 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4 \;------\; \alpha^{q-1} \\ 1,\ \beta,\ \beta^2,\ \beta^3,\ \beta^4 \;------\; \beta^{q-1} \\ 1,\ \gamma,\ \gamma^2,\ \gamma^3,\ \gamma^4 \;------\; \gamma^{q-1} \\ 1,\ \delta,\ \delta^2,\ \delta^3,\ \delta^4 \;------\; \delta^{q-1} \\ \quad \text{etc.} \end{array}$$

in quibus omnibus termini sequentes $\alpha^q, \beta^q, \gamma^q, \delta^q \;---\; \lambda^q$ vnitati aequiualebunt, quippe qui omnes vnitate minuti per diuisorem p erunt diuisibiles. Huiusmodi ergo pro-

gressi-

gressiones geometricas tot exhibere licet, quot vnitates in q continentur; in iisque omnibus nullus terminus occurret, qui non inter residua 1, α, β, γ - - - - - λ reperiatur.

§. 37. Euenire autem potest, vt supra est ostensum, vt non omnes istae progressiones geometricae, etiamsi cuiusque terminorum numerus sit $= q$, omnia residua praebeant, sed tantum eorum vel semissem, vel trientem, vel etiam quampiam partem aliquotam; quod quibus casibus contingat, accuratius est perpendendum. Primum igitur obseruo, si q fuerit numerus primus, hoc nullo modo vsu venire posse; si enim in huiusmodi progressione geometrica q terminorum non omnia residua occurrant, eorum quae occurrunt singula vel bis, vel ter, vel aliquoties occurrant necesse est. Vnde si q est numerus primus, quaelibet progressio geometrica omnia residua diuersa numero q complectitur. Ita si $p = 11$ et $q = 5$, ex quinque residuis 1, 4, -2, 5, 3, ab vnitate incipiendo hae quatuor progressiones geometricae formantur:

	1,	4,	4^2,	4^3,	4^4		1,	-2,	2^2,	-2^3,	2^4
seu	1,	4,	5,	-2,	3	seu	1,	-2,	4,	3,	5
	1,	5,	5^2,	5^3,	5^4		1,	3,	3^2,	3^3,	3^4
seu	1,	5,	3,	4,	-2	seu	1,	3,	-2,	5,	4

vbi singula residua per omnia loca variantur praeter primum.

§. 38. Hinc euidens est, ex qualibet harum progressionum geometricarum reliquas facile formari posse, dum ex illa, per saltum transiliendo vel vnum, vel duos, vel plures

t vnitates in
minus occurs
- - - λ re
ra est osten-
ricae, etiamsi
esidua praebe-
em, vel etiam
sibus contin-
itur obseruo,
o vsu venire
metrica q ter-
um quae oc-
ies occurrant
us, quaelibet
a numero q
inque residuis
quatuor pro
praeter pri-
iarum progres-
ri posse, dum
vel duos, vel
plures

plures terminos, termini excerpuntur, hac numeratione, cum ad finem fuerit peruentum, iterum ab initio instituta. Ita si casum sumamus, quo $p = 23$ et $q = 11$, ac residua 1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6, vna progressione geometrica formata, cuius terminis indices inscribo, quo deinceps reliquae, terminis per saltum excerpendis, facilius exhiberi queant, decem progressiones geometricae ita se habebunt:

													Seq.
1.	Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10	0
	Progr.	1,	4,	-7,	-5,	3,	-11,	2,	8,	9,	-10,	6	1
2.	Indices	0,	2,	4,	6,	8,	10,	1,	3,	5,	7,	9	0
	Progr.	1,	-7,	3,	2,	9,	6,	4,	[illegible]	5,	8,	[illegible]	[illegible]
3.	Indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8	0
	Progr.	1,	-5,	2,	-10,	4,	3,	8,	6,	-7,	-11,	9	1
4.	Indices	0,	4,	8,	1,	5,	9,	2,	6,	10,	3,	7	0
	Progr.	1,	3,	9,	4,	-11,	-10,	-7,	2,	6,	-5,	8	1
5.	Indices	0,	5,	10,	4,	9,	3,	8,	2,	7,	1,	6	0
	Progr.	1,	-11,	6,	3,	-10,	-5,	9,	-7,	8,	4,	2	1
6.	Indices	0,	6,	[illegible]	7,	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	5	0
	Progr.	1,	2,	4,	8,	-7,	-9,	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1
7.	Indices	0,	7,	3,	10,	6,	2,	9,	5,	1,	8,	4	0
	Progr.	1,	8,	-5,	6,	-2,	-7,	-10,	-11,	4,	9,	3	1
8.	Indices	0,	8,	5,	2,	10,	7,	4,	1,	9,	6,	3	0
	Progr.	1,	9,	-11,	-7,	6,	8,	3,	4,	-10,	2,	-5	1
9.	Indices	0,	9,	7,	5,	3,	1,	10,	8,	6,	4,	2	0
	Progr.	1,	-10,	8,	-11,	5,	4,	6,	9,	[illegible]	-3,	-7	1

10.

10. $\begin{cases}\text{Indices } 0,\ 10,\ 9,\ 8,\ 7,\ 6,\ 5,\ 4,\ 3,\ 2,\ 1 \mid 0\\ \text{Progr. } 1,\ 6,\ -10,\ 9,\ 8,\ 2,\ -11,\ 3,\ -5,\ -7,\ 4 \mid 1\end{cases}$

Indices ſcilicet hic vltra 11 aſcenſuri ſubtrahendo 11 ſunt depreſſi. Hic porro obſeruari conuenit bina reſidua, quorum indices iuncti faciunt 11, ſeu in genere q, eſſe inter ſe ſociata, eorumque productum vnitati aequiualere. Hoc nempe caſu reſidua ſociata ſunt 4; −7; −5; 3; −11.
6; −10; 9; 8; 2.

§. 39. Conſideremus nunc quoque caſus, quibus q eſt numerus compoſitus, ac primo quidem duplus cuiuspiam numeri primi. Ab exemplo exordiamur quo $p = 13$ et $q = 6 = 2 \cdot 3$, ac reſidua haec: 1, 4, −4, 3, −1, −3, vnde hae quinque progreſſiones geometricae formentur:

I. 1, 4, 3, −1, −4, −3
II. 1, −4, 3, 1, −4, 3
III. 1, 3, −4, 1, 3, −4
IV. 1, −1, 1, −1, 1, −1
V. 1, −3, −4, −1, 3, 4

Vbi prima et quinta omnia continent reſidua; ſecunda vero et tertia eorum tantum ſemiſſem 1, −4, 3, quae bis repetuntur, reliquis, −1, +4, −3, excluſis: quarta vero duo tantum habet, +1 et −1, ter repetita. Similis ratio deprehenditur in caſu $p = 29$ et $q = 14 = 2 \cdot 7$, quo reſidua ſunt: 1, −1, 4, −4, 5, −5, 6 −6, 7, −7, 9, −9, 13, −13, vnde hae progreſſiones geometricae formantur:

I. 1, -1,| 1, -1,| 1, -1,| 1, -1 | 1, -1| 1, -1| 1, -1
II. 1, 4, -13, 6, -5, 9, 7, -1, -4, 13, -6, 5, -9, -7
III. 1, -4, -13, -6, -5, -9, 7,| 1, -4, -13, -6, -5, -9, 7

3, 2, 1 | 0
-5, -7, 4 | 1
hendo 11 ſunt
a reſidua, quo-
q, eſſe inter ſe
quiualere. Hoc
−5; 3; −11.
9; 8; 2.
caſus, quibus q
n duplus cuius-
nur quo p = 13
4, 3, −1, −3,
: formentur:
eſidua; ſecunda
, −4, 3, quae
xcluſis: quarta
petita. Similis
14 = 2. 7, quo
7, −7, 9, −9,
ae formantur:
1, -1| 1, -1
-6, 5, -9, -7
-6, -5, -9, 7
IV.

IV. 1, 5, -4, 9, -13, -7, -6, -1, -5, 4, -9, 13, 7, 6
V. 1, -5, -4, -9, -13, 7, -6,| 1, -5, -4, -9, -13, 7, -6
VI. 1, 6, 7, 13, -9, 4, -5, -1, -6, -7, -13, 9, -4, 5
VII. 1, -6, 7, -13, -9, -4, -5,| 1, -6, 7, -13, -9, -4, -5
VIII. 1, 7, -9, -5, -6, -13, -4,| 1, 7, -9, -5, -6, -13, -4
IX. 1, -7, -9, 5, -6, 13, -4, -1, 7, 9, -5, 6, -13, 4
X. 1, 9, -6, 4, 7, 5, -13, -1, -9, 6, -4, -7, -5, 13
XI. 1, -9, -6, -4, 7, -5, -13,| 1, -9, -6, -4, 7, -5, -13
XII. 1, 13, -5, -7, -4, 6, -9, -1, -13, 5, 7, 4, -6, 9
XIII. 1, -13, -5, 7, -4, -6, -9 | 1, -13, -5, 7, -4, -6, -9

§. 40. Antequam hinc quicquam concludimus, euoluamus etiam caſum, quo q eſt productum ex aliis binis numeris primis. Sit ergo diuiſor $p = 31$ et $q = 15 = 3 \cdot 5$, quo caſu reſidua ſunt:

1, 4, 9, −15, −6, 5, −13, 2, −12, 7, −3, −11, 14, 10, 8

vnde ſequentes progreſſiones geometricae formantur, vbi quidem cuique ſuam ſociatam retro diſpoſitam adiungo:

{ I. 1, 4, -15, 2, 8,| 1, 4, -15, 2, 8,| 1, 4, -15, 2, 8
{ II. 1, 8, 2, -15, 4,| 1, 8, 2, -15, 4,| 1, 8, 2, -15, 4
{ III. 1, 9, -12, -15, -11, -6, 8, 10, -3, 4, 5, 14, 2, -13, 7
{ IV. 1, 7, -13, 2, 14, 5, 4, -3, 10, 8, -6, -11, -15, -12, 9
{ V. 1, 2, 4, 8, -15,| 1, 2, 4, 8, -15,| 1, 2, 4, 8, -15
{ VI 1, -15, 8, 4, 2 | 1, -15, 8, 4, 2,| 1, -15, 8, 4, 2
{ VII. 1, -3, 9, 4, -12, 5, -15, 14, -11, 2, -6, -13, 8, 7, 10
{ VIII. 1, 10, 7, 8, -13, -6, 2, -11, 14, -15, 5, -12, 4, 9, -3
{ IX. 1, 5, -6 | 1, 5, -6,| 1, 5, -6,| 1, 5, -6,| 1, 5, -6
{ X. 1, -6, 5 | 1, -6, 5,| 1, -6, 5,| 1, -6, 5,| 1, -6, 5
{ XI. 1, -11, -3, 2, 9, -6, 4, -13, -12, 8, 5, 7, -15, 10, 14
{ XII. 1, 14, 10, -15, 7, 5, 8, -12, -13, 4, -6, 9, 2, -3, -11
{ XIII. 1, -12, -11, 8, -3, 5, 2, 7, 9, -15, -6, 10, 4, 14, -13
{ XIV. 1, -13, 14, 4, 10, -6, -15, 9, 7, 2, 5, -3, 8, -11, -12

§. 41. Has progressiones geometricas intuenti mox patet, earum alias esse completas, quarum termini omnia residua exhibeant; alias vero esse periodicas, quae scilicet duabus pluribusue periodis constent, in quibus eadem residua eodem ordine recurrant, quam distinctionem inter progressiones completas et periodicas probe notasse iuuabit. Periodicae scilicet locum inueniunt, quando, posito diuisore primo $p = 2q + 1$, numerus q in duos factores est resolubilis, vt sit $q = mn$; tum enim eiusmodi progressiones geometricae dabuntur, quae continent m periodos, quaelibet n residua complectente; ac tales quidem assignari poterunt tot, quot numerus $n - 1$ continet vnitates. Cum enim in eadem periodo cuiusque termini omnes potestates occurrant, euidens est quemque pro denominatore sumtum similem progressionem periodicam producere, nisi forte periodorum numerus adeo duplicetur, vel multiplicetur, hoc est in duas pluresue periodos subdiuidatur.

§. 42. Ex progressione autem completa, quaecunque ea sit, facile reliquae omnes, siue sint completae siue periodicae formantur. Sit enim diuisor primus $p = 2q + 1$, haecque progressio completa:

Indices	0.	1.	2.	3.	4.	5.	-	-	-	$q - 1$
Progr.	1.	α.	α^2.	α^3.	α^4.	α^5.	-	-	-	α^{q-1}

si hinc excerpantur per saltus aequales termini:

$$\begin{array}{cccccccccc} 0. & n. & 2n. & 3n. & 4n. & - & - & - & - & nq-n \\ 1. & \alpha^n. & \alpha^{2n}. & \alpha^{3n}. & \alpha^{4n}. & - & - & - & - & \alpha^{nq-n} \end{array}$$

haec progressio erit completa, si numerus n ad q fuerit primus; sin autem n et q habeant communem diuisorem, puta d, tum haec progressio totidem habebit periodos, in qua-

icas intuenti mox
n termini omnia
is, quae scilicet
ibus eadem resi-
tionem inter pro-
: notasse iuuabit,
o, posito diuisore
ctores est resolu-
rogressiones geo-
dos, quaelibet n
ignari poterunt
Cum enim in
potestates occur-
ore sumtum simi-
nisi forte perio-
iplicetur, hoc est
npleta, quaecun-
t completae siue
imus $p = 2q + 1$,
- - - $q - 1$
- - α^{q-1}
mini:
- $nq - n$
- α^{nq-n}
us n ad q fuerit
unem diuisorem,
ebit periodos, in
qua-

quarum singulis eadem residua numero $\frac{q}{d}$ recurrent, reliqua autem inde prorsus excludentur. Numerus autem harum periodorum maximo communi diuisore inter n et q definietur. At vero vicissim ex progressione periodica non licet progressionem completam formare.

§. 43. Imprimis autem hic notari meretur, in omnibus his progressionibus summam omnium terminorum semper esse nihilo aequalem, seu per diuisorem p diuisibilem, quod hoc modo demonstratur: Cum $\alpha^q - 1$ per p diuisionem admittat, haec autem forma in factores resoluatur $\alpha - 1$ et $1 + \alpha + \alpha^2 + \alpha^3 - - - - - + \alpha^{q-1}$, quorum ille $\alpha - 1$ certe non per p est diuisibilis, necesse est hunc alterum, hoc est summam totius nostrae progressionis per numerum p diuisionem admittere. Ac si progressio habeat periodos, termini cuiusque periodi iunctim sumti, seu summa omnium residuorum inde oriundorum per p erit diuisibilis, id quod in exemplis supra allatis per se est manifestum.

§. 44. Ex eodem autem fonte colligitur, si progressio geometrica fuerit completa, et q habeat factorem m, vt sit $q = mn$ et diuisor primus $p = 2mn + 1$, tum ob formam $\alpha^{mn} - 1$ diuisibilem per $\alpha^m - 1$, quae per p diuisibilis non existit, quia progressio alioquin completa non foret, quotum inde ortum:

$$1 + \alpha^m + \alpha^{2m} + \alpha^{3m} + \ldots\ldots + \alpha^{(n-1)m}$$

per diuisorem p fore diuisibilem. Quamobrem si tota progressio in membra distribuatur, hoc modo:

$$1, \alpha \ldots \alpha^{m-1} | \alpha^m + \alpha^{m+1} \ldots \alpha^{2m-1} | \alpha^{2m} + \alpha^{2m+1} \ldots \alpha^{3m-1} | \ldots | \alpha^{(n-1)m} \ldots \alpha^{mn-1}$$

 quo-

quorum membrorum numerus est n, haecque membra ita sibi subscribantur:

$$\begin{array}{lllll}
1, & a, & a^2 & \ldots\ldots & a^{m-1} \\
a^m, & a^{m+1}, & a^{m+2} & \ldots\ldots & a^{2m-1} \\
a^{2m}, & a^{2m+1}, & a^{2m+2} & \ldots\ldots & a^{3m-1} \\
\cdot & \cdot & \cdot & & \cdot \\
\cdot & \cdot & \cdot & & \cdot \\
\cdot & \cdot & \cdot & & \cdot \\
\cdot & \cdot & \cdot & & \cdot \\
a^{(n-1)m}, & a^{(n-1)m+1}, & a^{(n-1)m+2} & \ldots & a^{nm-1}
\end{array}$$

tum summae terminorum in qualibet columna verticali positorum ad nihilum reducentur, seu per diuisorem primum $p = 2mn + 1$ diuisibiles erunt. Tot autem diuersis modis progressio completa in huiusmodi membra distribui potest, quot numerus q habuerit diuisores.

§. 45. Prima autem columna verticalis simul dabit periodos pro omnibus progressionibus periodicis. De his numeris tenendum est, eos non solum esse residua quadratorum, sed etiam altiorum potestatum parium. Scilicet si diuisor primus sit huius formae: $p = 2mn + 1$, quemadmodum inter numeros ipso minores, quorum multitudo est $= 2mn$, tantum semissis mn in residuis quadratorum occurrit, totidemque inde excluduntur, ita potestates exponentis $2m$ per eundem numerum p diuidendo, tantum n diuersa residua inde resultant, et reliqui omnes, quorum multitudo est $(2m - 1)n$, ita sunt comparati, vt in forma $a^{2m} - ip$ nullo modo contineantur; seu nulla exhiberi possit potestas exponentis $2m$, quae vllo istorum numerorum minuta per numerum primum $p = 2mn + 1$ fiat diuisibilis.

§. 46.

:que membra ita
expone . a^{m-1}
ciare li . a^{2m-1}
scilicet . a^{3m-1}
ac pot
per eu
numerc
reliqui
$(m-1$. a^{nm-1}
numer mna verticali po-
numer uisorem primum
m diuersis modis
distribui potest,
hinc n
ant, e rticalis simul da-
visum periodicis. De
tum n esse residua qua-
praesen parium. Scilicet
1. I $mn + 1$, quem-
1 iorum multitudo
uis quadratorum
ta potestates ex-
3. I iidendo, tantum
F omnes, quorum
rati, vt in forma
lla exhiberi possit
rum numerorum
1 fiat diuisibilis.
§. 46.

§. 46. Neque vero haec proprietas ad potestates exponentium parium est adstricta; sed in genere pronunciare licet, si diuisor primus sit formae $p = mn + 1$, qui scilicet vnitate minutus in factores m et n resolui possit, ac potestates exponentis m, nempe:

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m,\ \ldots\ (p-1)^m$$

per eum diuidantur, tum inter residua tantum n diuersos numeros occurrere, quorum singuli m vicibus repetantur, reliqui autem numeri omnes, quorum multitudo est $(m-1)n$, hinc excludantur: ex quo insignes proprietates numerorum, qui sunt potestates, ratione diuisibilitatis per numeros primos, agnoscere licet.

§. 47. Quoniam igitur nullum est dubium, quin hinc multae praeclarae numerorum proprietates erui queant, exempla plurium numerorum primorum hic adiicere visum est, pro iisque residua, quae ex diuisione potestatum nascuntur exhibere, vbi quidem sociata iunctim repraesentantur:

1. Diuisor $p = 3 = 2 + 1$

Potest.	Resid.
a^2)	1

2. Diuisor $p = 5 = 2.2 + 1$

Potest.	Resid.
a^2)	1, − 1
a^4)	1

3. Diuisor $p = 7 = 2.3 + 1$

Potest.	Residua
a^2	1, 2, − 3
a^3)	1, − 1
a^6)	1

4. Diuisor $p = 11 = 2.5 + 1$

Potest.	Resid.
a^2	1, 4, 5, − 3 − 2
a^5)	1, − 1
a^{10})	1

5. Di-

5. Diuifor $p = 13 = 2.2.3 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 4, & 3, & -1 \\ & -3 & -4 & \end{matrix} \right)$

$a^3 \left\{ \begin{matrix} 1, & -5, & -1 \\ & 5 & \end{matrix} \right)$

$a^4 \left\{ \begin{matrix} 1, & 3 \\ & -4 \end{matrix} \right)$

$a^6)\ 1, -1$

$a^{12})\ 1$

6. Diuifor $p = 17 = 2^4 + 1$

Poteft Refidua

$a^2 \left\{ \begin{matrix} 1, & 2, & 4, & 8, & -1 \\ & -8 & -4 & -2 & \end{matrix} \right]$

$a^4 \left\{ \begin{matrix} 1, & 4, & -1 \\ & -4 & \end{matrix} \right]$

$a^8)\ 1, -1$

$a^{16})\ 1$

7. Diuif. $p = 19 = 2.3.3 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 4, & -3, & 7, & 9 \\ & 5, & 6, & -8, & -2 \end{matrix} \right)$

$a^3 \left\{ \begin{matrix} 1, & 8, & 7, & -1 \\ & -7 & -8 & \end{matrix} \right)$

$a^6 \left\{ \begin{matrix} 1, & 7 \\ & -7 \end{matrix} \right)$

$a^9)\ 1, -1$

8. Diuif. $p = 23 = 2.11 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 4, & -7, & -5, & 3, & -11 \\ & 6, & -10, & 9, & 8, & 2 \end{matrix} \right]$

$a^{11})\ 1, -1$

9. Diuifor $p = 29 = 2.2.7 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 4, & -13, & 6, & -5, & 9, & 7, & -1 \\ & -7 & -9, & 5, & -6, & 13, & -4 & \end{matrix} \right)$

$a^4 \left\{ \begin{matrix} 1, & -13, & -5, & 7 \\ & -9 & -6 & -4 \end{matrix} \right)$

$a^7 \left\{ \begin{matrix} 1, & 12, & -1 \\ & -12 & \end{matrix} \right)$

$a^{14})\ 1, -1$

10.

10. P 17=2^4+1 dua 4, 8,-1 4 -2 1 :2. 11+1 11. P 5,3,-11 9,8, 2 12. P 10.

10. Diuifor $p = 31 = 2.3.5 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 9, & -12, & -15, & -11, & -6, & 8, & 10 \\ & 7, & -13, & 2, & 14, & 5, & 4, & -3 \end{matrix} \right)$

$a^3 \left\{ \begin{matrix} 1, & -4, & -15, & -2, & 8, & -1 \\ & -8, & 2, & -15, & 4 & \end{matrix} \right)$

$a^5 \left\{ \begin{matrix} 1, & -5, & -6, & -1 \\ & 6, & 5 & \end{matrix} \right)$

$a^6 \left\{ \begin{matrix} 1, & 2, & 4 \\ & -15, & 8 \end{matrix} \right)$

$a^{10} \left\{ \begin{matrix} 1, & 5 \\ & -5 \end{matrix} \right)$

$a^{15})\ 1, -1$

11. Diuifor $p = 37 = 2.2.3.3 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & 4, & 16, & -10, & -3, & -12, & -11, & -7, & 9, & -1 \\ & -9, & 7, & 11, & 12, & 3, & 10, & -16, & -4 & \end{matrix} \right)$

$a^3 \left\{ \begin{matrix} 1, & 8, & -10, & -6, & -11, & -14, & -1 \\ & 14, & 11, & 6, & 10, & -8 & \end{matrix} \right)$

$a^4 \left\{ \begin{matrix} 1, & 16, & -3, & -11, & 9 \\ & 7, & 12, & 10, & -4 \end{matrix} \right)$

$a^6 \left\{ \begin{matrix} 1, & -10, & -11, & -1 \\ & 11, & 10 & \end{matrix} \right)$

$a^9 \left\{ \begin{matrix} 1, & -6, & -1 \\ & 6 & \end{matrix} \right)$

$a^{12} \left\{ \begin{matrix} 1, & -11 \\ & 10 \end{matrix} \right)$

$a^{18} (1, -1)$

12. Diuifor $p = 41 = 2^3.5 + 1$

Poteft. Refidua

$a^2 \left\{ \begin{matrix} 1, & -2, & 4, & -8, & 16, & 9, & -18, & -5, & 10, & -20, & -1 \\ & 20, & -10, & 5, & 18, & -9, & -16, & 8, & -4, & 2 & \end{matrix} \right)$

$$a^{4}\left\{1,\ \begin{matrix}4, 16, -18, 10,\\ -10, 18, -16, -4\end{matrix}\ -1\right)$$
$$a^{5}\left\{1,\ \begin{matrix}-3, 9, 14,\\ -14, -9\ 3,\end{matrix}\ -1\right)$$
$$a^{8}\left\{1,\ \begin{matrix}16, 10\\ 18, -4\end{matrix}\right)$$
$$a^{10}\left\{1,\ \begin{matrix}9,\\ -9,\end{matrix}\ -1\right)$$
$a^{20}\big)\ 1, -1$

---

13. Diuisor $p = 43 = 2.3.7 + 1$

Poteſt. Reſidua

$$a^{2}\left\{1,\ \begin{matrix}9, -5, -2, -18, 10, 4, -7, -20, -8, 14\\ -19, 17, 21, -12, 13, 11, 6, 15, 16, -3\end{matrix}\right)$$
$$a^{3}\left\{1,\ \begin{matrix}8, 21, -4, 11, 2, 16,\\ -16, -2, -11, 4, -21, -8,\end{matrix}\ -1\right)$$
$$a^{6}\left\{1,\ \begin{matrix}21, 11, 16\\ -2, 4, -8\end{matrix}\right)$$
$$a^{7}\left\{1,\ \begin{matrix}-6, -7,\\ 7, 6,\end{matrix}\ -1\right)$$
$$a^{14}\left\{1,\ \begin{matrix}-7\\ 6\end{matrix}\right)$$
$a^{21}\big)\ 1, -1$

---

14. Diuisor $p = 47 = 2.23 + 1$

Poteſt. Reſidua

$$a^{2}\left\{1,\ \begin{matrix}4, 16, 17, 21, -10, 7, -19, 18, -22, 6, -23\\ 12, 3, -11, 9, 14, -20, -5, -13, -15, 8, 2\end{matrix}\right)$$
$a^{23}\big)\ 1, -1$

---

15. Diuisor $p = 53 = 2.2.13 + 1$

Poteſt. Reſidua

$$a^{2}\left\{1,\ \begin{matrix}4, 16, 11, -9, 17, 15, 7, -25, 6, 24, -10, 13\\ -13, 10, -24, -6, 25, -7, -15, -17, 9, -11, -16, -4\end{matrix}\ -1\right)$$

-7, -20, -8, 14)
6, 15, 16, -3)
16, -1)
-8,
9, 18, -22, 6, -23)
5, -13, -15, 8, 2)
24 -10, 13 -1)
-11, -16, -4
a^4

$$a^{4}\left\{1,\ \begin{matrix}16, -9, 15, -25, 24, 13\\ 10, -6, -7, -17, -11, -4\end{matrix}\right)$$
$$a^{13}\left\{1,\ \begin{matrix}-23,\\ 23\end{matrix}\ -1\right)$$
$a^{26}\big)\ 1, -1$

---

16. Diuisor $p = 59 = 2.29 + 1$

Poteſt. Reſidua

$$a^{2}\left\{1,\ \begin{matrix}4, 16, 5, 20, 21, 25, -18, -13, 7, 28, -6, -24, 22, -29\\ 15, -11, 12, 3, -14, 26, -23, 9, 17, 19, -10, 27, -8, -2\end{matrix}\right)$$
$a^{29}\big)\ 1, -1$

---

17. Diuisor $p = 61 = 2.2.3.5 + 1$

Poteſt. Reſidua

$$a^{2}\left\{1,\ \begin{matrix}4, 16, 3, 12, -13, 9, -25, 22, 27, -14, 5, 20, 19, 15\\ -15, -19, 20, -5, 14, -27, -22, 25, -9, 13, -12, -3, -16, -4\end{matrix}\ -1\right.$$
$$a^{3}\left\{1,\ \begin{matrix}8, 3, 24, 9, 11, 27, -28, 20, -23,\\ 23, -20, 28, -27, -11, -9, -24, -3, -8,\end{matrix}\ -1\right.$$
$$a^{4}\left\{1,\ \begin{matrix}16, 12, 9, 22, -14, 20, 15\\ -19, -5, -27, 25, 13, -3, -4\end{matrix}\right)$$
$$a^{5}\left\{1,\ \begin{matrix}-29, -13, 11, -14, -21,\\ 21, 14, -11, 13, 29,\end{matrix}\ -1\right)$$
$$a^{6}\left\{1,\ \begin{matrix}3, 9, 27, 20\\ -20, -27, -9, -3\end{matrix}\ -1\right)$$
$$a^{10}\left\{1,\ \begin{matrix}-13, -14,\\ 14, 13,\end{matrix}\ -1\right)$$
$$a^{12}\left\{1,\ \begin{matrix}-3, 9\\ 20, -27\end{matrix}\right)$$
$$a^{15}\left\{1,\ \begin{matrix}11,\\ -11,\end{matrix}\ -1\right)$$
$$a^{20}\left\{1,\ \begin{matrix}-14\\ 13\end{matrix}\right)$$
$a^{30}\big(\ 1, -1$

Conclusio.
de poteſtatibus cuiusque ordinis et reſiduis in earum diuiſione per numeros primos relictis.

§. 48. Quemadmodum in his exemplis reſidua pro ſingulis poteſtatibus per progreſſiones geometricas ſunt exhibita, quae ſimul retro continuatae bina reſidua ſociata iunctim repraeſentant; ita idem pro poteſtatibus primi ordinis fieri poteſt, ubi quidem omnes plane numeri diuiſore minores occurrere debent, ita vt ſi diuiſor primus ſit $p = 2q + 1$, multitudo reſiduorum diuerſorum ſit $= 2q$, quae ad minimam formam reducta erunt ± 1, ± 2, ± 3, ± 4, etc. vsque ad $\pm q$. Haec vero reſidua omnia quoque ſecundum progreſſionem geometricam diſponi poſſunt ab vnitate incipientem, dummodo pro eius denominatore ſeu ſecundo termino eiusmodi numerus accipiatur, qui omnes plane numeros producat, quod euenit ſi is ita fuerit comparatus, vt nulla eius poteſtas, cuius exponens minor ſit quam $2q$, pro reſiduo vnitatem relinquat. Tales autem numeros pro quouis diuiſore dari certum eſt; etiamſi eos aſſignare maxime difficile videatur, eorumque indoles ad profundiſſima numerorum myſteria ſit referenda.

§. 49. Sit igitur in genere pro diuiſore primo $p = 2q + 1$, littera a eiusmodi numeros, cuius poteſtates per p diuiſae omnes numeros ipſo p minores pro reſiduis relinquat; neque in ſerie geometrica $1, a, a^2, a^3, a^4$, etc. vnitas ante recurrat, quam ad poteſtatem a^{2q} fuerit peruentum, quippe quae ſemper per $p = 2q + 1$ diui-

inis
numeros
emplis reſidua
ometricas ſunt
reſidua ſocia-
eſtatibus primi
e numeri diui-
diuiſor primus
orum ſit $= 2q$,
1, ± 2, ± 3,
ua omnia quo-
diſponi poſſunt
denominatore
ccipiatur, qui
it ſi is ita fue-
uius exponens
elinquat. Ta-
i certum eſt;
tur, eorumque
teria ſit refe-
diuiſore primo
cuius poteſta-
inores pro re-
$1, a, a^2, a^3$,
poteſtatem a^{2q}
$p = 2q + 1$
diui-

ſa vnitatem relinquit, ſicque omnes poteſtates hac minores diuerſa reſidua producant. Cum igitur poteſtas a^q non relinquat vnitatem, et $a^{2q} - 1 = (a^q + 1)(a^q - 1)$ per numerum p diuiſionem admittat, erit $a^q + 1$ per p diuiſibilis, et poteſtas a^q reſiduum dabit $- 1$; tum vero ſequentes poteſtates a^{q+1}, a^{q+2}, a^{q+3}, etc. dabunt reſidua $-a$, $-a^2$, $-a^3$, etc. quae ita ſunt comparata, vt cum antecedentibus a^{q-1}, a^{q-2}, a^{q-3}, etc. ordine iuncta bina reſidua ſociata exhibeant, quorum ſcilicet productum a^{2q} vnitati aequiualeat. Sequenti ergo modo haec reſidua per aſſociationem repraeſentare poterimus:

indices	0,	1,	2,	3,	4,		$q-3$,	$q-2$,	$q-1$,	q
	1,	a^1,	a^2,	a^3,	a^4,	- - -	a^{q-3},	a^{q-2},	a^{q-1},	
		$-a^{q-1}$,	$-a^{q-2}$,	$-a^{q-3}$,	$-a^{q-4}$		$-a^3$,	$-a^2$,	$-a$	-1
Indices	$2q$,	$2q-1$,	$2q-2$,	$2q-3$,	$2q-4$,		$q+3$,	$q+2$,	$q+1$,	q

vbi bina reſidua ſibi ſubſcripta ſunt inter ſe ſociata, extrema vero $+ 1$ et $- 1$ ſolitaria, quippe quae ſecum ipſa ſociantur.

§. 50. Tali progreſſione geometrica conſtituta, quae omnia reſidua ex poteſtatibus primi ordinis oriunda, hoc eſt omnes plane numeros complectitur, ex ea omnia reſidua pro poteſtatibus cuiusuis ordinis innoteſcent, eodem ſcilicet diuiſore primo $p = 2q + 1$ retento. Reſidua nimirum ex diuiſione quadratorum orta erunt:

$$1, a^2, a^4, a^6, a^8, \text{ etc. } - - - - a^{2q-2},$$

quae indicibus tantum paribus reſpondent, et ita per aſſociationem exhibentur:

 1,

$$1, \frac{a^2}{-a^{q-2}}; \frac{a^4}{-a^{q-4}}; \frac{a^6}{-a^{q-6}}; \frac{a^8}{-a^{q-8}}; \text{ etc.}$$

in quibus ergo -1 reperietur, ſi q fuerit numerus par. Pro cubis autem eos tantum terminos accipi oportet, quorum indices ſunt multipla ternarii $1, a^3, a^6, a^9$, etc. Vnde patet, ſi exponens $2q$ diuiſionem per 3 admittat. multitudinem reſiduorum ad trientem redigi, dum reliquis caſibus omnia plane reſidua occurrunt. Simili modo reſidua poteſtatum quartarum obtinentur ex indicibus per 4 diuiſibilibus, ſeu ex his poteſtatibus: $1, a^4, a^8, a^{12}$, etc. et reſidua poteſtatum quintarum ex his: $1, a^5, a^{10}, a^{15}$, etc.

§. 51. Tantum ergo opus eſt, vt pro quolibet diuiſore primo $p = 2q + 1$ idonei numeri pro a habeantur, ex cuius poteſtatibus omnia plane reſidua reſultent; ad quod autem nullam certam regulam mihi eſſe cognitam fateri cogor. Hoc ſaltem obſeruaſſe iuuabit, ſi vnus huiusmodi numerus a fuerit cognitus, eius ſocium, qui ſit b, vt $ab - 1$ per p fiat diuiſibile, quoque pari proprietate eſſe praeditum: vidimus autem hunc ſocium b vel per a^{2q-1} vel per $-a^{q-1}$ exhiberi poſſe. Ex quo concludere licet, tum etiam pro a quamuis eius poteſtatem a^n, cuius exponens n ſit ad numerum $2q$ primus, accipi poſſe, vbi quidem ſufficit pro n numeros ipſo $2q$ minores aſſumſiſſe, cum ex altioribus poteſtatibus eadem reſidua repetantur. Quoniam vero certa lex adhuc latet, pro diuiſoribus ſimplicioribus idoneos numeros pro a aſſumendos, ex cuius ſcilicet poteſtatibus omnia plane reſidua naſcantur, exhibebo:

Diuiſ.

numerus par. oportet, quo- etc. Vnde ttat. multi- reliquis ca- i modo reſi- icibus per 4 , a^{12}, etc. et a^{15}, etc.

pro quolibet pro a habe- ſidua reſul- n mihi eſſe iuuabit, ſi ius ſocium, quoque pari nc ſocium b . Ex quo eius poteſta- $2q$ primus, ros ipſo $2q$ tibus eadem adhuc latet, os pro a aſ- a plane reſi-

Diuiſ.

Diuiſ. primi.	Numeri pro a aſſumendi
$p = 3,\ q = 1$	-1
$p = 5,\ q = 2$	$+2, -2$
$p = 7,\ q = 3$	$-2, +3$
$p = 11,\ q = 5$	$+2, -3, -4, -5$
$p = 13,\ q = 6$	$+2, -2, +6, -6$
$p = 17,\ q = 8$	$+3, -3, +5, -5, +6, -6, +7, -7$
$p = 19,\ q = 9$	$+2, +3, -4, -5, -6, -9$
$p = 23,\ q = 11$	$-2, -3, -4, +5, -6, +7, -8, -9, +10, +11$
$p = 29,\ q = 14$	$+2, -2, +3, -3, +8, -8, +10, -10, +11, -11, +14, -14$
$p = 31,\ q = 15$	$+3, -7, -9, -10, +11, +12, +13, -14$
$p = 37,\ q = 18$	$+2, -2, +5, -5, +13, -13, +15, -15, +17, -17, +18, -18$
$p = 41,\ q = 20$	$\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$

§. 52. In caſu poſtremo $p = 41$ ergo patet, pro a minorem numerum quam 6 aſſumi non poſſe, cum in praecedentibus progreſſio geometrica ex minoribus numeris formari queat: vnde pro hoc diuiſore $p = 41$ iſta progreſſio geometrica ita ſe habebit:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1,	$+6,$	$-5,$	$+11,$	$-16,$	$-14,$	$-2,$	$-12,$	$+10,$	$+19,$	$-9,$	$-13,$	$+4,$	$-17,$	$-20,$
	$+7,$	$+8,$	$+15,$	$-18,$	$-3,$	$+20,$	$+17,$	$-4,$	$+13,$	$+9,$	$-19,$	$-10,$	$+12,$	$+2,$

15	16	17	18	19	20
$+3,$	$+18,$	$-15,$	$-8,$	-7	-1
$+14,$	$+16,$	$-11,$	$+5,$	$-6,$	

Hinc ſi ii numeri excerpantur, qui indicibus paribus reſpondent, habebuntur reſidua ex quadratis orta: ſin autem ii excerpantur, qui indicibus vel per 4, vel 5, vel 8, vel 10, vel 20 conueniunt, reſidua pro eiusdem no-

 minis

minis potestatibus obtinebuntur, eaque ipsa, quae iam supra sunt recensita. Similisque est ratio omnium reliquorum numerorum primorum.

§. 53. Quod autem ad multitudinem horum numerorum a attinet, obseruo eam quouis casu $p = 2q + 1$ aequalem esse multitudini eorum numerorum ipso p minorum, qui sint ad $2q$ primi: atque alio loco ostendi, ad hanc multitudinem inueniendam numerum $2q$ in factores suos primos resolui debere, ita vt si fuerit $2q = f^{\zeta} g^{\eta} h^{\theta} k^{\kappa}$, sit ista multitudo

$$= (f-1) f^{\zeta-1} \cdot (g-1) g^{\eta-1} \cdot (h-1) h^{\theta-1} \cdot (k-1) k^{\kappa-1}.$$

Definito autem pro quouis numero $p = 2q + 1$ hac multitudine, sint ipsi numeri ad $2q$ primi $1, \alpha, \beta, \gamma, \delta$, etc. atque si datus fuerit vnus numerus a quicunque, reliqui ideoque omnes erunt:

$$a,\ a^{\alpha} - np;\ a^{\beta} - np;\ a^{\gamma} - np;\ a^{\delta} - np;\ \text{etc.}$$

sumendo n ita, vt omnes isti numeri infra p deprimantur. Haec fortasse consideratio viam aperiet pro quouis casu hos numeros inuestigandi.

DE

iam su-
reliquo-
ME
rum nu-
$= 2q + 1$
so p mi-
ostendi,
r in fac-
it $2q =$
In n
va
dati
quoq
eoden
quae
ergo
curua
vani,
curua
sempe
aeque
cum
curua
maxir
stanti
innuit
primis
interp
nerali
$- 1) k^{\kappa-1}$.
hac mul-
γ, δ, etc.
, reliqui
etc.
depriman-
ro quouis
DE

DE EXIMIO VSV
METHODI INTERPOLATIONVM
IN SERIERVM DOCTRINA.

In methodo interpolationum eiusmodi relatio inter binas variabiles x et y quaeritur, vt si alteri x successiue dati valores a, b, c, d, etc. tribuantur, altera y inde quoque datos valores p, q, r, s, etc. sortiatur; seu quod eodem redit, aequatio pro eiusmodi linea curua quaeritur, quae per quotcunque puncta data transeat. Quo maior ergo fuerit horum punctorum numerus, eo magis linea curua limitatur: interim tamen iam alia occasione obseruaui, etiamsi punctorum numerus in infinitum augeatur, curuam per ea transeuntem non prorsus determinari, sed semper infinitas adhuc lineas curuas exhiberi posse, quae aeque per cuncta eadem puncta sint transiturae. Quare cum methodus interpolationum pro quouis casu lineam curuam suppeditet determinatam, solutio haec semper pro maxime particulari erit habenda: verum haec ipsa circumstantia singularem quandam indolem solutionis inuentae innuit, quae accuratiorem considerationem meretur. Imprimis autem ista solutionis indoles pendet a ratione, qua interpolatio instituitur, seu a forma, quae aequationi generali tribuitur, in qua aequationem quaesitam contineri

opor-