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-

DISQVISITIO ACCVRATIOR CIRCA RESIDVA

EX DIVISIONE QVADRATORVM ALIORVMQVE 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 $\alpha \pm p$

DIS-

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

§. 4. Innumera autem quadrata aa, per numerum p diuisa, idem relinquunt residuum α, quae omnia ex cognito vno aa facile inueniuntur. Cuncta haec quadrata ista forma $(a \pm mp)^2$ vel $(mp \pm a)^2$ contineri euidens est; sicque sufficit residuum ex harum forma minima, cuius radix non excedet $\frac{1}{2}p$, notasse: omnia scilicet haec quadrata $(mp \pm a)^2$ 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: $1, 4, 9, 16, \ldots 16, 9, 4, 1.$

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. $1, 2^2, 3^2, 4^2, \ldots (\frac{p-1}{2})^2$

Resid. $1, 4, 9, 16, \ldots \frac{pp-2p+1}{4}$

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.

§. 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 aa et bb, neutro quadratum $(\frac{p-1}{2})^2$ excedente, idem darent residuum r, differentia eorum $aa-bb$, 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 $np+\alpha$ 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 $np+\mathfrak{A}$ contineri. Quouis autem casu tam residuorum α quam non-residuorum $\mathfrak{A}$ multitudo est $= \frac{p-1}{2}$.

§. 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 $(\frac{p-1}{2})^2$ 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 $(\frac{p-3}{2})^2$ 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 $q+13$.

§. 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 $p = 4q+1$:

$p = 5$ { $1; 2^2$
$q = 1$ { $1, 4$
ſeu $1; -1$

$p = 13$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2$
$q = 3$ { $1; 4, 9, 3, 12, 10$
ſeu $1; 4, -4, 3, -1, -3$

$p = 17$ { $1; 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2$
$q = 4$ { $1; 4, 9, 16, 8, 2, 15, 13$
ſeu $1, 4, -8, -1, 8, 2, -2, -4$.

$p = 29$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2$
$q = 7$ { $1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22$
ſeu $1, 4, 9, -13, -4, 7, -9, 6, -6, 13, 5, -1, -5, -7$

$p =$

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

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

vbi obseruare licet, in residuis per negatiua ad minimam formam reductis, singulos numeros bis, positiue scilicet et negatiue occurrere.

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

$p=3\left\{\begin{array}{l}1\\ q=0\left\{1\right.\end{array}\right.$ | $p=7\left\{\begin{array}{l}1,\ 2^2,\ 3^2\\ q=1\left\{\begin{array}{l}1,\ 4,\ 2\\ \text{seu } 1,-3,\ 2\end{array}\right.\end{array}\right.$

$p=11\left\{\begin{array}{l}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2\\ q=2\left\{\begin{array}{l}1,4,\ 9,\ 5,\ 3\\ \text{seu } 1,4,-2,\ 5,\ 3\end{array}\right.\end{array}\right.$

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

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

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

$p=$

$p=43\left\{\begin{array}{l}\\ q=10\left\{\right.\end{array}\right.$ seu

$^2,14^2,15^2,16^2\ 17^2,18^2$
$1,\ 11,\ 3,\ 34,\ 30,\ 28$
$6,\ 11,\ 3,-3,-7,-9$

$^2,16^2,17^2,18^2,19^2,20^2$
$,10,\ 2,\ 37,\ 33,\ 31$
$,10,\ 2,-4,-8,-10$

ad minimam
iue scilicet et

ad numeros

$,11^2$
6
6

$^2,13^2,14^2,15^2$
$,14,\ 10,\ 8$
$1,14,\ 10,\ 8$

$p=$

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

In istis residuis ad minimam formam reductis omnes plane numeri ab vnitate vsque ad $2q+1$ occurrunt, alii signo positionis, alii negationis affecti. Verum has proprietates obseruatas demonstrari oportet.

§. 16. Iam supra, p. 69. demonstraui, si inter residua, ex diuisione 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 residua ex quadratis aa et bb, ita vt sit $aa = mp+\alpha$ et $bb = np+\beta$, atque manifestum est ex horum quadratorum producto

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

cuius forma est $Mp+\alpha\beta$, nasci residuum $\alpha\beta$; similique modo ex quadrato $a^{2m}b^{2n}$ prouenire residuum $\alpha^m\beta^n$, seu $\alpha^m\beta^n - Mp$, vt ad minimam formam reducatur. Quin etiam notari conuenit, hoc ipsum residuum $\alpha^m\beta^n$ nasci ex omnibus his quadratis: $(a^mb^n \pm N^{\frac{1}{2}}p)^2$ seu $(Np \pm a^mb^n)^2$, ideoque ex quadrato, cuius latus $a^mb^n - N^{\frac{1}{2}}p$ seu $N^{\frac{1}{2}}p - a^mb^n$ minus erit quam $\frac{1}{2}p$.

§. 17. Denotent litterae $a, b, c, d, \ldots\ldots l$ omnes numeros diuisoris p semisse $\frac{1}{2}p$ minores, quorum ergo multitudo est $= \frac{p-1}{2}$, sintque $\alpha, \beta, \gamma, \delta \ldots\ldots \lambda$ residua ex eorum quadratorum $a^2, b^2, c^2, d^2 \ldots\ldots l^2$ per numerum p diuisione relicta, quorum multitudo itidem est $= \frac{p-1}{2}$, ita vt ex omnibus numeris diuisore p mi-

minoribus, quorum multitudo est $p-1$, totidem ex reſiduorum ordine excludantur, quos nomine non-reſiduorum complexos litteris $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ... $\mathfrak{L}$ indicabo. Notatu ergo maxime dignum eſt, in ordine reſiduorum α, β, γ, δ, ... λ, 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; $px+\alpha$; $px+\beta$; $px+\gamma$; . . . . . $px+p-1$

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:

$px+\alpha$, $px+\beta$, $px+\gamma$, $px+\delta$, ... $px+\lambda$

$px+\mathfrak{A}$, $px+\mathfrak{B}$, $px+\mathfrak{C}$, $px+\mathfrak{D}$, ... $px+\mathfrak{L}$

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

§. 19.

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

, animaduerti
s numeros in
iſoris 2 duae
rium formulis
n 3 tres prae-
$x+2$, et di-
et $4x+3$,
a ſollicite di-
iuiſoris cuius-
ituuntur:

$\ldots px+p-1$
ia ſpecie px
ultitudo 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 α, β, γ, δ, ... λ determinatur, dum altera claſſis non-reſiduorum numeris $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ... $\mathfrak{L}$ 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 $bb-rs$ ſint 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 $mm\,aa-aas$ 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 aequivalens cenſetur huic formae generali, $\alpha + np$, vniuerſam ſpeciem continente, numerum n vtique ita accipere licet, vt $\frac{\alpha+n\beta}{\beta}$ 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,

vel omnia reſidua contineant ex quadratis orta, quorum multitudo eſt $= \frac{p-1}{2}$, vel indo excluſorum numerus ſit $= n$, 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 diuiſibilis reddatur, vel ipſi numero $\frac{p-1}{2}$, vel eiusdem partium aliquotae eſſe aequalem.

§. 25. Siue autem ſit $n = \frac{p-1}{2}$, 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 ſit $\frac{p-1}{2} = q$; ac ſi ex binis quadratorum reſiduis quibuscunque α et β, ſumendo $r = \frac{\beta+\alpha\gamma}{\alpha}$, formentur 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:

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

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 ſit $n < q-1$, 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 eiusmodi pars aliquota ipſius q, qualem eius indoles admittit. Quod ſi vtu 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 euolvere. 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

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

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:

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

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 $= 1, \alpha$, 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, 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 exit 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.

$p = 5$

$+1$	1^2	$+1$
-1	2^2	-1
		2^2

$p = 13$

$+1; +4; +3$	1^2	$+1; +4; +3$
$1; -4; -3$	2^2	$1; -4; -3$
		$5^2\ 3^2\ 6^2$

$p = 17$

$+1; +2; +4; +8$	1^2	$+1; +2; +4; +8$
$1; -2; 4; -8$	2^2	$1; -2; 4; -8$
		$4^2\ 7^2\ 8^2\ 2^2$

$p = 29$

$+1; +4; +5; +6; +7; +9; +13$	$1^2\ 2^2\ 11^2\ 8^2\ 6^2\ 3^2\ 10^2$	$+1; +4; +5; +6; +7; +9; +13$
$-1; -4; -5; -6; -7; -9; -13$		$-1; -4; -5; -6; -7; -9; -13$
		$12^2\ 5^2\ 13^2\ 9^2\ 14^2\ 7^2\ 4^2$

$p = 37$

$+1; +3; +4; +7; +9; +10; +11; +12; +16$	$1^2\ 25^2\ 2^2\ 9^2\ 3^2\ 22^2\ 14^2\ 7^2\ 4^2$	$+1; +3; +4; +7; +9; +10; +11; +12; +16$
$-1; -3; -4; -7; -9; -10; -11; -12; -16$		$-1; -3; -4; -7; -9; -10; -11; -12; -16$
		$6^2\ 16^2\ 12^2\ 17^2\ 18^2\ 8^2\ 10^2\ 5^2\ 13^2$

$p =$

$p = 41$

$+1; +2; +4; +5; +8; +9; +10; +16; +18; +20$	$1^2\ 17^2\ 2^2\ 33^2\ 7^2\ 3^2\ 18^2\ 4^2\ 10^2\ 15^2$	$+1; +2; +4; +5; +8; +9; +10; +16; +18; +20$
$-1; -2; -4; -5; -8; -9; -10; -16; -18; -20$		$-1; -2; -4; -5; -8; -9; -10; -16; -18; -20$
		$9^2\ 11^2\ 18^2\ 6^2\ 19^2\ 14^2\ 20^2\ 5^2\ 8^2\ 12^2$

§. 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 $a = nc$ et $b = nd$, 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 $29^2 + 11^2$ per eum diuisibilis, vt sit $a = 17$ et $b = 11$, atque per has regulas sequentes valores alii pro a et b reperientur:

$p = 41$;	$a = 17$	24	4	1	40	5
	$b = 11$	30	5	36	9	32	4

Tum

Tum vero porro ex casu quo alterutrum numerorum est $= x$, alteri valor quicunque tribui, alterque ita definiri potest, vt infra $\frac{1}{2}p$ subsistat. Scilicet inuento casu $a = x$ et $b = y$, satisfacit quoque $a = m$ et $b = ym$, vbi loco b sumi potest $ym - np$, seu $np - ym$, 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 $p = 2q + \varepsilon$, 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:

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

etc.

in quibus omnibus terminі sequentes $\alpha^q, \beta^q, \gamma^q, \delta^q \text{ - - - } \lambda^q$ vnitati aequiualebunt, quippe qui omnes vnitate minuti per diuisorem p erunt diuisibiles. Huiusmodi ergo progressi-

gressiones geometricas tot exhibere licet, quot unitates in q continentur; in iisque omnibus nullus terminus occurret, qui non inter residua $1, \alpha, \beta, \gamma$ - - - - - 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 obserno, si 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 unitate 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

plores terminos, e termino 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,	-5,	-11,	8,	-10	1
3.	Indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8	0
	Progr.	1,	-5,	2,	-10,	4,	3,	6,	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,	1,	7,	2,	8,	3,	9,	4,	10,	5	0
	Progr.	1,	2,	4,	8,	-7,	9,	-10,	3,	-5,	-11,	6	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,	3,	-7,	2	1

10. { Indices 0, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 | 0
{ Progr. 1, 6, -10, 9, 8, 2, -11, 3, -5, -7, 4 | 1

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 aequivalere. 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 $q = 6 = 2.3$, 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 $q = 14 = 2.7$, 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

IV.

3, 2, 1 | 0
-5, -7, 4 | 1

hendo 11 sunt
a residua, quo-
q, esse inter se
quivalere. 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
exclusis: 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 $q = 15 = 3.5$, 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

§. 51.

§. 44. Has progressiones geometricas intuenti mox patet, earum alias esse completas, quarum termini omnia residua exibeant, alias vero esse periodicas, quae scilicet duabus pluribusve 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, qualibet 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:

0. n. $2n$. $3n$. $4n$. - - - - $nq - n$

1. α^n. α^{2n}. α^{3n}. α^{4n}. - - - - α^{nq-n}

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-

qua
qua
rum
defi
non

omn
sem
lem
visi
tur
ille
alte
num
peri
ma
bilis
festu

gres
vt
forn
visi
fore

per
gres
1, α.
E

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-
odos, qualibet n
lignari 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 divisionem admittat, haec autem forma in factores resoluatur $\alpha - 1$ et $1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-1}$, 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 divisibilis non existit, quia progressio alioquin completa non foret, quotum inde ortum:

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

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

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

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

1,	a,	a^2		a^{m-1}
a^m,	a^{m+1},	a^{m+2}		a^{2m-1}
a^{2m},	a^{2m+1},	a^{2m+2} . . .		a^{3m-1}
.	.	.		.
.	.	.		.
.	.	.		.
.	.	.		.
$a^{(n-1)m}$,	$a^{(n-1)m+1}$,	$a^{(n-1)m+2}$ . . .		a^{nm-1}

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.

§. 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 $p = 3 = 2+1$		2. Diuiſor $p = 5 = 2.2+1$	
Poteſt.	Reſid.	Poteſt.	Reſid.
a^1)	1	a^2)	1, -1
		a^4)	1

3. Diuiſor $p = 7 = 2.3+1$		4. Diuiſor $p = 11 = 2.5+1$	
Poteſt.	Reſidua	Poteſt.	Reſid.
a^2	1, 2, -3	a^2	1, 4, 5, -3, -2
a^3)	1, -1	a^5)	1, -1
a^6)	1	a^{10})	1

5. Diuiſor $p = 13 = 2.2.3 + 1$

Poteſt. Reſidua

a^1 { 1, 4, 3, −1 / −3 −4)
a^2 { 1, −5, −1 / 5 1)
a^4 { 1, 3 / −4)
a^6) 1, −1
a^{12}) 1

6. Diuiſor $p = 17 = 2^4 + 1$

Poteſt. Reſidua

a^1 { 1, 2, 4, 8, −1 / −8 −4 −2]
a^4 { 1, 4, −1 / −4]
a^8) 1, −1
a^{16}) 1

7. Diuiſ. $p = 19 = 2.3.3 + 1$

Poteſt. Reſidua

a^1 { 1, 4, −3, 7, 9 / 5, 6, −5, −2)
a^2 { 1, 8, 7, −1 / −7 −8)
a^6 { 1, 7 / −7)
a^9) 1, −1

8. Diuiſ. $p = 23 = 2.11 + 1$

Poteſt. Reſidua

a^1 { 1, 4, −7, −5, 3, −11 / 6, −10, 9, 8, 2]
a^{11}) 1, −1

9. Diuiſor $p = 29 = 2.2.7 + 1$

Poteſt. Reſidua

a^1 { 1, 4, −13, 6, −5, 9, 7, −1 / −7 −9, 5, −6, 13, −4)
a^2 { 1, −13, −5, 7 / −9 −6 −4)
a^7 { 1, 12, −1 / −12)
a^{14}) 1, −1

10. Diuiſor $p = 31 = 2.3.5 + 1$

Poteſt. Reſidua

a^1 { 1, 9, −12, −15, −11, −6, 8, 10 / 7, −13, 2, 14, 5, 4, −3)
a^2 { 1, −4, −15, −2, 8, −1 / −8, 2, −15, 4)
a^5 { 1, −5, −6, −1 / 6, 5)
a^6 { 1, 2, 4 / −15, 8)
a^{10} { 1, 5 / −5)
a^{15}) 1, −1

11. Diuiſor $p = 37 = 2.2.3.3 + 1$

Poteſt. Reſidua

a^1 { 1, 4, 16, −10, −3, −12, −11, −7, 9, −1 / −9, 7, 11, 12, 3, 10, −16, −4)
a^2 { 1, 8, −10, −6, −11, −14, −1 / 14, 11, 6, 10, −8)
a^4 { 1, 16, −3, −12, 9 / 7, 12, 10, −4)
a^9 { 1, −10, −11, −1 / 11, 10)
a^9 { 1, −6, −1 / 6)
a^{12} { 1, −11 / 11)
a^{18}) 1, −1

12. Diuiſor $p = 41 = 2^3.5 + 1$

Poteſt. Reſidua

a^1 { 1, −2, 4, −8, 16, 9, −18, −5, 10, −20, −1 / 20, −10, 5, 18, −9, −16, 8, −4, 2)

a^4 { 1, 4, 16, −18, 10, −1
−10, 18, −16, −4)
a^5 { 1, −3, 9, 14, −1
−14, −9, 3,)
a^6 { 1, 16, 10
18, −4)
a^{10} { 1, 9, −1
−9,)
a^{20}) 1, −1

13. Diuisor $p = 43 = 2.3.7 + 1$
Poteſt. Reſidua
a^2 { 1, 9, −5, −2, −18, 10, 4, −7, −20, −8, 14
−19, 17, 21, −12, 13, 11, 6, 15, 16, −3)
a^3 { 1, 8, 21, −4, 11, 2, 16, −1
−16, −2, −11, 4, −21, −8,)
a^4 { 1, 21, 11, 16
−2, 4, −8)
a^7 { 1, −6, −7, −1
7, 6,)
a^{14} { 1, −7
6)
a^{21}) 1, −1

14. Diuisor $p = 47 = 2.23 + 1$
Poteſt. Reſidua
a^2 { 1, 4, 16, 17, 21, −10, 7, −19, 18, −22, 6, −23
12, 3, −11, 9, 14, −20, −5, −13, −15, 8, 2)
a^{23}) 1, −1

15. Diuisor $p = 53 = 2.2.13 + 1$
Poteſt. Reſidua
a^2 { 1, 4, 16, 11, −9, 17, 15, 7, −25, 6, 24, −10, 13, −1
−13, 10, −24, −6, 25, −7, −15, −17, 9, −11, −16, −4)

-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 { 1, 16, −9, 15, −25, 24, 13)
10, −6, −7, −17, −11, −4)
a^{12} { 1, −23, −1)
23)
a^{26}) 1, −1

16. Diuisor $p = 59 = 2.29 + 1$
Poteſt. Reſidua
a^2 { 1, 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)
a^{29}) 1, −1

17. Diuisor $p = 61 = 2.2.3.5 + 1$
Poteſt. Reſidua
a^2 { 1, 4, 16, 3, 12, −13, 9, −25, 22, 27, −14, 5, 20, 19, 15, −1
−15, −19, 20, −5, 14, −27, −22, 25, −9, 13, −12, −3, −16, −4
a^3 { 1, 8, 3, 24, 9, 11, 27, −28, 20, −23, −1
23, −20, 28, −27, −11, −9, −24, −3, −8,)
a^4 { 1, 16, 12, 9, 22, −14, 20, 15)
−19, −5, −27, 25, 13, −3, −4)
a^5 { 1, −29, −13, 11, −14, −21, −1)
21, 14, −11, 23, 29,)
a^6 { 1, 3, 9, 27, 20 −1)
−20, −27, −9, −3)
a^{10} { 1, −13, −14, −1)
14, 13,)
a^{12} { 1, −3, 9)
20, −27)
a^{15} { 1, 11, −1)
−11,)
a^{20} { 1, −14)
13)
a^{30} (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 $\pm 1, \pm 2, \pm 3, \pm 4$, 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-

diuiſa 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^1 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, $-a^{q-1}$,	a^2, $-a^{q-2}$,	a^3, $-a^{q-3}$,	a^4, $-a^{q-4}$	a^{q-3}, $-a^3$,	a^{q-2}, $-a^2$,	a^{q-1}, $-a$,	-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:

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

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

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

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.

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 nominis

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 $2q = f^\varphi g^\eta h^\theta k^\kappa$, ſit iſta multitudo

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

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 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