DE QVIBVSDAM EXIMIIS PROPRIETATIBVS CIRCA DIVISORES POTESTATVM OCCVRRENTIBVS.

§. 1.

Conſtat omnes progreſſiones geometricas, veluti $1; a; a^2; a^3; a^4$; etc. ita eſſe comparatas, vt, dum ſinguli termini per numerum quemcunque N, qui ad a ſit primus, diuiduntur, reſidua poſt certum interuallum iterum eodem ordine reuertantur; et quia primum reſiduum eſt vnitas, ſemper dabitur eiusmodi poteſtas a^n, quae per N diuiſa iterum relinquat vnitatem; ſequentes vero poteſtates a^{n+1}; a^{n+2}; a^{n+3}; etc. eadem reſidua praebebunt, quae ex terminis a, a^2, a^3, etc. ſunt nata. Deinde etiam demonſtratum eſt, ſi N fuerit numerus primus, tum ſemper poteſtatem a^{N-1} iterum pro reſiduo vnitatem exhibere. Saepenumero autem iſta poteſtas a^{N-1} minima eſt, quae per N diuiſa vnitatem relinquit; interdum vero etiam vſu venit, vt minor poteſtas a^n idem praeſtet; tum autem ſemper n eſt pars aliquota exponentis $N-1$; atque hinc naſcitur quaeſtio attentione noſtra non indigna: *Quaenam pro quo-*

uouis diuiſore N ſit minima poteſtas a^n, *ex qua reſiduum oriatur* $= 1$? Atque hinc quaeſtio alia latius patens proponi poteſt: *Quaenam ſit infima poteſtas* a^n, *quae per datum numerum N diuiſa datum relinquat reſiduum* 1? Quae quaeſtio huc redit, vt exhibeatur minima formula $a^n - r$, quae per datum numerum N fuerit diuiſibilis. Quin etiam quaeſtio adhuc generalius proponi poteſt, vt *inueſtigetur exponens x, quo haec formula* $fa^x + g$ *reddatur diuiſibilis per datum numerum N.*

§. 2. Solutio huius problematis inprimis requiritur ad numeros perfectos inueſtigandos. Cum enim forma horum numerorum ſit $2^{n-1}(2^n - 1)$, quoties $2^n - 1$ fuerit numerus primus; ſtatim euidens eſt, hoc euenire non poſſe, niſi ipſe exponens n fuerit numerus primus; quandoquidem huiusmodi forma $2^{\alpha\beta} - 1$ ſemper habet diuiſores $2^\alpha - 1$ et $2^\beta - 1$. Neque vero viciſſim ſequitur, quoties n fuerit numerus primus, tum etiam formulam $2^n - 1$ fore numerum primum. Plures enim caſus iam ſunt explorati, quibus hoc non euenit; veluti ſi fuerit $n = 11$; $n = 23$; item $n = 29$; $n = 37$; ac praeterea ſine dubio pluribus aliis caſibus, quos omnes nondum explorare licuit. Alia autem via non patet ad hos caſus inueſtigandos, praeter eam, qua olim ſum vſus, quae ita ſe habebat: Fingatur formulae $2^n - 1$ diuiſor, ſi quem habet, eſſe $2p + 1$; et cum formula $2^{np} - 1$ ſemper diuiſorem habeat $2p + 1$; ſequitur hoc fieri non poſſe, niſi n fuerit pars aliquota ipſius $2p$, ſiue $2p$ multiplum ipſius n. Sumto ergo $p = \lambda n$, fiet diuiſor $2\lambda n + 1$; ex quo concluditur, ſi formula $2^n - 1$ non ſit numerus primus, eam alios diuiſores certe habere non poſſe, niſi qui in

forma $2\lambda n + 1$ contineantur; atque hoc principio olim ſum vſus in inueſtigatione numerorum primorum. Simili modo cum olim aſſertionem *Fermatii* examinaſſem, qua aſſeuerarat, formulam $2^n + 1$ ſemper eſſe numerum primum, quoties exponens n fuerit ipſe poteſtas binarii, quaeſtionem ſupra memoratam in ſubſidium vocare ſum coactus, qua poſt plures calculos tandem inueni, formulam $2^{32} + 1$ diuiſorem habere 641; ex quo nunc quaeſtio formari poteſt: quaenam ſit binarii poteſtas infima, quae vnitate aucta fiat per 641 diuiſibilis? Methodus quidem, qua olim ſum vſus, per calculos ſatis taedioſos procedebat; nunc autem ſe mihi obtulit alia methodus multo ſimplicior et expeditior, non ſolum hos memoratos caſus circa poteſtates binarii reſoluendi, ſed quae adeo ad quaeſtionem illam generaliſſimam adplicari poſſit, qua ſcilicet quaeritur infima poteſtas a^α, vt formula $fa^\alpha + g$ per datum numerum N fiat diuiſibilis. Hanc ergo nouam methodum hic breuiter ſum expoſiturus; huic autem in finem ſequentia Lemmata ſunt praemittenda:

Lemma 1.

§. 3. Si numerus quicunque A per alium N diuiſus relinquat reſiduum r; tum etiam omnes hi numeri: $r \mp N$; $r \mp 2N$; $r \mp 3N$, et in genere $r \mp \lambda . N$, aeque tanquam reſidua ſpectari poſſunt, quandoquidem hae ipſae formulae per N diuiſae relinquunt r.

Lemma 2.

§. 4. Si numerus A per diuiſorem N diuiſus relinquat reſiduum a, numerus vero B per eundem diuiſus reſi-

reſic
reſid
bunt
per

det
A^{x+}
a^{1x};

beat
aſſign
quide
loco
rit, v
quotu

fiatqu
ſpectar
quandi
muner

principio olim
norum. Simili
ninaſſem, qua
numerum pri-
s binarii, quae-
rocare ſum co-
ni, formulam
nc quaeſtio for-
ſima, quae vni-
s quidem, qua
os procedebat;
multo ſimpli-
itos caſus circa
ad quaeſtionem
ilicet quaeritur
datum nume-
methodum hic
inem ſequentia

r alium N di-
nes hi numeri:
$r \mp \lambda . N$, ae-
ndoquidem hae

N diuiſus re-
eundem diuiſus
reſi-

reſiduum β; tum productum AB per N diuiſum relinquet reſiduum ab. Hinc ergo poteſtates A^2; A^3; A^4; etc. dabunt reſidua a^2; a^3; a^4; etc., quae pro lubitu, diuiſione per N facta, ad minimos valores reducere licet.

Lemma 3.

§. 5. Si propoſito diuiſore N poteſtas a^α reſiduum det $= r$, poteſtas vero a^β reſiduum $= s$; tum poteſtas A^{x+y} reſiduum dabit $= rs$; vnde etiam hae poteſtates a^{2x}; a^{3x}; a^{4x}; etc. reſidua producent r^2; r^3; r^4; etc.

Lemma 4.

§. 6. Si vt ante pro diuiſore N poteſtas a^α praebeat reſiduum r, poteſtas vero a^β reſiduum s; hinc etiam aſſignari poterit reſiduum reſpondens poteſtati a^{x-y}, quod quidem fiet $= \frac{r}{s}$, ſi r per s diuidi poſſet. Quia autem loco r ſumere licet $r \mp \lambda N$, ſemper λ ita definiri poterit, vt haec forma $r \mp \lambda N$ per s diuidi queat, ac tum quotus dabit ipſum reſiduum poteſtati a^{x-y} reſpondens.

Lemma 5.

§. 7. Si pro diuiſore N poteſtas a^α relinquat r, fiatque $r \mp \lambda N = a^\alpha s$, ita vt $a^\alpha s$ tanquam reſiduum ſpectari poſſit; tum poteſtas $a^{x-\alpha}$ reſiduum relinquet s, quandoquidem diuidendum et reſiduum ſemper per communem diuiſorem deprimere licet.

Problema generale.

§. 8. Propoſita formula $fa^x + g$, inuenire minimum exponentem x, quo haec formula per datum numerum N fiat diuiſibilis, ſiquidem id fuerit poſſibile.

Solutio.

Quaeſtio ergo huc reducitur, vt forma fa^x per numerum datum N diuiſa relinquat reſiduum $= -g$. Quia nunc per Lemma primum pro reſiduo etiam haberi poteſt $-g \mp \lambda N$, facile λ ita aſſumere licebit, vt haec formula factorem obtineat a, vel adeo eius altiorem poteſtatem a^α. Sit igitur $-g \mp \lambda N = a^\alpha . r$, atque per lemma poſtremum quantitas $fa^{x-\alpha}$ per N diuiſa reſiduum relinquet $= r$. Iam ſimili modo fiat $r \mp \lambda N = a^\beta . s$, et quantitas $fa^{x-\alpha-\beta}$ dabit reſiduum s, ſicque vlterius progredi licebit, ſumendo $s \mp \lambda N = a^\gamma . t$; tum vero etiam $t \mp \lambda N = a^\delta . u$; porro $u \mp \lambda . N = a^\varepsilon . v$ etc.; quo pacto quantitas $a^{x-\alpha-\beta-\gamma-\delta-\varepsilon}$ per N diuiſa reſiduum relinquet $= v$; haeque operationes eousque continuentur, donec perueniatur ad reſiduum $= f$; ita, vt haec quantitas $fa^{x-\alpha-\beta-\gamma \text{ etc.}}$ reſiduum det $= f$; id quod ſemper continget, ſiquidem quaeſtio fuerit poſſibilis; atque hoc adeo antequam numeri ab exponente ſubtrahendi $\alpha + \beta + \gamma + \delta + \varepsilon$ etc. ſuperent numerum $N - 1$, quia ſi exponentes ipſius a vltra hunc limitem continuentur, eadem reſidua recurrunt. Cum autem ad talem caſum fuerit peruentum, quo reſiduum eſt f, quia hoc euenit, ſi exponens ipſius a fuerit $= 0$; hinc concludemus $x = \alpha + \beta + \gamma + \delta$ etc. Omnes ergo has operationes ita ſuccincte repraesentaſſe iuuabit:

$$
\begin{aligned}
-g \mp \lambda . N &= a^\alpha . r \\
r \mp \lambda . N &= a^\beta . s \\
s \mp \lambda . N &= a^\gamma . t \\
t \mp \lambda . N &= a^\delta . u \\
&\text{- - - - - -} \\
&\text{- - - - - -} \\
&\text{- - - - - -} \\
&\text{- - - - - -} \\
z \mp \lambda . N &= a^\zeta . f
\end{aligned}
$$

hincque deducitur concluſio $x = \alpha + \beta + \gamma + \delta \ldots + \zeta$. Sin autem nunquam perueniatur ad tale reſiduum f, antequam ſumma $\alpha + \beta + \gamma + \delta$ . . . . . vsque ad $N - 1$ aſcendat, problema pro impoſſibili eſt habendum.

Quanquam hae operationes expedite inſtituuntur; tamen eas ſaepenumero haud mediocriter contrahere licebit, praecipue ſi peruentum fuerit ad exiguum reſiduum, puta t, reſpondens formulae $f . a^{x-\Theta}$, ponendo $\Theta = \alpha + \beta + \gamma$; tum enim eius quadratum t^2 reſpondebit formulae $f^2 . a^{2x-2\Theta}$, quae per primam diuidatur, vt formulae $fa^{x-2\Theta}$ reſpondeat reſiduo $\frac{t^2}{-g}$, quod ſi non fuerit numerus integer, loco t^2 ſcribendo $t^2 \mp \lambda N$, facile eo reducitur. Quin etiam cubus reſidui t^3 reſpondebit formulae $f^3 a^{3x-3\Theta}$, quae per quadratum primae diuiſa dabit formulae $fa^{x-3\Theta}$ reſiduum $= \frac{t^3}{g^2}$. Quin etiam binas formulas diuerſas in ſe inuicem ducere licebit, et per primam diuidendo iterum ad nouam huiusmodi formulam perueniretur. Inprimis autem hoc compendium maximum vſum praeſtabit, vbi ad reſidua ſatis parua fuerit peruentum; quorum poteſtates etiam ſuperio-

res facile capiuntur, atque insuper fuerit primum residuum $-g$ numerus satis paruus vel adeo vnitas.

Corollarium.

§. 9. Quoniam has operationes clare descripsimus, eas adplicemus ad casus magis speciales. Ac primo quidem occurrit formula $2^x \mp 1$. Pro variis igitur diuisoribus quaeramus exponentem x, vt potestas 2^x residuum relinquat ∓ 1. Sufficiet autem hoc residuum $+1$ statuisse; si enim 2^x fuerit minima potestas residuum dans $= +1$; tum potestas $2^{\frac{1}{2}x}$ necessario dabit residuum $= -1$, siquidem x fuerit numerus par; sin autem x fuerit impar, hic casus plane est impossibilis.

Exemplum 1.

§. 10. Quaeratur minima potestas 2^x, quae per 23 diuisa relinquat 1, siue vt $2^x - 1$ diuisibilis fiat per 23. Hic igitur est $N = 23$; $a = 2$ et primum residuum $= 1$; vnde operationes nostrae sequenti modo procedent:

$1 + 23 = 24 = 2^3 . 3$

$3 - 23 = -20 = -2^2 . 5$

$-5 - 23 = -28 = -2^2 . 7$

$-7 + 23 = +16 = +2^4 . 1.$

Sic iam peruentum est ad residuum optatum $+1$, ob $f = 1$; sicque concludimus $x = 11$. Cum ergo formula $2^{11} - 1$ sit diuisibilis per 23 et 11 numerus impar, nulla plane datur formula $2^x + 1$ per 23 diuisibilis.

Exem-

Exemplum 2.

§. 11. Proponatur diuisor 41, per quem formula $2^x - 1$ reddi debeat diuisibilis. Ergo ob $N = 41$; $a = 2$; $f = 1$ et primum residuum $= 1$, habebimus:

$1 - 41 = -40 = -2^3 . 5$

$-5 . + 41 = +36 = +2^2 . 9$

$+9 - 41 = -32 = -2^5 . 1.$

Hic iam subsistere possumus; cum enim potestas 2^{x-10} relinquat -1, eius quadratum 2^{2x-20} relinquet $+1$, et per primam formam diuidendo prodit 2^{x-20} pro residuo $+1$ optato; sicque habemus $x = 20$. Simul autem hinc patet, potestati 2^{10} residuum conuenire -1. ita vt formulae simpliciissimae per 41 diuisibiles sint: $2^{10} + 1$ et $2^{10} - 1$.

Exemplum 3.

§. 12. Pro diuisore 73 quaeratur formula simpliciissima $2^x \mp 1$ per eum diuisibilis. Hic est $N = 73$; $a = 2$; et sumto primo residuo $= +1$ fiet

$1 - 73 = -72 = -2^3 . 9$

$-9 + 73 = +64 = +2^6 . 1$

vbi ergo iam subsistere licet, eritque $x = 9$, vnde formula $2^9 - 1$ per 73 est diuisibilis; et quia 9 est numerus impar, nulla plane datur formula $2^x + 1$ per eundem numerum N diuisibilis.

Exemplum 4.

§. 13. Proponatur diuisor $N = 77$ et sumto primo residuo $= 1$, calculus ita se habebit:

$+1-77=-76=-2^2.19$
$-19-77=-96=-2^5.3$
$-3-77=-80=-2^4.5$
$-5+77=+72=+2^3.9$
$+9-77=-68=-2^2.17$
$-17+77=+60=2^2.15$
$+15+77=+92=2^2.23$
$+23+77=+100=2^2.25$
$+25-77=-52=-2^2.13$
$-13+77=+64=2^6.1$

Vnde $x=30$; ita vt $2^{30}-1$ sit simplicissima forma per 77 diuisibilis. Hinc tamen non sequitur, istam: $2^{15}+1$ diuisibilem esse per 77, propterea quod 77 non est numerus primus; etsi enim $2^{30}-1$ diuisibile sit per 77; neutiquam sequitur, alterutrum eius factorum $2^{15}+1$ siue $2^{15}-1$ diuisibilem esse debere, quemadmodum rite concludere liceret, si diuisor esset numerus primus; hoc enim casu fieri potest, vt alter factor per 7, alter vero per 11 sit diuisibilis; ac reuera, cum 2^5+1 per 11 sit diuisibile, etiam $2^{15}+1$ per 11 erit diuisibile; at vero per 7 diuisibilis est altera formula $2^{15}-1$, quia factorem habet $2^3-1=7$.

Exemplum 5.

§. 14. Sit diuisor $N=89$, et sumto iterum primo residuo $=1$, faciemus:

$1-89=-88=-2^3.11$
$-11-89=-100=-2^2.25$
$-25+89=+64=2^6.1$.

Hinc

Hin
bet

Sum
diui
mus
tum
diuil

fiet:

na forma per 77
: $2^{15}+1$ diuisi-
on est numerus
77; neutiquam
-1 siue $2^{15}-1$
: concludere li-
: enim casu fieri
per 11 sit diui-
diuisibile, etiam
per 7 diuisibilis
: $2^3-1=7$.

nto iterum pri-

Hinc

Hinc ergo $x=11$, sicque formula $2^{11}-1$ diuisorem habet 89; nulla autem datur formula alterius speciei $2^{11}+1$.

Exemplum 6.

§. 15. Sit diuisor $N=105$; eritque:

$1-105=-104=-2^3.13$
$-13+105=+92=+2^2.23$
$+23+105=+128=+2^7.1$.

Summa exponentium $=12$; ergo $x=12$, et formula $2^{12}-1$ diuisibilis erit per 105. At quia 105 non est numerus primus, non sequitur, fore 2^6+1 per 105 diuisibile. Tantum enim diuidi potest per 5; dum altera formula 2^6-1 diuisibilis est per 3. 7.

Exemplum 7.

§. 16. Sit $N=223$. et primum residuum $=1$, fiet:

	Summae exponentium.
$1+223=224=2^5.7$	5
$7-223=-216=-2^3.27$	8
$-27+223=+196=2^2.49$	10
$49+223=+272=2^4.17$	14
$17+223=+240=2^4.15$	18
$15-223=-208=-2^4.13$	22
$-13-223=-236=-2^2.59$	24
$-59+223=+164=2^2.41$	26
$41+223=+264=2^3.33$	29
$33+223=+256=2^8.1$	37

Summa exponentium $=37$

ergo $x = 37$, et formula $2^{37} - 1$ diuisibilis per 223. Hinc quia 23 est numerus impar, certum est, nullam dari formulam $2^x + 1$ per 223 diuisibilem.

§. 17. Quo nunc pateat, quomodo has operationes possint subleuari, subsistamus iam in quinta, vbi residuum prodiit 15, et summa exponentium $= 18$; vnde haec potestas 2^{x-18} residuum dat 15. Sumantur quadrata, et potestas 2^{2x-36} residuum dat 225 siue 2; haec iam per primam diuisa praebet pro potestate 2^{x-36} residuum $2 = 2^1 \cdot 1$, ergo potestas 2^{x-37} praebet residuum 1, vnde iam liquet esse $x = 37$.

Exemplum 8.

§. 18. Sit $N = 641$. et primum residuum $= 1$, fiet:

$1 - 641 = -640 = -2^7 \cdot 5$	. . .	7
$-5 + 641 = +636 = 2^2 \cdot 159$	. .	9
$+159 + 641 = +800 = 2^5 \cdot 25$	. .	14
$+25 - 641 = -616 = -3^1 \cdot 77$	. .	17
$-77 + 641 = 564 = 2^2 \cdot 141$	. .	19
$+141 - 641 = -500 = -2^2 \cdot 125$	.	21
$-125 + 641 = 516 = 2^2 \cdot 129$	. .	23
$+129 - 641 = -512 = -2^9 \cdot 1$	. .	32

vbi iam subsistere possumus. Quia enim residuum est -1, si pro primo residuo sumsissemus -1, vt formula quaereretur $2^x + 1$ per 641 diuisibilis, omnia sequentia residua signo contrario adfecta prodiissent et vltimum fuisset $+1$; vnde rite concludimus esse $x = 32$; ita vt iam formula $2^{32} + 1$ sit diuisibilis per 641. Euidens autem est, pro minima formula huius formae $2^x - 1$ fore $x = 64$.

§. 19.

§. 19. Hunc autem laborem mirifice contrahere licet. Statim enim post primam operationem subsistere possemus, quae pro potestate 2^{x-7} praebet residuum 9. Sumamus statim potestatem quartam, et pro 2^{4x-28} habebimus residuum 625, siue $-16 = -2^4 \cdot 1$. ita vt 2^{x-28} conueniat residuum -1. Diuidendo igitur per cubum primae, seu 2^{3x}, cuius residuum itidem est 1, etiam huius potestatis 2^{x-28} residuum erit -1, id quod ante per ambages eruimus.

Exemplum 9.

§. 20. Sit $N = 385 = 5 \cdot 7 \cdot 11$. et primum residuum $= 1$. erit:

$1 - 385 = -384 = -2^7 \cdot 3$	. . .	7
$-3 - 385 = -388 = -2^2 \cdot 97$	. .	9
$-97 + 385 = 288 = +2^5 \cdot 9$	. . .	14
$+9 - 385 = -376 = -2^3 \cdot 47$	. .	17
$-47 - 385 = -432 = -2^4 \cdot 27$	. .	21
$-27 - 385 = -412 = -2^2 \cdot 103$	.	23
$-103 - 385 = -488 = -2^3 \cdot 61$	. .	26
$-61 + 385 = +324 = +9^2 \cdot 81$	. .	28
$+81 - 385 = -304 = -2^4 \cdot 19$	. .	32
$-19 - 385 = -404 = -2^2 \cdot 101$	.	34
$-101 + 385 = +284 = +2^2 \cdot 71$	. .	36
$+71 + 385 = +456 = +2^3 \cdot 57$	. .	39
$+57 - 385 = -328 = -2^3 \cdot 41$	. .	42
$-41 + 385 = +344 = +2^3 \cdot 43$	. .	45
$+43 + 385 = +428 = +2^2 \cdot 107$	. .	47
$+107 + 385 = +492 = +2^2 \cdot 123$	. .	49
$+123 + 385 = +508 = +2^2 \cdot 127$	.	51
$+127 + 385 = +512 = +2^9 \cdot 1$	. .	60

 ergo

ergo $x = 60$, ita vt formula $2^{60} - 1$ diuisibilis sit per 385; quod etiam inde concludi potuisset, quod diuisoris nostri factores sunt 5, 7, 11. quorum primus 5 est diuisor formulae $2^2 + 1$. secundus 7 est formulae $2^3 - 1$; tertius 11 est formulae $2^5 + 1$; at formula per has tres diuisibilis simplicior non datur quam $2^{60} - 1$.

§. 21. Videamus nunc, quomodo hae operationes contrahi potuissent. Tertia operatione prodiit potestas $2^{3^3 - 14}$ residuum dans 9; vnde eius quadratum $2^{3^4 - 28}$ residuum praebet 81; cubus autem $2^{3^5 - 42}$ praebet residuum 729, siue 344, siue -41; hinc quarta potestas $2^{4 \cdot 3^5 - 56}$ dabit residuum -369, siue $+16 = 2^4 \cdot 1$. ergo per 2^4 diuidendo potestas $2^{4 \cdot 3^5 - 60}$ dat residuum $+1$. et diuidendo per 2^{3^5}, cuius residuum etiam est $+1$, potestas $2^{3^5 - 60}$ residuum dabit $+1$, vti modo inuenimus.

Exemplum 10.

§. 22. Sit $N = 311$. fietque:

$1 + 311 = +312 = 2^3 \cdot 39$	3
$39 - 311 = -272 = -2^4 \cdot 17$	7
$-17 - 311 = -328 = -2^3 \cdot 41$	10
$-41 - 311 = -352 = -2^5 \cdot 11$	15
$-11 + 311 = +300 = +2^2 \cdot 75$	17
$+75 - 311 = -236 = -2^2 \cdot 59$	19
$-59 + 311 = +252 = +2^2 \cdot 63$	21
$+63 - 311 = -248 = -2^3 \cdot 31$	24
$-31 + 311 = +280 = +2^3 \cdot 35$	27
$+35 - 311 = -276 = -2^2 \cdot 69$	29
$-69 - 311 = -380 = -2^2 \cdot 95$	31
	-95

bilis sit per
od diuisoris
5 est diui-
ae $2^5 - 1$;
er has tres

operationes
otestas $2^{3^5 - 14}$
residuum
duum 729,
$^{-56}$ dabit re-
^{4} diuidendo
lo per 2^{3^5},
^{60} residuum

	3
	7
	10
	15
	17
	19
	21
	24
	27
	29
	31
	-95

$-95 + 311 = +216 = +2^3 \cdot 27$	34
$+27 - 311 = -284 = -2^2 \cdot 71$	36
$-71 + 311 = +240 = +2^4 \cdot 15$	40
$+15 - 311 = -296 = -2^3 \cdot 37$	43
$-37 - 311 = -348 = -2^2 \cdot 87$	45
$-87 + 311 = +224 = +2^5 \cdot 7$	50
$+7 - 311 = -304 = -2^4 \cdot 19$	54
$-19 + 311 = +292 = +2^2 \cdot 73$	56
$+73 + 311 = +384 = +2^7 \cdot 3$	63
$+3 - 311 = -308 = -2^2 \cdot 77$	65
$-77 - 311 = -388 = -2^2 \cdot 97$	67
$-97 - 311 = -408 = -2^3 \cdot 51$	70
$-51 + 311 = +260 = +2^2 \cdot 65$	72
$+65 + 311 = +376 = +2^3 \cdot 47$	75
$+47 - 311 = -264 = -2^3 \cdot 33$	78
$-33 - 311 = -344 = -2^3 \cdot 43$	81
$-43 + 311 = +268 = +2^2 \cdot 67$	83
$+67 - 311 = -244 = -2^2 \cdot 61$	85
$-61 - 311 = -372 = -2^2 \cdot 93$	87
$-93 - 311 = -404 = -2^2 \cdot 101$	89
$-101 - 311 = -412 = -2^3 \cdot 103$	91
$-103 + 311 = +208 = +2^4 \cdot 13$	95
$+13 + 311 = +324 = +2^2 \cdot 81$	97
$+81 + 311 = +392 = +2^3 \cdot 49$	100
$+49 + 311 = +360 = +2^3 \cdot 45$	103
$+45 + 311 = -356 = -2^2 \cdot 89$	105
$-89 - 311 = -400 = -2^4 \cdot 25$	109
$-25 - 311 = -336 = -2^4 \cdot 21$	113
$-21 - 311 = -332 = -2^2 \cdot 83$	115
$-83 + 311 = +228 = +2^2 \cdot 57$	117
$+57 + 311 = +368 = +2^4 \cdot 23$	121
	+ 29

$$+23-311=-288=+2^5.9 \quad \ldots 126$$
$$+9+311=+320=+2^6.5 \quad \ldots 132$$
$$+5+311=+316=+2^2.79 \quad \ldots 134$$
$$+79-311=-232=-2^3.29 \quad \ldots 137$$
$$-29-311=-340=-2^2.85 \quad \ldots 139$$
$$-85-311=-396=-2^2.99 \quad \ldots 141$$
$$-99+311=+212=+2^2.53 \quad \ldots 143$$
$$+53+311=+364=+2^2.91 \quad \ldots 145$$
$$+91-311=+220=-2^2.55 \quad \ldots 147$$
$$-55+311=+256=2^8.1 \quad \ldots 155$$

ergo $x=155$, ſicque minima formula per 311 diuiſibilis eſt $2^{155}-1$.

Si ſubſtitiſſemus in 25^ta operatione, habuiſſemus 2^{x-75}, eiusque reſiduum 47; et ſumtis quadratis 2^{2x-150}, ſiue per principalem diuidendo, 2^{x-150} cum reſiduo 2209, ſiue $32=2^5.1$. vnde poteſtas 2^{x-155} reſiduum optatum producit $+1$. Sin autem in operatione 17^ma ſubſtitiſſemus, habuiſſemus 2^{x-50} cum reſiduo 7; ſumtisque cubis 2^{3x-150} cum reſiduo 343, ſiue $32=2^5.1$, ita vt iam poteſtas 2^{3x-155}, ſiue etiam 2^{x-155} reſiduum det $+1$; vnde ſequitur $x=155$, vt ante.

Exemplum II.

§. 23. Sit diuiſor $N=233$, et ſumto primo reſiduo $=1$, faciemus:

	Summa exponent.
$1-233=-232=-2^3.29$	3
$-29+233=+204=+2^2.51$	5
$+51+233=+284=+2^2.71$	7
$+71+233=+304=+2^4.19$	11
	$+19$

$$+19+233=+252=+2^2.63 \quad \ldots 13$$
$$+63+233=+296=+2^3.37 \quad \ldots 16$$
$$+37-233=-196=-2^2.49 \quad \ldots 18$$
$$-49+233=+184=+2^3.23 \quad \ldots 21$$
$$+23+233=+256=+2^8.1 \quad \ldots 29$$

Scholion.

§. 24. Hac igitur methodo pro quolibet diuiſore N facile computatur formula ſimpliſſima $2^x \pm 1$ per eum diuiſibilis. Haud igitur abs re viſum eſt, tabulam hic adiungere, in qua pro omnibus numeris primis vsque ad 400 ſimpliciſſimae formulae exhibentur; diuiſores autem primos commode in quatuor ordines, ſecundum formas $8n+1$; $8n-1$; $8n+3$ et $8n-3$, diſtribui conueniet:

N		N	
$8n+1$	$2^x \pm 1$	$8n-1$	2^x+1
1	2^0-1.	7	2^3-1
17	2^4+1.	23	$2^{11}-1$.
41	$2^{10}+1$.	31	2^5-1.
73	2^9-1.	47	$2^{23}-1$.
89	$2^{11}-1$.	71	$2^{35}-1$.
97	$2^{24}+1$.	79	$2^{39}-1$.
113	$2^{14}+1$.	103	$2^{51}-1$.
137	$2^{34}+1$.	127	2^7-1.
193	$2^{48}+1$.	151	$2^{75}-1$.
233	$2^{29}+1$.	167	$2^{83}-1$.
241	$2^{15}+1$.	191	$2^{95}-1$.
257	2^8+1.	199	$2^{99}-1$.
281	$2^{35}+1$.	223	$2^{37}-1$.

N $8n+1$	$2^x \pm 1$	N $8n-1$	$2^x \pm 1$
313	$2^{78}+1$	239	$2^{119}-1$
337	$2^{21}-1$	263	$2^{131}-1$
353	$2^{44}+1$	271	$2^{135}-1$
401	$2^{100}+1$	311	$2^{155}-1$
		359	$2^{179}-1$
		367	$2^{183}-1$
		383	$2^{191}-1$
		431	$2^{215}-1$.

N $8n+3$	2^x+1	N $8n-3$	$2^x \pm 1$
3	2^1+1	5	2^2+1
11	2^5+1	13	2^6+1
19	2^9+1	29	$2^{14}+1$
43	2^7+1	37	$2^{18}+1$
59	$2^{29}+1$	53	$2^{26}+1$
67	$2^{33}+1$	61	$2^{30}+1$
83	$2^{41}+1$	101	$2^{50}+1$
107	$2^{53}+1$	109	$2^{18}+1$
131	$2^{65}+1$	149	$2^{74}+1$
139	$2^{69}+1$	157	$2^{36}+1$
163	$2^{81}+1$	173	$2^{86}+1$
179	$2^{89}+1$	181	$2^{90}+1$
211	$2^{105}+1$	197	$2^{98}+1$
227	$2^{113}+1$	229	$2^{38}+1$
251	$2^{85}+1$	269	$2^{134}+1$

N

Hos
theor
firma

$8n \pm$
fin au
bilis
fempe
ceſſe
per e
nibus
fuerit
mamu

$12n$

N

N $8n+3$	$2^x \pm 1$	N $8n-3$	$2^x \pm 1$
283	$2^{47}+1$	277	$2^{46}+1$
307	$2^{51}+1$	293	$2^{146}+1$
331	$2^{15}+1$	317	$2^{158}+1$
347	$2^{173}+1$	349	$2^{174}+1$
371	$2^{185}+1$	373	$2^{186}+1$
379	$2^{189}+1$	389	$2^{194}+1$
		397	$2^{22}+1$

Hos caſus probe perpendentes ſtabilire poterimus ſequens theorema, quod eo magis notatu dignum videtur, quod firma demonſtratione etiamnum indiget.

Theorema.

§. 25. Si numerus primus $2p+1$ fuerit formae $8n \pm 1$, per eum ſemper diuiſibilis erit formula 2^p-1; ſin autem habeat hanc formam: $8n \pm 3$, per eum diuiſibilis erit formula 2^p+1. Cum enim formula $2^{2p}-1$ ſemper diuiſibilis ſit per numerum primum $2p+1$; neceſſe eſt, vt altervtra harum formularum: 2^p-1, vel 2^p+1 per evndem diuidi queat; quod cum aeque valeat de omnibus aliis poteſtatibus $a^{2p}-1$, dummodo a ad $2p+1$ fuerit primus, prouti pro a alios atque alios valores aſſumamus, ſequentia theoremata vera deprehenduntur.

Theorema 2.

§. 26. Si numerus primus $2p+1$ fuerit formae $12n \pm 1$, per eum ſemper diuiſibilis erit formula 3^p-1.

Sin autem habeat formam $12n \mp 5$, per eum diuisibilis erit formula $3^p + 1$.

Theorema 3.

§. 27. Sumto $a = 5$, si $2p+1$ fuerit numerus primus, vtrum per eum diuisibilis sit siue formula $5^p - 1$, siue $5^p + 1$, sequens tabella declarat:

Si fuerit $2p+1$	Diuisibilis erit
$20.n \mp 1$	$5^p - 1$
$20.n \mp 3$	$5^p + 1$
$20.n \mp 7$	$5^p + 1$
$20.n \mp 9$	$5^p - 1$.

Theorema 4.

§. 28. Sumto $a = 6$, si fuerit $2p+1$ numerus primus, vtrum per eum diuisibilis sit siue formula $6^p - 1$, siue $6^p + 1$, sequens tabella declarat:

Si fuerit $2p+1$	Diuisibilis erit
$24n \pm 1$	$6^p - 1$
$24n \pm 5$	$6^p - 1$
$24n \pm 7$	$6^p + 1$
$24n \pm 11$	$6^p + 1$

Theorema 5.

§. 29. Sumto $a = 7$, si fuerit $2p+1$ numerus primus, vtrum per eum diuisibilis sit siue formula $7^p - 1$, siue

siue formula $7^p + 1$, ex sequenti tabella patet:

Si fuerit $2p+1$	Diuisibilis erit
$28n \pm 1$	$7^p - 1$
$28n \pm 3$	$7^p - 1$
$28n \pm 5$	$7^p + 1$
$28n \pm 9$	$7^p - 1$
$28n \pm 11$	$7^p + 1$
$28n \pm 13$	$7^p + 1$

Theorema 6.

§. 30. Sumto $a = 8$, si fuerit $2p+1$ numerus primus, vtrum per eum diuisibilis sit siue formula $8^p - 1$, siue $8^p + 1$, sequens tabella ostendit:

Si fuerit $2p+1$	Diuisibilis erit
$32n \pm 1$	$8^p - 1$
$32n \pm 3$	$8^p + 1$
$32n \pm 5$	$8^p + 1$
$32n \pm 7$	$8^p - 1$
$32n \pm 9$	$8^p - 1$
$32n \pm 11$	$8^p + 1$
$32n \pm 13$	$8^p + 1$
$32n \pm 15$	$8^p - 1$

Theorema 7.

§. 31. Sumto $a = 10$, si fuerit $2p+1$ numerus primus, vtrum per eum diuisibilis sit siue formula $10^p - 1$, siue $10^p + 1$, ex sequenti tabella perspicitur:

Si fuerit $2p+1$.	Diuiſibilis erit
$40.n \pm 1$	$10^p - 1$
$40.n \pm 3$	$10^p - 1$
$40.n \pm 7$	$10^p + 1$
$40.n \pm 9$	$10^p - 1$
$40.n \pm 11$	$10^p + 1$
$40.n \pm 13$	$10^p - 1$
$40.n \pm 17$	$10^p + 1$
$40.n \pm 19$	$10^p + 1$

Theorema generale.

§. 32. Quicunque fuerit numerus a, ſi $2p+1$ denotet numerum primum et caſu $p = f$ innotuerit, vtrum formula $a^f - 1$, an $a^f + 1$ diuiſibilis ſit per $2f+1$; tum generatim eiusdem generis formula, ſiue $a^p - 1$, ſiue $a^p + 1$ diuiſibilis erit per $2p+1$, ſi fuerit $2p+1 = 4an \mp (2f+1)$, quicunque numerus pro n accipiatur, dummodo inde prodeat $2p+1$ numerus primus.

Corollarium 1.

§. 33. Ex praecedentibus theorematibus ſatis liquet, caſu $f = 0$ ſemper formulam $a^p - 1$ diuiſibilem fore per $2p+1 = 4an \mp 1$, quoties ſcilicet hic numerus fuerit primus.

Corollarium 2.

§. 34. Sin autem ſit $f = 1$, prouti ſiue $a-1$, ſiue $a+1$ per 3 diuidi poteſt, ſimili caſu generatim ſiue for-

formula $a^p + 1$ per numerum primum $2p+1$ erit diuiſibilis, quoties $2p+1$ in hac forma: $4an \pm 3$ continetur.

Scholion.

§. 35. Theoremata autem particularia allata facile vlterius continuari poſſunt, ſi ſequens problema in ſubſidium vocetur, cuius quidem ſolutio firmiſſimis rationibus innititur.

Problema.

§. 36. Quicunque fuerit numerus a, ſi $2p+1$ denotet numerum primum, quouis caſu oblato inueſtigare, vtrum formula $a^p - 1$, an altera $a^p + 1$ diuiſibilis ſit per $2p+1$.

Solutio.

Quaerantur omnia reſidua, quae ex diuiſione quadratorum per numerum $ap+1$ reſultant, quae ſint 1; α; β; γ; δ; etc. multitudine $= p$, numeri autem ab his diuerſi non-reſidua adpellentur. Quo facto ſi numerus a inter reſidua reperiatur; tum ſemper formula $a^p - 1$ erit diuiſibilis; ſin autem numerus a inter non-reſidua occurrat; tum altera formula $a^p + 1$ diuiſibilis erit. Haec autem regula ita demonſtratur: Si fuerit a reſiduum ex cuiusdam quadrati x^2 diuiſione per $2p+1$ natum; tum erit $x^2 - a$ per $2p+1$ diuiſibile; ſiue aequabitur cuipiam multiplo $m(2p+1)$; ita vt ſit $a = x^2 - m(2p+1)$. Hinc ergo fiet $a^p = (x^2 - m(2p+1))^p$, quae poteſtas per $2p+1$ diuiſa idem reſiduum relinquet ac poteſtas

$(x^\alpha)^\beta$; verum haec poteſtas abit in $x^{\alpha\beta}$, quae per $2p+1$ diuiſa certe vnitatem relinquit. Ex quo ſequitur, etiam poteſtatem a^β vnitatem relinquere, ſiue formulam $a^\beta - 1$ eſſe diuiſibilem.

Corollarium.

§. 37. Cum reſidua 1; α; β; γ; δ; etc. minora eſſe ſoleant quam diuiſor $2p+1$; iis adhuc annumerari licet $1+(2p+1)$; $\alpha+(2p+1)$; $\beta+(2p+1)$; etc. quod obſeruandum eſt, ſi numerus a maior fuerit diuiſore $2p+1$.

Scholion.

§. 38. Cum igitur in hoc negotio maximi ſit momenti, tam reſidua, quam non reſidua noſſe, pro diuiſoribus primis minoribus; ſequentem tabulam hic adiiciamus: ſuperfluum autem foret, non-reſidua adpoſuiſſe.

Diuiſor.	Reſidua.
3.	1, 4, 7, 10, 13, 16, 19, 22, 25, etc.
5.	1, 4, 6, 9, 11, 14, 16, 19, 21, 24, etc.
7.	1, 2, 4, 8, 9, 11, 15, 16, 18, 22, etc.
11.	1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23, etc.
13.	1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27, etc.
17.	1, 2, 4, 8, 9, 13, 15, 16, 18, 19, 21, 25, 26, 30 etc.
19.	1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26, etc.
23.	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 24, 25, 26, 27, etc.

Diui-

Diuiſor.	Reſidua.
29.	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28, etc.
31.	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 etc.
37.	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36, etc.

etc.

Ope huius tabulae ſequentia theoremata particularia facillime deriuabimus.

Theorema 8.

§. 39. Sumto $a = 11$, ſi fuerit $2p+1$ numerus primus, vtrum per eum diuiſibilis ſit formula $11^p - 1$, ſiue $11^p + 1$, ſequens tabella oſtendit.

Si fuerit $2p+1$	Diuiſibilis erit
$44.n \pm 1$	$11^p - 1$
$44.n \pm 3$	$11^p + 1$
$44.n \pm 5$	$11^p - 1$
$44.n \pm 7$	$11^p - 1$
$44.n \pm 9$	$11^p - 1$
$44.n \pm 13$	$11^p + 1$
$44.n \pm 15$	$11^p + 1$
$44.n \pm 17$	$11^p + 1$
$44.n \pm 19$	$11^p - 1$
$44.n \pm 21$	$11^p + 1$

Theorema 9.

§. 40. Sumto $a = 12$, si fuerit $2p + 1$ numerus primus, vtrum per eum diuisibilis sit siue forma $12^p + 1$, siue $12^p - 1$, ex sequenti tabella patet:

Si fuerit $2p+1$	Diuisibilis erit
$48.n \pm 1$	$12^p - 1$
$48.n \pm 5$	$12^p + 1$
$48.n \pm 7$	$12^p + 1$
$48.n \pm 11$	$12^p - 1$
$48.n \pm 13$	$12^p - 1$
$48.n \pm 17$	$12^p + 1$
$48.n \pm 19$	$12^p + 1$
$48.n \pm 23$	$12^p - 1$

Theorema 10.

§. 41. Sumto a successiue $= 13, 14, 15$, si fuerit $2p + 1$ numerus primus, vtrum per eum diuisibilis sit siue forma $a^p + 1$, siue $a^p - 1$, ex sequentibus tabellis patet.

$a = 13$.

$2p$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$
$52.n$

$a = 13$		$a = 14$		$a = 15$	
$2p+1$		$2p+1$		$2p+1$	
$52.n \pm 1$	$13^p - 1$	$56.n \pm 1$	$14^p - 1$	$60.n \pm 1$	$15^p - 1$
$52.n \pm 3$	$13^p - 1$	$56.n \pm 3$	$14^p + 1$	$60.n \pm 7$	$15^p - 1$
$52.n \pm 5$	$13^p + 1$	$56.n \pm 5$	$14^p - 1$	$60.n \pm 11$	$15^p - 1$
$52.n \pm 7$	$13^p + 1$	$56.n \pm 9$	$14^p - 1$	$60.n \pm 13$	$15^p + 1$
$52.n \pm 9$	$13^p - 1$	$56.n \pm 11$	$14^p - 1$	$60.n \pm 17$	$15^p - 1$
$52.n \pm 11$	$13^p + 1$	$56.n \pm 13$	$14^p - 1$	$60.n \pm 19$	$15^p + 1$
$52.n \pm 15$	$13^p + 1$	$56.n \pm 15$	$14^p + 1$	$60.n \pm 23$	$15^p + 1$
$52.n \pm 17$	$13^p - 1$	$56.n \pm 17$	$14^p + 1$	$60.n \pm 29$	$15^p + 1$
$52.n \pm 19$	$13^p + 1$	$56.n \pm 19$	$14^p + 1$		
$52.n \pm 21$	$13^p + 1$	$56.n \pm 23$	$14^p + 1$		
$52.n \pm 23$	$13^p - 1$	$56.n \pm 25$	$14^p - 1$		
$52.n \pm 25$	$13^p - 1$	$56.n \pm 27$	$14^p + 1$		

ADDITAMENTVM.

Quae hactenus sunt tradita, plerumque adhuc firmis demonstrationibus destituuntur; omnia autem dubia maximam partem diluentur sequentibus propositionibus, quibus simul omnia ad multo maiorem euidentiae gradum euehentur.

Theorema 1.

§. 1. *Si formula* $4p+(2q+1)^2$ *fuerit numerus primus, per eumque omnia quadrata diuidantur, inter residua occurret tam* $+p$ *quam* $-p$.

Demonstratio.

In his residuis primo occurrunt omnia quadrata, quatenus sunt ipso diuisore, quem littera D designemus, minora; praeterea vero ex quadratis maioribus, veluti Q^2, nascuntur residua Q^2-D, vel $Q^2-\lambda D$. Quin etiam notum est, ad residua referri posse omnes formulas $Q^2\mp\lambda D$. Capiatur igitur $Q^2=(2q+1)^2$, et ob $D=4p+(2q+1)^2$, residuum prodit $-4p$; ergo etiam inter residua erit $-p$, quia generatim, si inter residua fuerit $\alpha^2\beta$, tum ibidem quoque semper β reperitur. Porro quoniam hic diuisor $4p+(2q+1)^2$ in forma $4n+1$ continetur, iam demonstratum est, singula residua vtroque signo $+$ et $-$ adfecta reperiri; vnde manifestum est, nostro casu tam $+p$ quam $-p$ inter residua reperiri debere.

Corol-

§. 2
buntur ferr
propositum

§. 3
$xx-pyy$,
formulis co
sub iisdem

§. 4
omnium rel
omnes ad n
formulam p^n
$2m+1$ si
testates ipsi
tantum est
tatem, seu 1
diuisorem 2

§. 5
primus, per
semper occur
eodem redit
referetur.

mis de-
aximam
is simul
entur.

numerus
r residua

uadrata,
gnemus,
eluti Q^2,
tiam no-
$^2+\lambda D$.
$2q+1)^2$,
erit $-p$,
ibidem
: diuisor
iam de-
et $-$ ad-
tam $+p$

Corol-

Corollarium 1.

§. 2. Quia tam $+p$ quam $-p$ est residuum, dabuntur formulae tam $xx+pyy$ quam $xx-pyy$ per propositum diuisorem D diuisibiles.

Corollarium 2.

§. 3. Cum autem hae formae: $xx+pyy$ et $xx-pyy$, alios non admittant diuisores, nisi qui in certis formulis contineantur, necesse est, vt etiam numerus p sub iisdem formulis comprehendatur.

Corollarium 3.

§. 4. Quia, posito diuisore $=2m+1$, numerus omnium residuorum tantum est $=m$, dum reliqui numeri omnes ad non-residua sint referendi; hinc sequitur, etiam formulam p^m-1 diuisibilem fore per $2m+1$, dummodo $2m+1$ fuerit numerus primus. Quia enim omnes potestates ipsius p quoque sunt residua, horumque numerus tantum est m, necesse est, vt potestas p^m iterum ad vnitatem, seu p^0 reducatur, hincque p^m-1 diuidi poterit per diuisorem $2m+1$.

Theorema 2.

§. 5. *Si formula* $4p-(2q+1)^2$ *fuerit numerus primus, per eumque omnia quadrata diuidantur, in residuis semper occurret numerus* p; *at eius negatiuum* $-p$, *siue quod eodem redit* $D-p$, *denotante* D *diuisorem, ad non-residuo referetur.*

Demonſtratio.

Praeter ipſa quadrata, diuiſore minora, etiam inter reſidua occurret quadratum $(2q+1)^2$, diuiſore auctum, ideoque $4p$; ergo etiam, ob rationem ante allegatam, occurret numerus p. Et quia hic diuiſor $4p-(2q+1)^2$ eſt numerus formae $4n-1$, vbi nullum reſiduum vtroque ſigno + et − adfectum occurrit, ſequitur $-p$ inter non-reſidua reperiri debere.

Corollarium 1.

§. 6. Quia ergo p certe eſt reſiduum, dabitur formula $xx-pyy$ per noſtrum diuiſorem diuiſibilis, vnde etiam diuiſor eiusmodi formam habebit, qualem diuiſores formulae $xx-pyy$ poſtulant.

Corollarium 2.

§. 7. At quia $-p$ eſt non-reſiduum, nulla dabitur formula $xx+pyy$ per noſtrum diuiſorem diuiſibilis, vnde etiam diuiſor e formula generali, quae omnes diuiſores ipſius $xx+pyy$ complectitur, excluditur.

Corollarium 3.

§. 8. Ob rationem ante allegatam, ſi diuiſor vocetur $2m+1$, formula p^m-1 per eum diuiſibilis eſſe debet; neque vero haec formula: $(-p)^m-1$ erit diuiſibilis, id quod etiam per ſe eſt perſpicuum. Cum enim diuiſor noſter formam habeat $4n-1$, fiet $m=2n-1$, ideoque numerus impar, et $(-p)^m=-p^m$; quare cum p^m-1 ſit diuiſibile, certe haec formula $-p^m-1$, ſiue p^m+1, non erit diuiſibilis.

Theo-

Theorema 3.

§. 9. *Si $4n+1$ fueris numerus primus, per cumque omnia quadrata diuidantur; inter reſidua omnes occurrent numeri ſiue in hac forma generali: $n-qq-q$, ſiue in hac. $qq+q-n$, contenti.*

Demonſtratio.

Manifeſtum eſt, diuiſorem noſtrum $4n+1$ infinitis modis ad formam $4p+(2q+1)^2$ reduci poſſe. Poſito enim $4n+1=4p+(2q+1)^2$, fiet $n=p+q^2+q$, ideoque $p=n-q^2-q$; vnde ſequitur, quicunque numerus pro q accipiatur, numerum $n-qq-q$ inter reſidua reperiri; deinde quia etiam $-p$ eſt reſiduum (§. 1.), manifeſtum eſt, etiam omnes numeros in hac forma $qq+q-n$ fore reſidua.

Corollarium 1.

§. 10. Hoc ergo modo, dum pro q ſucceſſiue accipiuntur omnes numeri 0, 1, 2, 3, 4, 5, etc. infiniti prodibunt numeri ad reſidua referendi, qui tamen omnes ad multitudinem $2n$ ſe reduci patientur, quandoquidem plura reſidua diuerſa non dantur quam $2n$.

Corollarium 2.

§. 11. Neceſſe igitur eſt, vt omnes numeri, ſiue in forma $n-qq-q$, ſiue in forma $qq+q-n$ contenti, omnia plane praebeant reſidua, diuiſori $4n+1$ conuenientia. Quin etiam ex aliquot huiusmodi reſiduis reliqua ſponte naſcuntur, cum tam poteſtates quoque ſingulorum, quam

quam producta ex binis pluribusue, pariter in reſiduis occurrere debeant; vnde patet, ſi iam prodierint reſidua $\alpha\gamma$ et $\beta\gamma$, tum etiam reſiduum fore $\alpha\beta$. Quia enim productum $\alpha\beta\gamma^2$ eſt reſiduum, omiſſo quadrato γ^2 etiam $\alpha\beta$ erit reſiduum.

Corollarium 3.

§. 12. Quodſi ergo compertum fuerit reſiduum $\alpha\beta$, ex alio autem caſu reſiduum prodeat α, etiam alter factor β erit reſiduum.

Scholion.

§. 13. Cum huiusmodi combinationes binorum reſiduorum pluribus, immo infinitis modis inſtitui queant, hinc iam maxime veriſimile videtur, praeter ipſos numeros in formulis $n-qq-q$ et $qq+q-n$ contentos etiam omnes eorum factores primos in reſiduis occurrere, quae coniectura vtrum fundamento certo innitatur nec ne, per ſequentia exempla exploremus. Hunc in finem exponamus numeros in formula $qq+q$ contentos, qui ſunt

0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156,
182, 210, 240, 272, 306, 342, 380, 420, etc.

et quemadmodum reſidua hinc nata littera p deſignamus, ita reſidua prima ſeu ſimplicia littera r indicemus, et quo facilius perſpiciatur, omnes factores numerorum p quoque eſſe reſidua, ipſos numeros p per ſuos factores primos repraeſentemus:

1°. Sit $4n+1=5$; erit $n=1$.
$p=1, 1, 5, 11, 19, 29, 41, 5\cdot 11, 71$, etc.
$r=1, 5, 11, 19, 29, 41, 71$, etc.

vbi

vbi patet, numeri compoſiti p, qui eſt vnicus $5\cdot 11$, ipſos factores quoque eſſe reſidua.

2°. Sit $4n+1=13$; $n=3$.
$p=3, 1, 3, 3^2, 3^3, 3\cdot 13, 53, 3\cdot 23$, etc.
$r=1, 3, 13, 23, 53$, etc.

3°. Sit $4n+1=17$; $n=4$.
$p=2^2, 2, 2, 2^3, 2^4, 2\cdot 13, 2\cdot 19, 2^2\cdot 13, 2^2\cdot 17, 2\cdot 43$ etc.
$r=1, 2, 13, 17, 19\ 43$, etc.

4°. Sit $4n+1=29$; $n=7$.
$p=7, 5, 1, 5, 13, 23, 5\cdot 7, 7^2, 5\cdot 13, 83, 103$, etc.
$r=1, 5, 7, 13, 23, 83, 103$, etc.

5°. Sit $4n+1=37$; $n=9$.
$p=3^2, 7, 3, 3\ 11, 19, 3\cdot 11, 43, 59, 7\cdot 11, 101$, etc.
$r=1, 3, 7, 11, 19, 43, 59, 101$, etc.

6°. Sit $4n+1=41$; $n=10$.
$p=2\cdot 5, 2^3, 2^2, 2, 2\cdot 5, 2^2\cdot 5, 2^2\cdot 2\cdot 23, 2\cdot 31, 2^4\cdot 5, 2^5\cdot 5^2$, etc.
$r=1, 2, 5, 23, 31$, etc.

vbi patet, in numeris p nullos factores primos conſpici, qui non ſimul ſint reſidua.

7°. Sit $4n+1=53$; $n=13$.
$p=13, 11, 7, 1, 7, 17, 29, 43, 59, 7\cdot 11, 97$, etc.
$r=1, 7, 11, 13, 17, 29, 43, 59, 97$, etc.

8°. Sit $4n+1=61$; $n=15$.
$p=3\cdot 5, 13, 3^2, 3, 5, 3\cdot 5, 3^2, 41, 3\cdot 19, 3\cdot 5^2, 5\cdot 19$ etc.
$r=1, 3, 5, 13, 19, 41$, etc.

9°. Sit $4n+1=73$; $n=18$.

$p=2.3^3, 2^4, 2^2.3, 2.3, 2, 2^2.3, 2^3.3, 2.19, 2.3^3, 2^3.3^2, 2^2.23$, etc.
$r=1, 2, 3, 19, 23$, etc.

10°. Sit $4n+1=89$; $n=22$.

$p=2.11, 2^2.5, 2^4, 2.5, 2, 2^3, 2^2.5, 2.17, 2.5^2, 2^2.17, 2^2.11$, etc.
$r=1, 2, 5, 11, 17$, etc.

11°. Sit $4n+1=97$; $n=24$.

$p=2^3.3, 2.11, 2.3^2, 2^2.3, 2^3, 2.3, 2.3^2, 2^2, 2^4.3, 2.3.11, 2.43$, etc.
$r=1, 2, 3, 11, 43$, etc.

12°. Sit $4n+1=111$; $n=25$.

$p=5^2, 23, 19, 13, 5, 5, 17, 31, 47, 5.13, 5.17$, etc.
$r=1, 5, 13, 17, 19, 23, 31, 47$, etc.

13°. Sit $4n+1=109$; $n=27$.

$p=3^3, 5^2, 3.7, 3.5, 7, 3, 3.5, 3.13, 3^2.5, 3^2.7, 83$, etc,
$r=1, 3, 5, 7, 13, 83$, etc.

14°. Sit $4n+1=113$; $n=28$.

$p=2^2.7, 2.13, 2.11, 2^4, 2^3, 2, 2.7, 2^2.7, 2^2.11, 2.31, 2.41$, etc.
$r=1, 2, 7, 11, 13, 31, 41$, etc.

15°. Sit $4n+1=137$; $n=34$.

$p=2.17, 2^5, 2^2.7, 2.11, 2.7, 2^2, 2^3, 2.11, 2.19, 2^3.7, 2^2.19$, etc.
$r=1, 2, 7, 11, 17, 19$, etc.

16°.

8.
.. 19, 2. 3^3,

$p=$
$r=$

2.
17, 2. 5^2,

$p=$

$r=$

t.
3^3, 2^4, $2^2.3$,

$p=$
$r=$

5.
3, 5. 17, etc.

$p=$

$r=$

7.
5, $3^2.7$,

$p=$

$r=$

:.
7, $2^2.11$,

$p=$
$r=$

1, 2. 19,

nullos n
currere,
omnem
ductione

16°.

16°. Sit $4n+1=149$; $n=37$.

$p=37, 5.7, 31, 5^2, 17, 7, 5, 19, 5.7, 53, 73$, etc.
$r=1, 5, 7, 17, 19, 31, 37, 53, 73$, etc.

17°. Sit $4n+1=157$; $n=39$.

$p=3.19, 37, 3.11, 3^2, 19, 3^2, 3, 17, 3.11, 3.17, 71$, etc.
$r=1, 3, 11, 17, 19, 37, 71$, etc.

18°. Sit $4n+1=173$; $n=43$.

$p=41, 37, 31, 23, 13, 1, 13, 29, 47, 67$, etc.
$r=1, 13, 23, 29, 31, 37, 41, 47, 67$, etc.

19°. Sit $4n+1=181$; $n=45$.

$p=3^2.5, 43, 3.13, 3.11, 5^2, 3.5, 3, 11, 2^2, 3^2.5, 5.13$, etc.
$r=1, 2, 3, 5, 11, 13, 43$, etc.

20°. Sit $4n+1=193$; $n=48$.

$p=2^4.3, 2.23, 2.3.7, 2^2.3^2, 2^2.7, 2.3^2, 2.3, 2^5, 2^2.3, 2.3.7, 2.31$, etc.
$r=1, 2, 3, 7, 23, 31$, etc.

21°. Sit $4n+1=197$; $n=49$.

$p=7^2, 47, 43, 37, 29, 19, 7, 7, 23, 41, 61$, etc.
$r=1, 7, 19, 23, 29, 37, 41, 43, 47, 61$, etc.

Scholion.

§. 14. Ex his omnibus exemplis manifeſto liquet, nullos numeros primos ſub littera p tamquam factores occurrere, qui non ſimul ipſi ſint reſidua; quae veritas certe omnem attentionem eo magis meretur, quod ex ſola inductione eſt concluſa, neque etiamnunc firma demonſtra-

tione corroborata; quia tamen in omnibus allatis exemplis tam luculenter se offert, neutiquam desperandum videtur. Qui autem hanc inuestigationem suscipere voluerit, probe perpendat, hanc egregiam proprietatem tum tantum locum habere, quando $4n+1$ est numerus primus; si enim non est primus, plurimi occurrunt casus, quibus hoc secus euenit. Huius generis exemplum est, quo $n=11$; tum enim prodit $p=11$; 3^2; 5; 1; 3^2; 19; 31; 61; 79; 3^2. 11; etc. vnde de numero 8 nihil plane concludere licet, an ad residua pertineat nec ne? Quod autem casibus, quibus $4n+1$ est numerus primus, semper succedat, ratio fortasse in eo est quaerenda, quod pro diuisore $2n+1$ numerus residuorum semper est n, dum contra si $2n+1$ non est primus, numerus residuorum multo est minor; id quod in caussa esse videtur, quod in allato exemplo circa numerum 3 nihil decidatur. Quicquid autem sit, nullum plane dubium supereſſe videtur, quominus sequens stabiliatur.

Conclusio.

§. 15. Quoties numerus $4n+1$ fuerit primus, per eumque omnia quadrata diuidantur, non solum omnes numeri in hac formula: $n-qq-q$, siue etiam hac: $qq+q-n$ contenti, inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sint compositi.

Theorema 4.

§. 16. *Si $4n-1$ fuerit numerus primus et per eum omnia quadrata diuidantur, inter residua omnes occurrent numeri in hac formula: $n+qq+q$, contenti.*

De-

Demonstratio.

Hic etiam clarum est, numerum $4n-1$ infinitis modis sub hac forma: $4p-(2q+1)^2$, repraesentari posse; posito enim $4n-1=4p-(2q+1)^2$, fiet $n=p-q^2-q$, siue $p=n+q^2+q$. Cum ergo $4p-(2q+1)^2$ sit numerus primus, ante demonstratum est, numerum p inter residua reperiri; quocirca etiam omnes numeri in hac formula contenti: $n+qq+q$, inter residua reperientur.

Corollarium 1.

§. 17. Si ergo pro q omnes numeri 0, 1, 2, 3, 4, etc. substituantur, infiniti huiusmodi oriuntur numeri, quos tamen omnes ad multitudinem $2n-1$ deprimere licet, siquidem isti numeri $n+qq+q$ per diuisorem $4n-1$ diuidantur.

Corollarium 2.

§. 18. Necesse ergo est, hoc modo omnia plane prodire residua, quandoquidem etiam tam potestates, quam producta singulorum istorum numerorum inter residua reperiuntur; vnde vt ante sequitur, si iam habeantur duo residua α et $\alpha\beta$, tum etiam β fore residuum; quin etiam si $\alpha\gamma\gamma$ fuerit residuum, ipsum α quoque erit residuum.

Scholion.

§. 19. Cum eiusmodi bina residua infinitis modis combinari possint, maxime verisimilis est suspicio, praeter ipsos numeros, in forma $n+qq+q$ contentos, etiam omnes eorum factores primos in residuis occurrere; quae coniectura vtrum pariter vt ante, certo fundamento nitatur

tur nec ne, per sequentia exempla exploremus. Iam supra autem exposuimus numeros in formula $qq+q$ contentos, vnde pro quolibet numero primo residua simplicia, pariter vt ante, littera r indicemus.

1°. Sit $4n-1=3$; erit $n=1$.

$p=1, 3, 7, 13, 3\cdot 7, 31, 43, 3\cdot 19, 73, 7\cdot 13, 3\cdot 37,$ etc.

$r=1, 3, 7, 13, 19, 31, 37, 43, 73,$ etc.

2°. Sit $4n-1=7$; erit $n=2$.

$p=2, 2^2, 2^3, 2\cdot 7, 2\cdot 11, 2^5, 2^2\cdot 11, 2\cdot 29, 2\cdot 37, 2^2\cdot 23$ $2^4\cdot 7,$ etc.

$r=1, 2, 7, 11, 23, 29, 34, 37,$ etc.

3°. Sit $4n-1=11$; erit $n=3$.

$p=3, 5, 3^2, 3\cdot 5, 23, 3\cdot 11, 3^2\cdot 5, 59, 3\cdot 5^2, 3\cdot 31,$ $113,$ etc.

$r=1, 3, 5, 11, 23, 31, 59, 113,$ etc.

4°. Sit $4n-1=19$; erit $n=5$.

$p=5, 7, 11, 17, 5^2, 5\cdot 7, 47, 61, 7\cdot 11, 5\cdot 19, 5\cdot 23,$ etc.

$r=1, 5, 7, 11, 17, 19, 23, 47, 61,$ etc.

5°. Sit $4n-1=23$; $n=6$.

$p=2\cdot 3, 2^3, 2^2\cdot 3, 2\cdot 3^2, 2\cdot 13, 2^2\cdot 3^2, 2^4\cdot 3, 2\cdot 31,$ $2\cdot 3\cdot 13, 2^5\cdot 3, 2^2\cdot 29,$ etc.

$r=1, 2, 3, 13, 29, 31,$ etc.

6°. Sit $4n-1=31$; erit $n=8$.

$p=2^3, 2\cdot 5, 2\cdot 7, 2^2\cdot 5, 2^3\cdot 7, 2\cdot 19, 2\cdot 5^2, 2^6, 2^4\cdot 5,$ $2\cdot 7^2, 2\cdot 59,$ etc.

$r=1, 2, 5, 7, 19, 59,$ etc.

7°.

7°. Sit $4n-1=43$; erit $n=11$.

$p=11, 13, 17, 23, 31, 41, 53, 67, 83, 101, 11^2,$ etc.

$r=1, 11, 13, 17, 23, 31, 41, 53, 67, 83, 101,$ etc.

8°. Sit $4n-1=47$; $n=12$.

$p=2^2\cdot 3, 2\cdot 7, 2\cdot 3^2, 2^5\cdot 3, 2^3, 2\cdot 3\cdot 7, 2\cdot 3^2, 2^2\cdot 17,$ $2^2\cdot 3\cdot 7, 2\cdot 3\cdot 17, 2\cdot 61,$ etc.

$r=1, 2, 3, 7, 17, 61,$ etc.

9°. Sit $4n-1=59$; $n=15$.

$p=3\cdot 5, 17, 3\cdot 7, 3^2, 5\cdot 7, 3^2\cdot 5, 3\cdot 19, 71, 3\cdot 29,$ etc.

$r=1, 3, 5, 7, 17, 19, 29, 71,$ etc.

10°. Sit $4n-1=67$; $n=17$.

$p=17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127,$ etc.

$r=1, 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127,$ etc.

11°. Sit $4n-1=71$; $n=18$.

$p=2\cdot 3^2, 2^2\cdot 5, 2^2\cdot 3, 2\cdot 3\cdot 5, 2\cdot 19, 2^4\cdot 3, 2^2\cdot 3\cdot 5,$ $2\cdot 37, 2\cdot 3^2\cdot 5, 2^2\cdot 3^2, 2^7, 2\cdot 3\cdot 5^2,$ etc.

$r=1, 2, 3, 5, 19, 37,$ etc.

12°. Sit $4n-1=79$; $n=20$.

$p=2^2\cdot 5, 2\cdot 11, 2\cdot 13, 2^5, 2^3\cdot 5, 2\cdot 5^2, 2\cdot 31, 2^2\cdot 19,$ $2^5\cdot 23, 2\cdot 5\cdot 11,$ etc.

$r=1, 2, 5, 11, 13, 19, 23, 31,$ etc.

13°. Sit $4n-1=83$; $n=21$.

$p=3\cdot 7, 23, 3^3, 3\cdot 11, 41, 3\cdot 17, 3^2\cdot 7, 7\cdot 11, 3\cdot 31,$ $3\cdot 37,$ etc.

$r=1, 3, 7, 11, 17, 23, 31, 37, 41,$ etc.

14°.

14°. Sit $4n-1=103$; $n=26$.

$p=2.13, 2^2.7, 2^5, 2.19, 2.23, 2^3.7, 2^2.17, 2.41, 2.7^2, 2^2.29$, etc.

$r=1, 2, 7, 13, 17, 19, 23, 29, 41$, etc.

Scholion.

§. 20. Ex his exemplis iterum abunde patet, omnes plane numeros primos in numeris p contentos ipsos quoque esse residua. Euidens autem est, vt primum hoc de minoribus numeris fuerit certum, de maioribus nullum amplius dubium relinqui; at vero in numeros p binarius non ingreditur, nisi iam fuerit in ipso numero primo n; ternarius autem, nisi in duobus primis insit, ex tota serie p excluditur. Eodem modo patet, quinarium, nisi in tribus primis insit, quoque excludi; septenarius autem penitus excluditur, nisi in quatuor primis iam occurrat, et sic de reliquis. Vnde patet, in continuatione vlteriori istius seriei nullos numeros primos minores ingredi posse, qui non iam ante fuerint ingressi; quae obseruatio fortasse ad demonstrationem deducere posset. Verum hic iterum probe notetur, hanc insignem proprietatem tantum locum habere, quoties $4n-1$ fuerit numerus primus; si enim esset compositus, tum vtique eiusmodi numeri primi occurrere possunt, de quibus neutiquam liquet, vtrum in ordinem r sint referendi. Veluti si fuerit $n=30=2.3.5$; tum numeri pro p ita se habebunt:

$p=2.3.5, 2^5, 2^2.3^2, 2.3.7, 2.5^2, 2^2.3.5, 2^3.3^2, 2.43, 2.3.17, 2^2.3.5, 2^2.5.7, 2.9^2$, etc.

Hic

17, 2. 41,

Hic qui
rendu
3
Hinc aut
siue 7 i
non-resi
producun
non est

nde patet,
ntentos ip-
vt primum
maioribus
numeros p
ipso numero
is insit, ex
narium, nisi
rius autem
occurrat, et
lteriori isti-
gredi posse,
atio fortasse
hic iterum
tum locum
s; si enim
primi oc-
rum in or-
$=2.3.5$;

§.
eumque
meri in
runt ipsi,
bus illi si

§.
formula
vel $4as$
tur, tum

C
ille primi
$+4at-$
hoc vero
rem habe
residuis e

, $2^2.3^2$,
$.9^2$, etc.

Hic

Euleri

Hic quidem statim adparet, binarium ad residua esse referendum; quo sublato iudicium redit ad sequentes numeros:

$3.5, 3^2, 3.7, 5^2, 43, 3.17, 5.7, 3^4$, etc.

Hinc autem nullo modo concludi potest, siue 3, siue 5, siue 7 in residuis reperiri; et fieri posset, vt singuli essent non-residua; quandoquidem producta ex binis non-residuis producunt residua; verum etiam hinc numerus $4n-1=319$ non est primus. De primis autem certa videtur haec

Conclusio.

§. 21. Quoties numerus $4n-1$ fuerit primus per eumque diuidantur omnia quadrata; non solum omnes numeri in forma $n+qq+q$ contenti inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sunt compositi.

Theorema generale.

§. 22. *Denotante T numerum quemcunque in hac formula $(2q+1)^2-4at$ contentum, si fuerit vel $4as+T$, vel $4as-T$ numerus primus, per eumque quadrata diuidantur, tum in residuis semper reperietur numerus a.*

Demonstratio.

Cum enim sit $T=(2q+1)^2-4at$; numerus ille primus erit vel $4as-4at+(2q+1)^2$, vel $4as+4at-(2q+1)^2$. Illo casu habebimus $p=a(s-t)$; hoc vero $p=a(s+t)$, sicque in vtroque casu p factorem habet a, qui ergo per praecedentes conclusiones in residuis ex quadratis ortis occurret.

Corollarium 1.

§. 23. Hoc ergo modo numeri T ex quadratis $(2q+1)^2$ formati infra $4a$ deprimi poterunt; ſicque multitudo horum valorum ad numerum determinatum reducetur, etiamſi numeri $(2q+1)^2$ in infinitum progrediantur. Inuentis autem omnibus ipſius T valoribus ipſo $4a$ minoribus, ſi illis continuo addantur multipla ipſius $4a$, hos valores in infinitum continuare licebit.

Corollarium 2.

§. 24. Quia numerus a inter reſidua quadratorum occurrit, ſemper dabitur formula $xx-ayy$ per numerum illum primum diuiſibilis, ſiue is ſit $4as+T$; ſiue $4as-T$; ac ſi iſte numerus primus vocetur $2m+1$, tum formula a^m-1 diuiſorem habebit $2m+1$.

Scholion.

§. 25. Quot autem valores diuerſos littera T infra $4a$ ſortiatur, id pendet ab indole numeri a, ſiue is fuerit primus ſiue compoſitus; atque hoc diſcrimen probe eſt notandum, cum vlterior euolutio harum formularum pro caſibus, quibus a eſt numerus compoſitus, commode expediri nequeat, niſi caſus, quibus a eſt numerus primus, ante fuerint explorati.

Theorema.

§. 26. *Si* a *fuerit numerus primus, puta* $2\alpha+1$, *tum numerus valorum litterae* T *ipſo* $4a$ *minorum erit* $=\alpha$, *et totidem numeri formae* $4n+1$ *inde excludentur.*

De-

Demonſtratio.

Omnes valores diuerſi litterae T ipſo $4a$ minorum colliguntur ex quadratis imparibus minoribus quam $a^2=(2\alpha+1)^2$, quae ergo ſunt $1, 9, 25, 49 \ldots (2\alpha-1)^2$, quorum numerus vtique eſt α. Perſpicuum autem eſt, ex quadratis maioribus quam a eosdem prorſus valores ipſius T reſultare, qui ex minoribus prodierunt. Sit enim quadratum quoduis maius $(a+\beta)^2$, hocque comparetur cum quadrato minore $(\alpha-\beta)^2$, et quia eorum differentia $4a\beta$ diuiſibilis eſt per $4a$, vtrinque idem reſiduum oriatur neceſſe eſt Facile autem porro intelligitur, ex omnibus quadratis ipſo a^2 minoribus diuerſa reſidua naſci debere. Quia iam T denotat numeros formae $4n+1$, videamus, quot huiusmodi numeri ab vnitate vsque ad $4a=8\alpha+4$ occurrant. Facile autem patet, eorum numerum fore $=2\alpha+1$, inter quos occurit vnus per a diuiſibilis; quo excluſo multitudo reliquorum eſt $=2\alpha$; quare cum multitudo valorum idoneorum ipſius T ſit $=\alpha$, euidens eſt totidem numeros formae $4n+1$ inde excludi.

Corollarium 1.

§. 27. Quia omnes valores litterae T in forma $4n+1$ continentur, ſi omnes numeri huius formae ab vnitate vsque ad $4a$ ſcribantur, eorum ſemiſſis tantum praebet veros valores litterae T, reliqui vero omnes inde excluduntur. Vtamur autem littera Θ ad huiusmodi numeros excluſos denotandos.

Corollarium 2.

§. 28. Cum ergo omnes numeri formae $4n+1$, qui ſunt:

1, 5, 9, 13, 17, 21, 25, 29, 33, etc.

pro quouis casu numeri a siue ad ordinem terminorum $T = (2q+1)^2 - 4at$, siue ad ordinem excluſorum Θ referantur, operae pretium erit, ambos iſtos ordines, pro minoribus ſaltem ipſius a valoribus, qui quidem ſint primi, exhibere; atque vtile erit, non ſolum primam periodum horum numerorum ipſo $4a$ minorum, ſed etiam ſequentes periodos, addendo continuo $4a$, ob oculos exponere:

1°. Sit $a = 2$; erit $4a = 8$.

$T = 1 \mid 9 \mid 17 \mid 25 \mid 33 \mid$ etc.
$\Theta = 5 \mid 13 \mid 21 \mid 29 \mid 37 \mid$

2°. Sit $a = 3$; erit $4a = 12$.

$T = 1 \mid 13 \mid 25 \mid 37 \mid 49 \mid 61 \mid$ etc.
$\Theta = 5 \mid 17 \mid 29 \mid 41 \mid 53 \mid 65 \mid$

Quia hic a erat 3, quadrata per 3 diuiſibilia excludi debebant:

3°. Sit $a = 5$, erit $4a = 20$.

$T = 1, 9 \mid 21, 29 \mid 41, 49 \mid 61, 69 \mid 81, 89 \mid$ etc.
$\Theta = 13, 17 \mid 33, 37 \mid 53, 57 \mid 73, 77 \mid 93, 97 \mid$

Hic ſcilicet ex ordine Θ excluſimus numerum 5, vtpote ipſi a aequalem.

4°. Sit $a = 7$; erit $4a = 28$.

$T = 1, 9, 25 \mid 29, 37, 53 \mid 57, 65, 81 \mid$ etc.
$\Theta = 1, 13, 17 \mid 33, 41, 45 \mid 61, 69, 73 \mid$

Hic in ordine Θ omiſimus numerum 21, vtpote per $a = 7$ diuiſibilem.

5°.

minorum
orum Θ
nes, pro
ſint pri-
m perio-
etiam ſe-
ulos ex-

ludi de-

etc.

, vtpote

per $a = 7$

5°.

5°. Sit $a = 11$; $4a = 44$.

$T = 1, 5, 9, 25, 37 \mid 45, 49, 53, 69, 81 \mid$ etc.
$\Theta = 13, 17, 21, 29, 41 \mid 57, 61, 65, 73, 85 \mid$

$89, 93, 97, 113, 125 \mid$ etc.
$101, 105, 109, 117, 129 \mid$

6°. Sit $a = 13$; $4a = 52$.

$T = 1, 9, 17, 25, 29, 49, 53, 61, 69, 77, 81, 101,$ etc.

$\Theta = 5, 21, 33, 37, 41, 45, 57, 73, 85, 89, 93, 97,$ etc.

7°. Sit $a = 17$; $4a = 68$.

$T = 1, 9, 13, 21, 25, 33, 49, 53,$ etc.
$\Theta = 5, 29, 37, 41, 45, 57, 61, 65,$ etc.

8°. Sit $a = 19$; $4a = 76$.

$T = 1, 5, 9, 17, 25, 45, 49, 61, 73, 77, 81, 85, 93,$
$101, 121, 125, 137, 149,$ etc.

$\Theta = 13, 21, 29, 33, 37, 41, 53, 65, 69, 89, 97, 105,$
$109, 113, 117, 129, 141, 145,$ etc.

9°. Sit $a = 23$; $4a = 92$.

$T = 1, 9, 13, 25, 29, 41, 49, 73, 77, 81, 85,$ etc.
$\Theta = 5, 17, 21, 33, 37, 45, 53, 57, 61, 65, 89,$ etc.

10°. Sit $a = 29$; $4a = 116$.

$T = 1, 5, 9, 13, 25, 33, 45, 49, 53, 57, 65, 81, 93,$
$109,$ etc.

$\Theta = 17, 21, 37, 41, 61, 69, 73, 77, 85, 89, 97, 101,$
$105, 113,$ etc.

Scholion.

§. 29. Hinc ergo pro iſtis numeris primis a innoteſcunt tam valores litterae T, quam litterae Θ, quos ita intelligere decet, vt quoties formula $4as + T$, vel $4as - T$ fuerit numerus primus, puta $2m+1$, tum ſemper exhiberi poſſit formula $xx - ayy$ per $2m+1$ diuiſibilis; tum vero etiam ſemper formula $a^m - 1$ eundem habebit diuiſorem $2m+1$, ita vt iam plura theoremata ſupra allata, ſcilicet quoties a fuerit numerus primus, ita ſuccincte poſſimus enuntiare, vt, quoties fuerit $4as \mp T$ numerus primus $= 2m+1$, tum ſemper formula $a^m - 1$ eundem admittat diuiſorem; quo obſeruato nullum amplius dubium ſupererit, quin numeri ſub ordine Θ comprehenſi contraria gaudeant proprietate, quam iam ita enuntiare licebit, vt, quoties formula $4as \mp \Theta$ fuerit numerus primus $= 2m+1$; tum non amplius formula $a^m - 1$ per eum ſit diuiſibilis; vnde cum formula $a^{2m} - 1$ ſemper ſit diuiſibilis, ſequitur hoc caſu ſemper formulam $a^m + 1$ per numerum primum $2m+1$ fore diuiſibilem. Atque haec duo enuntiata omnes caſus ſupra allatos exhauriunt, quibus numerus a erat primus; quando autem a habet factores, res ſecus ſe habet, hosque caſus peculiari modo tractari conueniet.

Problema.

§. 30. Si numerus a fuerit compoſitus, puta $a = fg$, inuenire numeros vtriusque indolis per litteras T et Θ deſignatos.

So

Solutio.

Hic igitur quaeruntur omnes diuiſores primi $2m+1$ ſub formula $4fgs \mp T$ contenti, per quos formula $(fg)^m - 1$ ſit diuiſibilis; id quod duplici modo fieri poteſt, vel quando hae duae formulae: $f^m - 1$ et $g^m - 1$ per $2m+1$ ſunt diuiſibiles, vel etiam hae duae formulae: $f^m + 1$ et $g^m + 1$. Priore enim caſu, cum ſit

$$(fg)^m - 1 = g^m (f^m - 1) + g^m - 1,$$

vtique haec formula per $2m+1$ diuidi poterit. Iam pro numeris primis f et g diuiſores primi hoc praeſtantes ſupra ſunt inuenti, quos diſtinctionis gratia ita repraeſentemus:

$$4f.gs \mp T^{(f)}; \text{ et } 4g.fs \mp T^{(g)};$$

quae duae formulae in vnam coaleſcent, ſi ex valoribus ſupra datis litterarum $T^{(f)}$ et $T^{(g)}$ eos excerpamus, qui vtrique ſunt communes. Hi enim ſi littera T comprehendantur, vtique omnes numeri primi huius formae $4fgs \mp T$ quaeſito ſatisfacient. Poſteriore autem caſu, quo formulae $f^m + 1$ et $g^m + 1$ diuiſorem habent $2m+1$, quia eſt

$$(fg)^m - 1 = f^m (g^m + 1) - f^m - 1;$$

huic formulae idem diuiſor conueniet. Pro hoc autem caſu ſupra vidimus, formam diuiſorum primorum eſſe

$$4f.gs \mp \Theta^{(f)} \text{ et } 4g.fs \mp \Theta^{(g)};$$

quare ſi ex valoribus litterae Θ pro numeris f et g ii, qui ipſis ſunt communes, excerpantur, eos nunc etiam valoribus litterae T accenſeri oportet; ſicque omnes valores quaeſiti litterae T obtinebuntur, ſi tam numeri formulis $T^{(f)}$ et $T^{(g)}$ communes, quam etiam ii, quos formulae

mulae $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent, coniungantur, atque vsque ad terminum $4fg = 4a$ producantur; quem in finem iam supra valores harum litterarum vltra primam periodum continuauimus. His autem inuentis reliqui numeri formae $4n+1$ hinc excluſi valores dabunt litterae Θ, quos etiam ita colligere licet, vt eo referantur tam termini litteris $T^{(f)}$ et $\Theta^{(g)}$, quam litteris $T^{(g)}$ et $\Theta^{(f)}$ communes.

Exemplum.

§. 31. Quia haec operatio facillime exemplo illuſtrabitur, ſit $a = 15$, ideoque $f = 3$, et $g = 5$, pro quo vtroque numero ex ſupra allatis depromantur valores litterarum T et Θ. Inde igitur habebimus:

Pro $f = 3$: $T^{(f)} = 1, 13, 25, 37, 49, 61.$ $\Theta^{(f)} = 5, 17, 29, 41, 53, 65.$

Pro $g = 5$: $T^{(g)} = 1, 9, 21, 29, 41, 49, 61, 69.$ $\Theta^{(g)} = 13, 17, 33, 37, 53, 57, 73, 77.$

quos valores vltra terminum $4a = 4fg = 60$ continuauimus.

Iam litterae $T^{(f)}$ et $T^{(g)}$ ſequentes habent terminos communes: 1, 49, 61, litterae autem $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent iſtos terminos 17, 53, qui numeri coniunctim praebent valores litterae T pro iſto caſu. At pro littera Θ capiantur primo termini communes ex litteris $T^{(f)}$ et $\Theta^{(g)}$, qui ſunt 13, 37; tum vero etiam numeri litteris $T^{(g)}$ et $\Theta^{(f)}$ communes, qui ſunt 29, 41. Conſequenter pro caſu propoſito $a = 15$ valores litterarum T et Θ per primam periodum, vsque ad $4a = 60$ continuati, erunt:

T =

antur, at-
u.; quem
vltra pri-
itis rel.qui
abunt lit-
referantur
s $T^{(g)}$ et

§
telligatur
dit, quo
rant nun
N fuerit
quorum
primos;
tus, ſemp
N
vbi a, b,
titudo nu
(
Cum nun
tudo nun
=
qui cum
formae 4
numeri 8
ad litteras
uenta ad
ex binis

Hic ſcilic
quidem
dem ſen
gredi.

:emplo il-
pro quo
alores lit-

7.
continua-

terminos
$^{(g)}$ com-
i coniun-
At pro
:x litteris
n numeri
1. Con-
rarum T
50 conti-

T =

T = 1, 17, 49, 53.

Θ = 13, 29, 37, 41.

Hic ſcilicet occurrunt omnes numeri formae $4n+1$, qui quidem ad 15 ſunt primi; et leuiter attendenti patet, totidem ſemper terminos in vtrumque ordinem T et Θ ingredi.

Scholion.

§. 32. Quo haec poſtrema obſeruatio melius intelligatur, regula haud adeo communis notetur, quae oſtendit, quot ab vnitate vsque ad datum numerum N occurrant numeri ad ipſum primi, vbi quidem ſtatim patet, ſi N fuerit ipſe numerus primus, tum omnes praecedentes, quorum multitudo eſt $N-1$, ſimul quoque ad eum eſſe primos; ſin autem N fuerit numerus vtcunque compoſitus, ſemper repraeſentari poterit hac forma generali

$$N = a^{\alpha}.b^{\beta}.c^{\gamma}.d^{\delta}\ldots\ldots$$

vbi a, b, c, etc. denotant numeros primos; tum autem multitudo numerorum ad N primorum ipſoque minorum erit

$$(a-1)a^{\alpha-1}.(b-1)b^{\beta-1}.(c-1)c^{\gamma-1}.\ldots\ldots$$

Cum nunc noſtro caſu ſit $N = 60 = 2^2.3^1.5^1$. erit multitudo numerorum ad N primorum ipſoque minorum

$$= 1.2.2.4. = 16,$$

qui cum omnes ſint impares et tam formae $4n+1$ quam formae $4n-1$, noſtrae formae $4n+1$ tantum aderunt numeri 8, quorum ſemiſſis ad litteram T, reliqui vero ad litteram Θ referuntur. Vtamur ergo hac regula inuenta ad numeros T et Θ pro ſimplicioribus numeris a ex binis factoribus primis conſtantibus euoluendos:

1°. Sit $a = 2.3$; $4a = 24$.

$T = 1, 5 \mid 25, 29 \mid 49, 53 \mid 73, 77,$
$\Theta = 13, 17 \mid 37, 41 \mid 61, 65 \mid 85, 89,$

2°. Sit $n = 2.5$; $4a = 40$.

$T = 1, 9, 13, 37 \mid 41, 49, 53, 77.$
$\Theta = 17, 33, 21, 29 \mid 57, 73, 61, 69.$

3°. Sit $a = 2.7$: $4a = 56$.

$T = 1, 5, 9, 13, 25, 45 \mid 57, 61, 65, 69, 81, 101.$
$\Theta = 17, 29, 33, 37, 41, 53 \mid 73, 85, 89, 93, 97, 109.$

4°. Sit $a = 2.11$; $4a = 88$.

$T = 1, 9, 13, 21, 25, 29, 49, 61, 81, 85.$
$\Theta = 5, 17, 37, 41, 45, 53, 57, 65, 69, 73.$

5°. Sit $a = 2.13$; $4a = 104$.

$T = 1, 5, 9, 17, 21, 25, 37, 45, 49, 81, 85, 93.$
$\Theta = 29, 33, 41, 53\ 57, 61, 69, 73, 77, 89, 97, 101.$

6°. Sit $a = 3.5$; $4a = 60$.

$T = 1, 17, 49, 53.$
$\Theta = 13, 29, 37, 41.$

7°. Sit $a = 3.7$; $4a = 84$.

$T = 1, 5, 17, 25, 37, 41.$
$\Theta = 13, 29, 53, 61, 65, 73.$

Problema.

§. 33. Si a fuerit numerus vtcunque compoſitus, inuenire valores litterarum T et Θ, qui illi conueniunt.

Solu-

Solutio.

Primo notetur, ſi a fuerit quadratum, puta ff, quia pro binis factoribus f et f, tam litterae T, quam Θ inter ſe conueniunt, omnes plane numeri formae $4m+1$, quatenus ſcilicet ad f ſunt primi, ad ordinem T ſunt referendi, ita vt ordo Θ plane vacuus relinquatur, id quod natura rei manifeſto poſtulat. Cum enim ſit $a = ff$, ideoque $a^m = f^{2m}$, ſemper formula $f^{2m} - 1$ diuiſibilis eſt per numerum primum $2m+1$, ſicque forma $a^m + 1$ nunquam hunc diuiſorem admittit. Deinde ſi fuerit $a = ffg$, quoniam pro ff in ordine T omnes numeri occurrunt, in Θ vero nulli, manifeſtum eſt, pro hoc caſu in ordinem T eosdem numeros ingredi, qui pro ſimplici numero g ſunt inuenti; neque vero ex ambobus Θ vllus praeterea accedet, omitti vero debent ii numeri, qui ad ff non ſunt primi. Denique ſi a fuerit productum ex pluribus numeris primis, veluti $a = fgbk$; quaerantur pro factoribus fg et bk numeri ad ordines T et Θ referendi, ex quibus deinceps valores harum litterarum pro ipſo numero f perinde concludentur, vti in problemate praecedente.

Exemplum.

§. 34. Sit $a = 30 = 2.3.5$, ideoque $4a = 120$; ſumantur primo litterae T et Θ pro numero $3.5 = 15$, qui autem vsque ad 120 continuentur, qui ſunt.

pro 3.5 { $T = 1, 17, 49, 53, 61, 77, 109, 113,$
$\Theta = 13, 29, 37, 41, 73, 89, 97, 101.$

Cum his comparentur ambae formae factori 2 reſpondentes atque termini communes vtrique T reperiuntur

1, 17, 49, 113,

ter-

termini autem communes vtriusque litterae Θ sunt

13, 29, 37, 101,

quocirca ordines quaesiti T et Θ pro numero $a = 30$ erunt:

$T = 1, 13, 17, 29, 37, 49, 101, 113$, etc.

$\Theta = 41, 53, 61, 73, 77, 89, 97, 109$, etc.

Scholion.

§. 35. Colligamus iam omnia hactenus inuenta, ac pro omnibus numeris a, exceptis ipsis quadratis, vsque ad 30 formas numerorum primorum $2m \pm 1$ ordine exhibeamus, per quos vel $a^m - 1$ vel $a^m + 1$ fit diuisibilis;

a.	$2m \pm 1$	$a^m \mp 1$.
2.	$8.s \mp 1$	$2^m - 1$.
	$8.s \mp 5$	$2^m + 1$.
3.	$12.s \mp 1$	$3^m - 1$.
	$12.s \mp 5$	$3^m + 1$.
5.	$20.s \mp 1, 9,$	$5^m - 1$.
	$20.s \mp 13, 17,$	$5^m + 1$.
6.	$24.s \mp 1, 5,$	$6^m - 1$.
	$24.s \mp 13, 17,$	$6^m + 1$.
7.	$28.s \mp 1, 9, 25,$	$7^m - 1$.
	$28.s \mp 5, 13, 17,$	$7^m + 1$.
8.	$32.s \mp 1, 9, 17, 25,$	$8^m - 1$.
	$32.s \mp 5, 13, 21, 29,$	$8^m + 1$.

10.

Θ sunt

mero $a = 30$

:c.

:tc.

enus inuenta, ac
ratis, vsque ad
1 ordine exhi-
fit diuisibilis;

	$a^m \mp 1$.
	$2^m - 1$.
	$2^m + 1$.
	$3^m - 1$.
	$3^m + 1$.
	$5^m - 1$.
	$5^m + 1$.
	$6^m - 1$.
	$6^m + 1$.
	$7^m - 1$.
	$7^m + 1$.
	$8^m - 1$.
	$8^m + 1$.

10.

10.	$40.s \mp 1, 9, 13, 37,$	$10^m - 1$.
	$40.s \mp 17, 21, 29, 33,$	$10^m + 1$.
11.	$44.s \mp 1, 5, 9, 25, 37,$	$11^m - 1$.
	$44.s \mp 13, 17, 21, 29, 41,$	$11^m + 1$.
12.	$48.s \mp 1, 13, 25, 37,$	$12^m - 1$.
	$48.s \mp 5, 17, 29, 41,$	$12^m + 1$.
13.	$52.s \mp 1, 9, 17, 25, 29, 49,$	$13^m - 1$.
	$52.s \mp 5, 21, 33, 37, 41, 45,$	$13^m + 1$.
14.	$56.s \mp 1, 9, 13, 25, 45$	$14^m - 1$.
	$56.s \mp 17, 29, 33, 37, 41,$	$14^m + 1$.
15.	$60.s \mp 1, 17, 49, 53,$	$15^m - 1$.
	$60.s \mp 13, 29, 37, 41,$	$15^m + 1$.
17.	$68.s \mp 1, 9, 13, 21, 25, 33, 49, 53,$	$17^m - 1$.
	$68.s \mp 5, 29, 37, 41, 45, 57, 61, 65,$	$17^m + 1$.
18.	$72.s \mp 1, 17, 25, 41, 49, 65,$	$18^m - 1$.
	$72.s \mp 5, 13, 29, 37, 53, 61,$	$18^m + 1$.
19.	$76.s \mp 1, 5, 9, 17, 25, 45, 49, 61, 73,$	$19^m - 1$.
	$76.s \mp 13, 21, 29, 33, 37, 41, 53, 65, 69,$	$19^m + 1$.
20.	$80.s \mp 1, 9, 21, 29, 41, 49, 61, 69,$	$20^m - 1$.
	$80.s \mp 13, 17, 33, 37, 53, 57, 73, 77,$	$20^m + 1$.
21.	$84.s \mp 1, 5, 17, 25, 37, 41,$	$21^m - 1$.
	$84.s \mp 13, 29, 53, 61, 65, 73,$	$21^m + 1$.
22.	$88.s \mp 1, 9, 13, 21, 25, 29, 49, 61, 81, 85,$	$22^m - 1$.
	$88.s \mp 5, 17, 37, 41, 45, 53, 57, 65, 69, 73,$	$22^m + 1$.

23.	92. $s \mp$ 1, 9, 13, 25, 29, 41, 49, 73, 77, 81, 85,	$23^m - 1$.
	92. $s \mp$ 5, 17, 21, 33, 37, 45, 53, 57, 61, 65. 89,	$23^m + 1$.
24.	96. $s +$ 1, 5, 25. 29, 49 53, 73, 77,	$24^m - 1$.
	96. $s \mp$ 13, 17, 37 41, 61, 65, 85, 89,	$24^m + 1$.
26.	104. $s +$ 1, 5, 9, 17, 21, 25, 37, 45, 49, 81, 85, 93,	$26^m - 1$.
	104. $s \mp$ 29, 33, 41, 53, 57, 61, 69, 73, 77, 89, 97. 101,	$26^m + 1$.
27.	108. $s \mp$ 1, 13. 25, 37, 49, 61, 73, 85. 97	$27^m - 1$.
	108. $s \mp$ 5, 17. 29, 41, 53, 65. 77, 89, 101,	$27^m + 1$.
28.	112. $s +$ 1, 9, 25, 29, 37, 53, 57, 65, 81, 93, 109,	$28^m - 1$.
	112 $s \mp$ 5, 13, 17, 33, 41, 45, 61, 69, 73, 89, 97, 101,	$28^m + 1$.
29.	116. $s \mp$ 1, 5, 9, 13, 25. 33, 45, 49, 53, 57, 65, 81, 93, 109,	$29^m - 1$.
	116. $s \mp$ 17, 21, 37, 41, 61. 69, 73, 77, 85, 89, 97, 101, 105, 113,	$29^m + 1$.
30.	120. $s +$ 1, 13, 17. 29, 37, 49, 101, 113,	$30^m - 1$.
	120. $s \mp$ 41, 53, 61, 73, 77, 89, 97, 109,	$30^m + 1$.

Nunc igitur omnia, quae ante fuerant tradita, satis clare perspicere licet atque in hoc genere nihil aliud superesse videtur, quam vt binae illae conclusiones ex obseruationibus deductae firmis demonstrationibus muniantur.

Post-

	77,	$23^m - 1$.
	7, 61,	$23^m + 1$.
		$24^m - 1$.
	9.	$24^m + 1$.
	49, 81.	$26^m - 1$.
	73, 77.	$26^m + 1$.
	5. 97	$27^m - 1$.
	9, 101,	$27^m + 1$.
	, 81,	$28^m - 1$.
	9, 73,	$28^m + 1$.
	53, 57,	$29^m - 1$.
	77, 85,	$29^m + 1$.
	113,	$30^m - 1$.
	, 109,	$30^m + 1$.

dita, satis clare
il aliud superesse
s ex obseruatio-
muniantur.

Post-

Postquam pro quouis numero a, siue primo, siue composito, valores litterarum T et $\odot$ fuerint inuenti, sequentia duo theoremata notari merentur.

I. Omnes diuisores primi formae $xx - ayy$ in alterutra harum formarum: $4as +$ T, vel $4as -$ T continentur.

II. Omnes diuisores primi huius formae: $xx + ayy$ in altervtra harum formularum: $4as +$ T vel $4as - \odot$ continentur.

Sponte autem patet pro x et y eiusmodi numeros sumi debere, vt bina membra xx et ayy nullum habeant diuisorem communem.

Propo-