University of the Pacific
Scholarly Commons

Euler Archive - All Works

Euler Archive

1783

De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus

Leonhard Euler

Follow this and additional works at: https://scholarlycommons.pacific.edu/euler-works

Part of the Mathematics Commons

Record Created:
2018-09-25

Recommended Citation

Euler, Leonhard, "De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus" (1783). *Euler Archive - All Works*. 557.
https://scholarlycommons.pacific.edu/euler-works/557

This Article is brought to you for free and open access by the Euler Archive at Scholarly Commons. It has been accepted for inclusion in Euler Archive - All Works by an authorized administrator of Scholarly Commons. For more information, please contact mgibney@pacific.edu.

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-*

BVS
1; a; li ter- primus, eodem is, sem- isa ite- a^{n+1}; ex ter- monstra- r pote- e. Sae- nae per vsu ve- n sem- inc na- *am pro quo-*

quouis 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 r?* Quae quaestio huc redit, vt exhibeatur minima formula $a^x - r$, 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 $2^{2p} - 1$ 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 for-

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^x, vt formula $f a^x + g$ per datum numerum N fiat diuisibilis. Hanc ergo nouam methodum hic breuiter sum expositurus; hunc 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^{2x};
beat
assign
quide
loco
rit, v
quotu
fiatqu
spectai
quand
muner
principio olim
norum. Simili
nina∫sem, qua
numerum pri-
s binarii, quae-
vocare sum co-
eni, formulam
nc quaestio for-
fima, quae vni-
s quidem, qua
os procedebat;
i 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-
evndem diuisus
resi-

residuum b; tum productum A B 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^x residuum det $= r$, potestas vero a^y 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^x praebeat residuum r, potestas vero a^y residuum s; hinc etiam assignari poterit residuum respondens potestati a^{x-y}, quod quidem foret $= \frac{r}{s}$, 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^x 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.

 Pro-

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 $u \mp \lambda . N = a^\epsilon . v$ etc.; quo pacto quantitas $a^{x-\alpha-\beta-\gamma-\delta-\epsilon}$ per N diuisa residuum relinquet $= v$; haeque operationes eovsque 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 $\alpha + \beta + \gamma + \delta + \epsilon$ 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:

enire mini- datum nu- ssibile. na fa^x per $: -g$. Quia haberi potest aec formula testatem a^α. postremum inquet $= r$. tas $fa^{x-\alpha-\beta}$ it, sumendo $a^\delta . u$; porro operationes siduum $= f$; m det $= f$; fuerit possi- ponente sub- rum $N-1$, n continuen- d talem ca- ia hoc eue- concludemus operationes — g

hin Sin qua asce tam bit, put tum qua deat co cubi qua duce huiu penc paru

$$-g \mp \lambda . N = a^\alpha . r$$
$$r \mp \lambda . N = a^\beta . s$$
$$s \mp \lambda . N = a^\gamma . t$$
$$t \mp \lambda . N = a^\delta . u$$
- - - - - -
- - - - - -
- - - - - -
- - - - - -
$$z \mp \lambda . N = a^\zeta . f$$

hincque deducitur conclusio $x = \alpha + \beta + \gamma + \delta \ldots + \zeta$. Sin autem nunquam perueniatur ad tale residuum f, antequam summa $\alpha + \beta + \gamma + \delta \ldots\ldots$ 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 $f . a^{x-\vartheta}$, ponendo $\vartheta = \alpha + \beta + \gamma$; tum enim eius quadratum t^2 respondebit formulae $f^2 . a^{2x-2\vartheta}$, quae per primam diuidatur, vt formulae $fa^{x-2\vartheta}$ 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 $f^3 a^{3x-3\vartheta}$, quae per quadratum primae diuisa dabit formulae $fa^{x-3\vartheta}$ 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 peruenietur. Inprimis autem hoc compendium maximum vsum praestabit, vbi ad residua satis parua fuerit peruentum; quorum potestates etiam superiores 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-

m reſiduum
§
$2^x - 1$ r
$f = 1$ et
leſcripſimus,
imo quidem
diuiſoribus
luum relin-
1 ſtatuiſſe;
Hic iam ns $= + 1$;
linquat -
primam — 1, ſiqui-
optato; ſ impar, hic
poteſtati
pliciſſima
§. , quae per
ciſſima 2^x ilis fiat per
$a = 2$; e m reſiduum
rocedent:
vbi ergo
la $2^9 - 1$
par, null.
merum N n $+ 1$, ob
go formula
mpar, nulla
§.
mo reſidu
Exem-
Euleri (

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 ſimpliciſſimae per 41 diuiſibiles ſint: $2^{10} + 1$ et $2^{20} - 1$.

Exemplum 3.

§. 12. Pro diuiſore 73 quaeratur formula ſimpliciſſima $2^x \mp 1$ per cum 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 evndem numerum N diuiſibilis.

Exemplum 4.

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

 $+1$

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

Vnde $x=30$; ita vt $2^{30}-1$ fit fimpliciffima forma per 77 diuifibilis. Hinc tamen non fequitur, iftam: $2^{15}+1$ diuifibilem effe per 77, propterea quod 77 non eft numerus primus; etfi enim $2^{30}-1$ diuifibile eft per 77; neutiquam fequitur, altervtrum eius factorum $2^{15}+1$ fiue $2^{15}-1$ diuifibilem effe debere, quemadmodum rite concludere liceret, fi diuifor effet numerus primus; hoc enim cafu fieri poteft, vt alter factor per 7, alter vero per 11 fit diuifibilis; ac reuera, cum 2^5+1 per 11 fit diuifibile, etiam $2^{15}+1$ per 11 erit diuifibile; at vero per 7 diuifibilis eft altera formula $2^{15}-1$, quia factorem habet $2^3-1=7$.

Exemplum 5.

§. 14. Sit diuifor $N=89$, et fumto iterum primo refiduo $=1$, faciemus:

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

Hinc

Hin
bet
Sun
diui
mus
tum
diui
na forma per 77
: $2^{15}+1$ diuifi-
on eft numerus
77; neutiquam
1 fiue $2^{15}-1$
: concludere li-
: enim cafu fieri
per 11 fit diui-
diuifibile, etiam
per 7 diuifibilis
: $2^3-1=7$.
fiet:
nto iterum pri-
Hinc

Hinc ergo $x=11$, ficque formula $2^{11}-1$ diuiforem habet 89; nulla autem datur formula alterius fpeciei $2^{n}+1$.

Exemplum 6.

§. 15. Sit diuifor $N=105$; 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 $2^{12}-1$ diuifibilis erit per 105. At quia 105 non eft numerus primus, non fequitur, fore 2^6+1 per 105 diuifibile. Tantum enim diuidi poteft per 5; dum altera formula 2^6-1 diuifibilis eft per 3. 7.

Exemplum 7.

§. 16. Sit $N=223$. et primum refiduum $=1$, 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

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-15} residuum dat 15. Sumantur quadrata, et potestas 2^{2x-30} residuum dat 225 siue 2; haec iam per primam diuisa praebet pro potestate 2^{x-16} residuum $2 = 2^1 . 1$, ergo potestas 2^{x-17} praebet residuum 1, vnde iam liquet esse $x = 37$.

Exemplum 8.

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

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

vbi iam subsistere possumus. Quia enim residuum est -1, si pro primo residuo sumsissemus -1, vt formula quaeretur $2^x + 1$ 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.

23. Hinc
ullam dari
lice
pof
Sur operatio-
bin vbi resi-
cor vnde haec
ma ata, et po-
test m per pri-
ges 1 2 = 2^1. 1,
iam liquet
dun ium = 1,
7
9
14
17
19
21
23
32
m est − 1,
la quaere-
tia residua
uisset + 1;
n formula
n est, pro
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 $-16 = -2^4 . 1$. ita vt 2^{x-32} conueniat residuum -1. Diuidendo igitur per cubum primae, seu 2^{3x}, cuius residuum itidem est 1, etiam huius potestatis 2^{x-32} residuum erit -1, id quod ante per ambages eruimus.

Exemplum 9.

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

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

ergo

ergo $x = 60$, ita vt formula $2^{60} - 1$ diuisibilis fit 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^{x-14} residuum dans 9; vnde eius quadratum 2^{2x-28} residuum praebet 81; cubus autem 2^{3x-42} praebet residuum 729, siue 344, siue -41; hinc quarta potestas 2^{4x-56} dabit residuum -369, siue $+16 = 2^4 . 1$. ergo per 2^4 diuidendo potestas 2^{4x-60} dat residuum $+1$. et diuidendo per 2^{3x}, cuius residuum etiam est $+1$, potestas 2^{x-60} residuum dabit $+1$, vti modo inuenimus.

Exemplum 10.

§. 22. Sit $N = 311$. fietque:

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

bilis fit per
od diuisoris
5 est diui-
ae $2^3 - 1$;
er has tres
operationes
otestas 2^{x-14}
residuum
duum 729,
dabit re-
diuidendo
lo per 2^{3x},
residuum
3 7 10 15 17 19 21 24 27 29 31 −95

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

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

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

Si substitissemus in 25^{to} 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

126 132 134 137 139 141 143 145 147 155
N fa... diuif... jung... 400 prim... 8 n − ... uenie...
liuisibilis ... aissemus 2^{2x-150}, o 2209, optatum bstitisse- ae cubis iam po- 1; vn-
imo re- xponent. 3 5 7 11 +19
Eu

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

Scholion.

§. 24. Hac igitur methodo pro quolibet diuisore N facile computatur formula simplicissima $2^x \pm 1$ 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 $8n+1$	$2^x \pm 1$	N $8n-1$	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	$2^{15}-1.$
233	$2^{29}+1.$	167	$2^{83}-1.$
241	$2^{12}+1.$	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	$2^{26}+1$
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	$2^{25}+1$	269	$2^{134}+1$

N

Hos
theor
firma
8 n ∓
fin at
bilis
sempe
cesse
per e
nibus
fuerit
mamu
12 n
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 $8n \mp 1$, per eum semper diuisibilis erit formula 2^p-1; sin autem habeat hanc formam: $8n \mp 3$, 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 $12n \mp 1$, per eum semper diuisibilis erit formula 3^p-1.

 Sin

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

si ... um diuisibilis
... erit numerus
... rmula $5^p - 1$,
pri ... fiu ... + 1 numerus
... rmula $6^p - 1$,
pri ... - 1 numerus
... rmula $7^p - 1$,
siue ... 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

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, fi $2p+1$ denotet numerum primum et cafu $p=f$ innotuerit, vtrum formula a^f-1, an a^f+1 diuifibilis fit per $2f+1$; tum generatim eiusdem generis formula, fiue a^p-1, fiue a^p+1 diuifibilis erit per $2p+1$, fi 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 fatis liquet, cafu $f=0$ femper formulam a^p-1 diuifibilem fore per $2p+1=4an\mp1$, quoties fcilicet hic numerus fuerit primus.

Corollarium 2.

§. 34. Sin autem fit $f=1$, prouti fiue $a-1$, fiue $a+1$ per 3 diuidi poteft, fimili cafu generatim fiue for-

form uifibi tinetu vlteri dium inniti denot vtrum $2p+$ fi $2p+1$:rit, vtrum $+1$; tum fiue a^p+1 $\mp(2f+1)$, inde pro- drator α; β; diuerfi inter diuifib rat; ti tem re iusdam x^2-a multip Hinc per 2 ɔus fatis li- fibilem fore ic numerus fiue $a-1$, :neratim fiue for-

formula a^p+1 per numerum primum $2p+1$ erit diuifibilis, quoties $2p+1$ in hac forma: $4an\pm3$ continetur.

Scholion.

§. 35. Theoremata autem particularia allata facile vlterius continuari poffunt, fi fequens problema in fubfidium vocetur, cuius quidem folutio firmiffimis rationibus innititur.

Problema.

§. 36. Quicunque fuerit numerus a, fi $2p+1$ denotet numerum primum, quouis cafu oblato inueftigare, vtrum formula a^p-1, an altera a^p+1 diuifibilis fit per $2p+1$.

Solutio.

Quaerantur omnia refidua, quae ex diuifione quadratorum per numerum $ap+1$ refultant, quae fint 1; α; β; γ; δ; etc. multitudine $=p$, numeri autem ab his diuerfi non-refidua adpellentur. Quo facto fi numerus a inter refidua reperiatur; tum femper formula a^p-1 erit diuifibilis; fin autem numerus a inter non-refidua occurrat; tum altera formula a^p+1 diuifibilis erit. Haec autem regula ita demonftratur: Si fuerit a refiduum ex cuiusdam quadrati x^2 diuifione per $2p+1$ natum; tum erit x^2-a per $2p+1$ diuifibile; fiue aequabitur cuipiam multiplo $m(2p+1)$; ita vt fit $a=x^2-m(2p+1)$. Hinc ergo fiet $a^p=(x^2-m(2p+1))^p$, quae poteftas per $2p+1$ diuifa idem refiduum relinquet ac poteftas (x^2)

$(x^2)^p$; verum haec poteſtas abit in x^{2p}, quae per $2p+1$ diuiſa certe vnitatem relinquit. Ex quo ſequitur, etiam poteſtatem a^p vnitatem relinquere, ſiue formulam $a^p - 1$ 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
$44 \cdot n \pm 1$	$11^p - 1$
$44 \cdot n \pm 3$	$11^p + 1$
$44 \cdot n \pm 5$	$11^p - 1$
$44 \cdot n \pm 7$	$11^p - 1$
$44 \cdot n \pm 9$	$11^p - 1$
$44 \cdot n \pm 13$	$11^p + 1$
$44 \cdot n \pm 15$	$11^p + 1$
$44 \cdot n \pm 17$	$11^p + 1$
$44 \cdot n \pm 19$	$11^p - 1$
$44 \cdot n \pm 21$	$11^p + 1$

 Theo-

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.

$a = 13$.

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

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 eueheutur.

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-

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 refertur.*

De-

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-

que o
rant 1
bac. q
tis mo
ſito e
ideoqu
rus pr
reperir
niſeſtu
fore. re
cipiunt
dibunt
multitu
reſidua
in forn
omnia
entia.
ſponte
ra, etiam inter
iuiſore auctum,
allegatam, oc-
$(2q+1)^2$ eſt
iduum vtroque
$-p$ inter non-
m, dabitur for-
iiſibilis, vnde
ualem diuiſores
n, nulla dabi-
rem diuiſibilis,
omnes diuiſo-
ur.
ſi diuiſor vo-
iiſibilis eſſe de-
erit diuiſibilis,
enim diuiſor
-1, ideoque
im p^m-1 ſit
p^m+1, non
Theo-

Theorema 3.

§. 9. *Si $4n+1$ fuerit numerus primus, per cumque omnia quadrata diuidantur; inter reſidua omnes occurrunt 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 | factoı residuis oc- residua $\alpha\gamma$ nim produ- etiam $\alpha\beta$ r residuum etiam alter ›inorum re- ui queant, ›sos num/ :ntos etiam ere, quae :c ne, per n expona- vbi qui :i sunt 32, 156, c, etc. iesignamus, us, et quo p quoque es primos E :. vbi

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

2°. Sit $4n + 1 = 13$; $n = 3$.

$p = 3, 1, 3, 3^2, 3^2, 3 \cdot 13, 53, 3 \cdot 23$, etc.
$r = 1, 3, 13, 23, 53$, etc.

3°. Sit $4n + 1 = 17$; $n = 4$.

$p = 2^2, 2, 2, 2^2, 2^4, 2 \cdot 13, 2 \cdot 19, 2^2 \cdot 13, 2^2 \cdot 17, 2 \cdot 43$ 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 $4n + 1 = 41$; $n = 10$.

$p = 2 \cdot 5, 2^3, 2^3, 2, 2 \cdot 5, 2^2 \cdot 5, 2^5 \cdot 2 \cdot 23, 2 \cdot 31, 2^4 \cdot 5, 2^5 \cdot 5^2$, 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 $4n+1=73$; $n=18$.

$p = 2.3^2, 2^4, 2^2.3, 2.3, 2, 2^2.3, 2^2.3, 2.19, 2.3^2, 2^2.3^2, 2^2.23$, 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 $4n+1=97$; $n=24$.

$p = 2^2.3, 2.11, 2.3^2, 2^2.3, 2^3, 2.3, 2.3^2, 2^3, 2^4.3, 2.3.11, 2.43$, 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 $4n+1=137$; $n=34$.

$p = 2.17, 2^5, 2^2.7, 2.11, 2.7, 2^3, 2^3, 2.11, 2.19, 2^3.7, 2^2.19$, etc.

$r = 1, 2, 7, 11, 17, 19$, etc.

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 $4n+1=157$; $n=39$.

$p = 3.19, 37, 3.11, 3^3, 19, 3^2, 3, 17, 3.11, 3.17, 71$, 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 $4n+1=181$; $n=45$.

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

$r = 1, 2, 3, 5, 11, 13, 43$, etc.

20°. Sit $4n+1=193$; $n=48$.

$p = 2^4.3, 2.23, 2.3.7, 2^3.3^2, 2^2.7, 2.3^3, 2.3, 2^3, 2^3.3, 2.3.7, 2.31$, 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 demonstratione

tione

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 3 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 ſubhac 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 nita-

tur

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 $n = 1$.

$p = 1, 3, 7, 13, 3.7, 31, 43, 3.19, 73, 7.13, 3.37,$ etc.

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

2°. Sit $4n - 1 = 7$; erit $n = 2$.

$p = 2, 2^2, 2^3, 2.7, 2.11, 2^5, 2^2.11, 2.29, 2.37, 2^2.23, 2^4.7,$ etc.

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

3°. Sit $4n - 1 = 11$; erit $n = 3$.

$p = 3, 5, 3^2, 3.5, 23, 3.11, 3^2.5, 59, 3.5^2, 3.31, 113,$ etc.

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

4°. Sit $4n - 1 = 19$; erit $n = 5$.

$p = 5, 7, 11, 17, 5^2, 5.7, 47, 61, 7.11, 5.19, 5.23,$ etc.

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

5°. Sit $4n - 1 = 23$; $n = 6$.

$p = 2.3, 2^3, 2^2.3, 2.3^2, 2.13, 2^2.3^2, 2^4.3, 2.31, 2.3.13, 2^5.3, 2^2.29,$ etc.

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

6°. Sit $4n - 1 = 31$; erit $n = 8$.

$p = 2^3, 2.5, 2.7, 2^2.5, 2^2.7, 2.19, 2.5^2, 2^6, 2^4.5, 2.7^2, 2.59,$ 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 $4n - 1 = 47$; $n = 12$.

$p = 2^2.3, 2.7, 2.3^2, 2^3.3, 2^5, 2.3.7, 2.3^3, 2^2.17, 2^2.3.7, 2.3.17, 2.61,$ etc.

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

9°. Sit $4n - 1 = 59$; $n = 15$.

$p = 3.5, 17, 3.7, 3^3, 5.7, 3^2.5, 3.19, 71, 3.29,$ 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 $4n - 1 = 71$; $n = 18$.

$p = 2.3^2, 2^2.5, 2^3.3, 2.3.5, 2.19, 2^4.3, 2^2.3.5, 2.37, 2.3^2.5, 2^2.3^3, 2^7, 2.3.5^2,$ etc.

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

12°. Sit $4n - 1 = 79$; $n = 20$.

$p = 2^2.5, 2.11, 2.13, 2^5, 2^3.5, 2.5^2, 2.31, 2^2.19, 2^2.23, 2.5.11,$ etc.

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

13°. Sit $4n - 1 = 83$; $n = 21$.

$p = 3.7, 23, 3^3, 3.11, 41, 3.17, 3^2.7, 7.11, 3.31, 3.37,$ etc.

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

14°.

14°. Sit $4n-1=103$; $n=26$.

$p = 2.13, 2^2.7, 2^5, 2.19, 2.23, 2^2.7, 2^2.17, 2.41, 2.7^2, 2^2.29$, 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:

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

Hic

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 $4n-1=119$ 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.

 Co-

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 $(\alpha+\beta)^2$, hocque comparetur cum quadrato minore $(\alpha-\beta)^2$, et quia eorum differentia $4\alpha\beta$ 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 $=\alpha$, eundens 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,

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

2°. Sit $a = 3$; erit $4a = 12$.

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

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

3°. Sit $a = 5$, erit $4a = 20$.

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

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

4°. Sit $a = 7$; erit $4a = 28$.

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

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	45, 49, 53, 69, 81	etc.
$\Theta =$ 13, 17, 21, 29, 41	57, 61, 65, 73, 85	

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

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 $c = 19$; $4a = 76$.

$T =$ 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.

Scho-

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.

Solutio.

Hic igitur quaeruntur omnes diuisores primi $2m+1$ sub formula $4fgs\mp T$ contenti, per quos formula $(fg)^m-1$ fit 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:

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

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

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 reliqui abunt lit- referantur s $T^{(g)}$ et
Hic scilic quidem dem sen gredi.
§ telligatur dit, quo rant nun N fuerit quorum primos; tus, semp N 7. vbi a, b, titudo nu (Cum nun tudo nun = qui cum formae 4 numeri 8 ad littera uenta ad ex binis
xemplo il- pro quo alores lit- continua- terminos (g) com- i coniun- At pro x litteris n numeri r. Con- rarum T 60 conti- T =
Euleri (

$T = 1, 17, 49, 53.$

$\Theta = 13, 29, 37, 41.$

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

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

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

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

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 $a = fg\,hk$; quaerantur pro factoribus fg et hk 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 $\begin{cases} T = 1, 17, 49, 53, 61, 77, 109, 113, \\ \Theta = 13, 29, 37, 41, 73, 89, 97, 101. \end{cases}$

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 funt

13, 29, 37, 101,

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

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

Θ = 41, 53, 61, 73, 77, 89, 97, 109, etc.

Scholion.

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

a.	$2m+1$	$a^m \mp 1$.
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 funt

mero $a = 30$

c.

tc.

nus inuenta, ac
ratis, vsque ad
1 ordine exhi-
fit diuifibilis;

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

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.	$56\ s \mp 1, 5\ 9, 13, 25, 45$	$14^m - 1$.
	$56.s \mp 17, 29, 33, 37, 41,$	$14^m + 1$.
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.	$88.s \mp 1, 9, 13, 21, 25, 29, 49, 61, 81, 85,$	$22^m - 1$.
	$88.s \mp 5, 17, 37, 41, 45, 53, 57, 65, 69, 73,$	$22^m + 1$.

Oo 3 23.

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, 23m − 1. 7, 61, 23m + 1. 24m − 1. 9. 24m + 1. 49, 81. 26m − 1. 73, 77. 26m + 1. 5, 97 27m − 1. 9, 101, 27m + 1. , 81, 28m − 1. 9, 73, 28m + 1. 53, 57, 29m − 1. 77, 85, 29m + 1. 113, 30m − 1. , 109, 30m + 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 Θ 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 $4as - \Theta$ continentur.

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

Propo-