1751

Theorema circa divisores numerorum in hac forma *paa*±*qbb* contentorum

Leonhard Euler

THEOREMATA
CIRCA DIVISORES NVMERORVM IN HAC FORMA $paa \pm qbb$ CONTENTORVM.

In sequentibus theorematis litterae a et b designant numeros quoscunque integros, primos inter se, seu, qui praeter vnitatem nullum alium habeant diuisorem communem.

Theorema 1.

Numerorum in hac forma $aa + bb$ contentorum diuisores primi omnes sunt vel 2 vel huius formae $4m + 1$ numeri.

Theorema 2.

Omnes numeri primi huius formae $4m + 1$ vicissim in hac numerorum formula $aa + bb$ continentur.

Theorema 3.

Summa ergo duorum quadratorum seu numerus huius formae $aa + bb$ diuidi nequit per vllum numerum huius formae $4m - 1$.

Theorema 4.

Numerorum in hac forma $aa + 2bb$ contentorum diuisores primi omnes sunt vel 2, vel numeri in hac forma $8m + 1$ vel in hac $8m + 3$ contenti.

Theorema 5.

Omnes numeri primi in hac $8m + 1$ vel hac $8m + 3$ forma contenti vicissim sunt numeri huius formae $aa + 2bb$.

Theo-

Theorema 6.

Nullus numerus huius formae $aa+2bb$ dividi poteſt per vllum numerum huius $8m-1$ vel huius $8m-3$ formae.

Theorema 7.

Numerorum in hac forma $aa+3bb$ contentorum diuiſores primi omnes ſunt vel 2 vel 3, vel in vna harum formularum $12m+1$, $12m+7$ contenti.

Theorema 8.

Omnes numeri primi in alterutra harum formularum $12m+1$, vel $12m+7$ ſiue in hac vna $6m+1$ contenti ſimul ſunt numeri huius formae $aa+3bb$.

Theorema 9.

Nullus numerus ſiue huius $12m-1$ ſiue huius $12m-7$ formulae, hoc eſt nullus numerus huius formae $6m-1$ eſt diuiſor vllius numeri in hac forma $aa+3bb$ contenti.

Theorema 10.

Numerorum in hac forma $aa+5bb$ contentorum diuiſores primi omnes ſunt vel 2, vel 5 vel in vna harum 4 formarum $20m+1$, $20m+3$, $20m+7$, $20m+9$ contenti.

Theorema 11.

Si fuerint numeri $20m+1$, $20m+3$, $20m+9$, $20m+7$ primi, tum erit vt ſequitur

$$20m+1=aa+5bb;\quad 2(20m+3)=aa+5bb$$
$$20m+9=aa+5bb;\quad 2(20m+7)=aa+5bb$$

Theo-

Theorema 12.

Nullus numerus in vna sequentium formularum contentus $20m-1$; $20m-3$; $20m-9$; $20m-7$ potest esse divisor vllius numeri huius formae $aa+5bb$.

Theorema 13.

Numerorum in hac forma $aa+7bb$ contentorum diuisores primi omnes sunt vel 2 vel 7 vel in vna sequentium sex formularum | seu in vna harum trium

$28m+1$	$28m+11$	$14m+1$
$28m+9$	$28m+15$	$14m+9$
$28m+25$	$28m+23$	$14m+11$

sunt contenti.

Theorema 14.

Si fuerint numeri in istis formulis $14m+1$, $14m+9$, $14m+11$ contenti primi, tum simul in hac forma $aa+7bb$ continentur.

Theorema 15.

Nullus numerus huius formae $aa+7bb$ potest diuidi per vllum numerum, qui in vna sequentium sex formularum | seu harum trium

$28m+3$,	$28m+5$	$14m+3$
$28m+13$,	$28m+17$	$14m+5$
$28m+19$,	$28m+27$	$14m+13$

contineatur.

Theorema 16.

Numerorum in hac forma $aa+11bb$ contentorum omnes diuiſores primi ſunt vel 2 vel 11 vel continentur in vna ſequentium

10 formularum		ſeu 5 formularum
$44m + 1$	$44m + 3$	$22m + 1$
$44m + 9$	$44m + 27$	$22m + 3$
$44m + 37$	$44m + 23$	$22m + 9$
$44m + 25$	$44m + 31$	$22m + 5$
$44m + 5$	$44m + 15$	$22m + 15$

Theorema 17.

Si fuerint numeri in his ſiue decem ſiue quinque formulis contenti primi, tum ſimul erunt vel ipſi vel eorum quadrupli numeri huius formae $aa + 11bb$.

Theorema 18.

Nullus numerus huius formae $aa + 11bb$ poteſt diuidi per vllum numerum, qui contineatur in vna ſequentium

ſiue 10 formularum		ſiue 5 formularum
$44m + 7$,	$44m + 29$	$22m + 7$
$44m + 13$,	$44m + 35$	$22m + 13$
$44m + 17$,	$44m + 39$	$22m + 17$
$44m + 19$,	$44m + 41$	$22m + 19$
$44m + 21$,	$44m + 43$	$22m + 21$

Theorema 19.

Numerorum in hac forma $aa + 13bb$ contentorum omnes diuiſores primi ſunt vel 2 vel 13, vel continentur in vna ſequentium 12 formularum.

$52m+1$	$52m+7$
$52m+49$	$52m+31$
$52m+9$	$52m+11$
$52m+25$	$52m+19$
$52m+29$	$52m+47$
$52m+17$	$52m+15$

Theorema 20.

Omnes numeri primi, qui in priori formularum istarum columna continentur, simul sunt numeri huius formae $aa+13bb$. Numerorum autem primorum, qui in altera formularum columna continentur, dupla sunt numeri formae $aa+13bb$.

Theorema 21.

Nullus numerus huius formae $aa+13bb$ diuidi potest per vllum numerum, qui contineatur in vna sequentium formularum

$52m+3$	$52m+35$
$52m+5$	$52m+37$
$52m+21$	$52m+41$
$52m+23$	$52m+43$
$52m+27$	$52m+45$
$52m+33$	$52m+51$

Theorema 22.

Numerorum in hac forma $aa+17bb$ contentorum omnes diuisores primi sunt vel 2 vel 17 vel in vna sequentium formularum continentur.

$68m+1$	$68m+3$
$68m+9$	$68m+27$
$68m+13$	$68m+39$
$68m+49$	$68m+11$
$68m+33$	$68m+31$
$68m+25$	$68m+7$
$68m+21$	$68m+63$
$68m+53$	$68m+23$

Theorema 23.

Omnes numeri primi, qui in priori harum formularum columna continentur ad, quos 2 referri debet, sint formae $aa+17bb$ vel ipsi quidem vel eorum noncupla. Numerorum autem primorum in altera columna contentorum tripla sunt numeri formae $aa+17bb$.

Theorema 24.

Nullus numerus huius formae $aa+17bb$ diuidi potest per vllum numerum, qui contineatur in aliqua sequentium formularum

$68m-1$	$68m-3$
$68m-9$	$68m-27$
$68m-13$	$68m-39$
$68m-49$	$68m-11$
$68m-33$	$68m-31$
$68m-25$	$68m-7$
$68m-21$	$68m-63$
$68m-53$	$68m-23$

Theo-

Theorema 25.

Numerorum in hac forma $aa+19bb$ contentorum omnes diuiſores primi ſunt vel 2, vel 19, vel continentur in vna ſequentium

18 formularum		vel harum 9
$76m+1$	$76m+5$	$38m+1$
$76m+25$	$76m+49$	$38m+5$
$76m+17$	$76m+9$	$38m+7$
$76m+45$	$76m+73$	$38m+9$
$76m+61$	$76m+7$	$38m+11$
$76m+35$	$76m+23$	$38m+17$
$76m+39$	$76m+43$	$38m+23$
$76m+63$	$76m+11$	$38m+25$
$76m+55$	$76m+47$	$38m+35$

Theorema 26.

Omnes numeri primi, qui in vna harum formularum continentur, ſunt vel ipſi, vel ſaltem quater ſumti numeri huius formae $aa+19bb$.

Theorema 27.

Nullus numerus huius formae $aa+19bb$ diuidi poteſt per vllum numerum, qui contineatur in aliqua ſequentium 9 formularum

$$38m-1$$
$$38m-5$$
$$38m-7$$
$$39m-9$$
$$38m-11$$

$38m - 17$
$38m - 23$
$38m - 25$
$38m - 35$

His igitur theorematis continetur indoles formularum $aa + qbb$, ſi q fuerit numerus primus, ac primum quidem vidimus omnes diuiſores primos huiusmodi formularum eſſe vel 2 vel q, vel in talibus expreſſionibus $4qm + \alpha$ ita comprehendi poſſe, vt nullus diuiſor in iis non contineatur, tum vero, vt omnis numerus primus $4qm + \alpha$ ſimul ſit diuiſor formulae cuiusdam $aa + qbb$. Deinde etiam hoc colligere licet; ſi numerus primus formae $4qm + \alpha$ fuerit diuiſor cuiusquam numeri $aa + qbb$, tum nullum numerum formae $4qm - \alpha$ diuiſorem eſſe poſſe eiusdem expreſſionis $aa + qbb$. Cum igitur inter formas diuiſorum formulae $aa + qbb$ ſemper contineatur haec $4mq + 1$ manifeſtum eſt, nullum numerum $aa + qbb$ diuidi poſſe per vllum numerum formae $4mq - 1$. Denique attendenti manifeſtum fiet, ſi q fuerit numerus primus formae $4n - 1$, tum diuiſorum formas ad numerum duplo minorem redigi poſſe, ita vt ad formulas $2qm + \alpha$ reuocari queant, quod fieri nequit, ſi q ſit numerus primus formae $4n + 1$. Si igitur pro hac forma $aa + (4n + 1)bb$ diuiſor fuerit $4(4n + 1)m + \alpha$, tum nullus numerus formae iſtius $4(4n + 1)m + 2(4n + 1) + \alpha$ poterit eſſe diuiſor eiusdem expreſſionis $aa + (4n + 1)bb$. Plures annotationes faciemus, cum etiam formulas $aa + qbb$, quando q non eſt numerus primus, fuerimus contemplati.

Theo-

Theorema 28.

Numerorum in hac forma $aa+6bb$, vel hac $2aa+3bb$ contentorum diuisores primi omnes ſunt vel 2 vel 3 vel in vna ſequentium formularum continentur

$$24m+1 \qquad 24m+7$$
$$24m+5 \qquad 24m+11$$

Theorema 29.

Omnes numeri primi formae vel $24m+1$ vel $24m+7$ continentur in expreſſione $aa+6bb$; at numeri primi iſtam formam $24m+5$ et $24m+11$ continentur in expreſſione $2aa+3bb$.

Theorema 30.

Nullus numerus ſiue $aa+6bb$ ſiue $2aa+3bb$ diuidi poteſt per vllum numerum, qui contineatur in aliqua harum formularum

$$24m-1 \qquad 24m-5$$
$$24m-7 \qquad 24m-11$$

Theorema 31.

Numerorum in hac $aa+10bb$ vel hac forma $2aa+5bb$ contentorum diuiſores primi omnes ſunt vel 2 vel 5 vel in vna ſequentium formularum continentur

$$40m+1 \qquad 40m+7$$
$$40m+9 \qquad 40m+23$$
$$40m+11 \qquad 40m+37$$
$$40m+19 \qquad 40m+13$$

Theo-

Theorema 32.

Numeri primi in priori harum formularum columna contenti simul sunt numeri huius formae $aa+10bb$ et numeri primi in altera columna contenti sunt numeri huius formae $2aa+5bb$

Theorema 33.

Nullus numerus siue huius $aa+10bb$, siue huius $2aa+5bb$ formae diuidi potest per vllum numerum, qui in aliqua sequentium formularum contineatur.

$40m-1$	$40m-7$
$40m-9$	$40m-23$
$40m-11$	$40m-37$
$40m-19$	$40m-13$

Theorema 34.

Numerorum in hac $aa+14bb$ vel hac $2aa+7bb$ forma contentorum diuisores primi omnes sunt vel 2 vel 7 vel in vna sequentium formularum continentur

$56m+1$	$56m+3$
$56m+9$	$56m+27$
$56m+25$	$56m+19$
$56m+15$	$56m+5$
$56m+23$	$56m+45$
$56m+39$	$66m+13$

Theorema. 35.

Numeri primi in priori harum formularum columna contenti simul sunt numeri vel huius $aa+14bb$ vel $2aa$

$+7$

$+7bb$ formae, qui autem in altera columna continentur, eorum tripla, demum in altera istarum formularum comprehenduntur.

Theorema 36.

Si in superioribus formulis signa $+$ in $-$ commutentur, tum nullus numerus in istis formulis contentus erit vel formae $aa+14bb$ vel $2aa+7bb$.

Theorema 37.

Numerorum in hac $aa+15bb$ vel hac $3aa+5bb$ forma contentorum diuisores primi omnes sunt vel 2, vel 3 vel 5, vel in vna sequentium formularum continentur.

		vel harum 4
$60m+1$	$60m+31$	$30m+1$
$60m+17$	$60m+47$	$30m+17$
$60m+19$	$60m+49$	$30m+19$
$60m+23$	$60m+53$	$30m+23$

Theorema 38.

Numerorum in hac $aa+21bb$ vel hac $3aa+7bb$ forma contentorum diuisores primi omnes sunt vel 2, vel 3 vel 7, vel in vna sequentium formularum continentur.

$84m+1$,	$84m+5$
$84m+25$,	$84m+41$
$84m+37$,	$84m+17$
$84m+55$,	$84m+11$
$84m+31$,	$84m+23$
$84m+19$,	$84m+71$

Theorema 39.

Numerorum in hac $aa + 35bb$ vel $5aa + 7bb$ forma contentorum diuisores primi omnes sunt vel 2, vel 5 vel 7, vel in vna sequentium formularum continentur.

		vel harum
$140m + 1$,	$140m + 3$	$70m + 1$
$140m + 9$,	$140m + 27$	$70m + 3$
$140m + 81$,	$140m + 103$	$70m + 9$
$140m + 29$,	$140m + 87$	$70m + 11$
$140m + 121$,	$140m + 83$	$70m + 13$
$140m + 109$,	$140m + 47$	$70m + 17$
$140m + 11$,	$140m + 33$	$70m + 27$
$140m + 99$,	$140m + 17$	$70m + 29$
$140m + 51$,	$140m + 13$	$70m + 33$
$140m + 39$,	$140m + 117$	$70m + 39$
$140m + 71$,	$140m + 73$	$70m + 47$
$140m + 79$,	$140m + 97$	$70m + 51$

Theorema 40.

Numerorum in aliqua harum formularum contentorum

$$aa + 30bb;\quad 2aa + 15bb$$

$$3aa + 10bb;\quad 5aa + 6bb$$

diuisores primi omnes sunt vel 2, vel 3, vel 5, vel in vna sequentium formularum continentur.

$120m + 1$;	$120m + 11$
$120m + 13$;	$120m + 23$
$120m + 49$;	$120m + 59$
$120m + 37$;	$120m + 47$

120

$120m + 17$;	$120m + 67$
$120m + 101$;	$120m + 31$
$120m + 113$;	$120m + 43$
$120m + 29$;	$120m + 79$

Theoremata haec sufficiunt ad sequentes annotationes formandas, ex quibus natura diuisorum huiusmodi formularum $paa + qbb$ penitius perspicietur.

Annotatio 1.

Formula $paa + qbb$ nullum habet diuisorem, quin sit simul diuisor formulae $aa + pqbb$. Cuius quidem rei ratio facile patet; nam qui numerus est diuisor formulae $paa + qbb$, idem diuidet hanc formam $ppaa + pqbb$, hoc est hanc $aa + pqbb$, posito a loco pa. Hancobrem sufficiet istam vnicam formam $aa + Nbb$ considerasse, quippe quae ratione diuisorum hanc $paa + qbb$ in se complectitur.

Annotatio 2.

Inter numeros primos, qui vllum numerum in hac formula $aa + Nbb$ contentum diuidunt, primum occurrit binarius. Si enim N sit numerus impar, sumendis pro a et b numeris imparibus, formula $aa + Nbb$ fiet per 2 diuisibilis; at si N sit numerus par, sumto a pari, formula quoque per 2 fit diuisibilis. Deinde vero ipse numerus N vel quaelibet eius pars aliquota poterit esse diuisor formulae $aa + Nbb$, quod sumendo $a = N$ est perspicuum.

Annotatio 3.

Reliqui diuisores primi omnes formulae $aa + Nbb$ in istiusmodi expressionibus $4Nm + \alpha$ comprehendi possunt

 ita,

ita, vt etiam viciſſim omnes numeri primi in formis iſtis $4Nm + \alpha$ contenti ſimul ſint diuiſores formulae $aa + Nbb$. Praeterea ſi expreſſio $4Nm + \alpha$ praebeat diuiſores formulae $aa + Nbb$, tum nullus numerus huiusmodi $4Nm - \alpha$ poterit eſſe diuiſor vllius numeri in formula $aa + Nbb$ contenti.

Annotatio 4.

Habebit autem α certos quosdam valores, qui ab indole numeri N pendebunt; ac ſemper quidem vnitas erit vnus ex valoribus ipſius α. Tum vero, quia de numeris primis in formula $4Nm + \alpha$ contentis quaeſtio eſt, perſpicuum eſt neque vllum numerum parem, neque vllum numerum, qui cum N communem habeat diuiſorem, valorem ipſius α conſtituere poſſe.

Annotatio 5.

Valores autem ipſius α omnes erunt minores quam $4N$, ſi enim qui eſſent maiores, per diminutionem numeri m minores, quam $4N$, reddi poſſent. Hinc valores ipſius α erunt numeri impares minores, quam $4N$, atque ad N primi. Neque vero omnes iſtiusmodi numeri impares ad N primi idoneos pro α valores exhibebunt, ſed eorum ſemiſſis ab hoc officio excluditur, quoniam, ſi x fuerit valor ipſius α, tum $-x$ ſeu $4N - x$ eius valor eſſe nequit; viciſſimque ſi x non fuerit valor ipſius α, tum $4N - x$ certo eius valor ſit futurus.

Annotatio 6.

Numerus igitur valorum ipſius α, ita vt $4Nm + \alpha$ contineat omnes diuiſores primos formulae $aa + Nbb$, ſequenti modo definietur. Sint p, q, r, s, cet. numeri

primi

primi inter se diuersi, excepto binario, qui seorsim est considerandus; atque

si fuerit	erit valorum ipsius α numerus
$N = 1$	1
$N = 2$	2
$N = p$	$p - 1$
$N = 2p$	$2(p - 1)$
$N = pq$	$(p - 1)(q - 1)$
$N = 2pq$	$2(p - 1)(q - 1)$
$N = pqr$	$(p - 1)(q - 1)(r - 1)$
$N = 2pqr$	$2(p - 1)(q - 1)(r - 1)$

etc.

Annotatio 7.

Quemadmodum autem vnitas semper reperitur inter valores ipsius α, ita etiam quiuis numerus quadratus impar et primus ad N locum habere debet in valoribus ipsius α. Posito enim b numero pari $2c$, formula fiet $aa + 4Ncc$, quae, si sit numerus primus, contineri debet in expressione $4Nm + \alpha$. Ergo α erit aa vel residuum, quod ex diuisione ipsius aa per $4N$ remanet. Simili modo inter valores ipsius α reperiri debent omnes numeri $aa + N$, vel quae ex eorum per $4N$ diuisione supererunt residua; posito enim $b = 2c + 1$ fiet $aa + Nbb = aa + N + 4N(cc + c)$, qui, si fuerit numerus primus, debebit $aa + N$ esse valor ipsius α.

Annotatio 8.

Intelligitur etiam, si x fuerit valor ipsius α, tum quoque xx (quod quidem ex praecedente patet) et omnes omnino potestates ipsius x, puta x^{μ} inter valores ipsius α locum habere debere. Deinde, si praeter x quoque y fuerit valor ipsius α, tum quoque xy et generaliter $x^{\mu} y^{\nu}$ dabit quoque valorem ipsius α. Scilicet si $x^{\mu} y^{\nu}$ maius fuerit quam $4N$, per hoc diuidatur et residuum erit valor ipsius α. Simili modo, si insuper z fuerit valor ipsius α, tum etiam $x^{\mu} y^{\nu} z^{\xi}$ erit valor ipsius α. Hincque ex cognito vno vel aliquot valoribus ipsius α facili negotio omnes omnino eius valores inueniuntur.

Annotatio 9.

Sit x quicunque numerus primus ad $4N$, eoque minor, atque vel $+x$ vel $-x$ valor erit ipsius α. Si igitur fuerit x numerus primus, ex sequenti tabula intelligetur, quibus casibus $+x$, quibusque $-x$ valorem ipsius α praebeat

Si	erit
$N = 3n - 1$	$\alpha = +3$
$N = $ [illegible] $n +$ [illegible]	$\alpha = -3$
si	
$N = \begin{cases} 5n+1 \\ 5n+4 \end{cases}$	$\alpha = +5$
$N = \begin{cases} 5n+2 \\ \text{[illegible]} n + \text{[illegible]} \end{cases}$	$\alpha = -5$
$N = \begin{cases} 7n + \text{[illegible]} \\ 7n + \text{[illegible]} \\ 7n+6 \end{cases}$	$\alpha = +7$
$N = \begin{cases} 7n+1 \\ \text{[illegible]} n + \text{[illegible]} \\ \text{[illegible]} n + \text{[illegible]} \end{cases}$	$\alpha = -7$
$N = \begin{cases} \text{[illegible]} n+2 \\ \text{[illegible]} n+6 \\ \text{[illegible]} n+7 \\ 11n+8 \\ 11n+10 \end{cases}$	$\alpha = +11$
$= \begin{cases} 11n+1 \\ \text{[illegible]} n + \text{[illegible]} \\ \text{[illegible]} n + \text{[illegible]} \\ 11n+5 \\ 11n+9 \end{cases}$	$\alpha = -11$

Si propositus sit numerus quicunque primus, qui vtrum signo $+$ an $-$ affectus valorem ipsius α praebeat, ita inuestigabitur. Bini casus debent euolui, alter, quo propositus numerus primus est formae $4u+1$, alter quo est formae $4u-1$. Priori casu erit $\alpha = +(4u+1)$ si fuerit $N = (4u+1)n + tt$, at $\alpha = -(4u+1)$, si fuerit $N = (4u+1)n + tt$. Posteriori casu autem erit $\alpha = +(4u-1)$ si sit $N = (4u-1)n + tt$ at $\alpha = -(4u-1)$ si $N = (4u-1)n + tt$.

Vbi

Vbi notandum est, quemadmodum signum $=$ aequalitatem denotat; ita signum $\neq$ aequalitatis impossibilitatem designare. Quod si autem fuerit pro vtroque casu $N \neq (4u \pm 1)n + s$; erit quoque $N \neq (4u \pm 1)n + s^{\nu}$, denotante ν numerum quemcunque integrum, vnde ista tabella pro quibusuis numeris primis sine negotio construitur.

Annotatio 10.

Quoniam inter formas diuisorum primorum ipsius $aa + Nbb$ habetur $4Nm + 1$, eadem expressio $aa + Nbb$ per nullum numerum diuidi poterit, qui contineatur in hac forma $4Nm - 1$. Simili modo cum $4Nm + tt$ exhibeat formam diuisorum expressionis $aa + Nbb$, sequitur nullum numerum huiusmodi $4Nm - tt$ posse esse diuisorem vllius numeri in hac forma $aa + Nbb$ contenti, si quidem quod semper pono a et b sint numeri inter se primi. Hanc ob rem impossibilis erit ista aequatio $(4Nm - tt)u = aa + Nbb$, ideoque erit $4Nmu - ttu - Nbb \neq aa$, si quidem fuerint $4Nmu - ttu$ et Nbb numeri inter se primi, quod cum certo eueniat, si $b = 1$ et $t = 1$, nanciscimur istud.

Consectarium.

Nullus numerus hac formula $4abc - b - c$ contentus vnquam esse potest quadratus.

Annotatio 11.

Si fuerit N numerus huius formae $4n - 1$, tum formae diuisorum ad numerum duplo minorem rediguntur, ita vt, in formulis huiusmodi $2Nm + \alpha$ comprehendantur. Scilicet si fuerit $4Nm + \alpha$ diuisorum forma, tum quoque

$4Nm + 2N + \alpha$ erit forma diuiſorum. Quare cum $2Nm + tt$ ſit forma diuiſorum, ſequitur nullum numerum $2Nm - tt$ diuiſorem eſſe poſſe formae $aa + Nbb$. Hinc erit $(2Nm - tt)u = aa + Nbb$, exiſtente $N = 4n - 1$, vnde oritur hoc.

Conſectarium.

Nullus numerus huius formae $2abc - b - c$, ſi vel b vel c fuerit numerus impar $4n - 1$, vnquam poteſt eſſe quadratus.

Annotatio 12.

Si fuerit N numerus impar huiusmodi $4n + 1$, vel etiam numerus impariter par, tum diuiſorum formae ad numerum duplo minorem redigi non poſſunt. Scilicet ſi $4Nm + \alpha$ fuerit diuiſor formae $aa + Nbb$ tum $4Nm + 2N + \alpha$ eiusdem formae diuiſor eſſe non poterit. Hinc $2(2m + 1)N + tt$ non erit diuiſor formae $aa - Nbb$, ideoque haec aequatio $(2(2m + 1)N + tt)u = aa + Nbb$ erit aequatio impoſſibilis, ſi quidem ſint a et b numeri primi inter ſe: et N ſit vel numerus impar formae $4n + 1$ vel numerus impariter par. Ex quo ſequitur iſtud

Conſectarium.

Nullus numerus huius formae $2abc - b + c$, exiſtente a numero impari, et b vel impariter pari vel impari formae $4n + 1$, vnquam eſſe poteſt quadratus.

Scholion 1.

Quae hic ſunt allata ſufficienter declarant indolem diuiſorum huiusmodi formularum $aa + Nbb$, ſimulque inſer-

viunt

viunt ad omnes diuiſorum formas expedite inueniendas, quibus cognitis quoque eae numerorum formae innoteſcunt, quae nunquam prebere queant diuiſores formulae $aa+N bb$. Cum igitu haec pateant ad omnes valores ipſius N, ſiue ſint numerir primi, ſiue compoſiti; reliquum eſt, vt etiam caſus euoluamus, quibus N denotet numeros negatiuos tam primos quam compoſitos; perſpicuum autem eſt formulam $paa-qbb$ nullum diuiſorem habere poſſe, quin ſit diuiſor huius $aa-pqbb$ ſeu $pqaa-bb$, vnde ſufficiet huiusmodi tantum formas $aa-Nbb$ euoluiſſe.

Theorema 41.

Numerorum in hac forma $aa-bb$ contentorum diuiſores primi omnes ſunt vel 2 vel $4m+1$, nullus ſcilicet datur numerus, qui non ſit diuiſor differentiae duorum quadratorum. Viciſſim autem omnes numeri, praeter impariter pares, ipſi ſunt differentiae duorum quadratorum.

Theorema 42.

Numerorum in hac forma $aa-2bb$ contentorum omnes diuiſores primi ſunt vel 2 vel huius formae $8m\pm1$. Omnesque numeri primi huius formae $8m\pm1$ ipſi infinitis modis in formula $aa-2bb$ continentur.

Theorema 43.

Numerorum in hac forma contentorum $aa-3bb$ omnes diuiſores primi ſunt vel 2 vel 3 vel huius formae $12m\pm1$. Atque viciſſim omnes huiusmodi numeri primi ſimul in hac $aa-3bb$ vel hac $3aa-bb$ forma infinitis modis continentur.

Theorema 44.

Omnes diuiſores primi huius formae $aa-5bb$ ſunt vel 2 vel 5 vel continentur.

in altera harum formularum	vel in hac vna
$20m \pm 1, \quad 20m \pm 9$	$10m \pm 1.$

Omnesque numeri primi in his formis contenti ſimul ſunt diuiſores formae $aa-5bb$.

Theorema 45.

Omnes diuiſores primi huius formae $aa-7bb$ ſunt vel 2 vel 7 vel in vna ſequentium formularum continentur

$$28m \pm 1;\quad 28m \pm 3;\quad 28m \pm 9$$

atque viciſſim omnes numeri primi in his formis contenti ſimul ſunt diuiſores formae $aa-7bb$.

Theorema 46.

Omnes diuiſores primi huius formae $aa-11bb$ ſunt vel 2 vel 11 vel in vna ſequentium formarum continentur

$$44m \pm 1;\ 44m \pm 5;\ 44m \pm 7;\ 44m \pm 9;\ 44m \pm 19$$

atque viciſſim omnes numeri primi in his formulis contenti ſimul ſunt diuiſores formae $aa-11bb$, quae reciprocatio in omnibus ſequentibus theorematis locum habet.

Theorema 47.

Omnes diuiſores primi formae $aa-13bb$ ſunt vel 2 vel 13 vel in ſequentibus formulis continentur:

		quae reuocantur ad has
$52m \pm 1$;	$52m \pm 3$	$26m \pm 1$
$52m \pm 9$;	$52m \pm 25$	$26m \pm 3$
$52m \pm 23$;	$52m \pm 17$	$26m \pm 9$

Theorema 48.

Omnes diuisores primi numerorum huius formae $aa - 17bb$ sunt vel 2 vel 17, vel in sequentibus formulis continentur:

		quae revocantur ad has
$68m \pm 1$;	$68m \pm 9$	$34m \pm 1$
$68m \pm 13$;	$68m \pm 19$	$34m \pm 9$
$68m \pm 33$;	$68m \pm 25$	$34m \pm 13$
$68m \pm 21$;	$68m \pm 15$	$34m \pm 15$

Theorema 49.

Omnes diuisores primi numerorum huius formae $aa - 19bb$ sunt vel 2 vel 19 vel in sequentibus formulis continentur

$76m \pm 1$;	$76m \pm 3$;	$76m \pm 9$
$76m \pm 27$;	$76m \pm 5$;	$76m \pm 15$
$76m \pm 31$;	$76m \pm 17$;	$76m \pm 25$

Theorema 50.

Omnes diuisores primi numerorum formae huius $aa - 6bb$ sunt vel 2 vel 3 vel in his formulis continentur:

$24m \pm 1$; $24m \pm 5$;

Theorema 51.

Omnes diuisores primi numerorum formae $aa - 10bb$ sunt vel 2 vel 5 vel in his formulis continentur;

$40m \pm 1$; $40m \pm 3$
$40m \pm 9$; $40m \pm 13$

Theorema 52.

Omnes diuisores primi numerorum huius formae $aa - 14bb$ sunt vel 2 vel 7 vel in his formulis continentur:

$56m \pm 1$; $56m \pm 5$; $56m \pm 25$
$56m \pm 13$; $56m \pm 9$; $56m \pm 11$

Theorema 53.

Omnes diuisores primi numerorum huius formae $aa - 22bb$ sunt vel 2 vel 11 vel in his formulis continentur:

$88m \pm 1$; $88m \pm 3$; $88m \pm 9$;
$88m \pm 27$; $88m \pm 7$; $88m \pm 21$;
$88m \pm 25$; $88m \pm 13$; $88m \pm 39$;
$88m \pm 29$.

Theorema 54.

Omnes diuisores primi numerorum huius formae $aa - 15bb$ sunt vel 2 vel 3 vel 5 vel in his formulis continentur:
$60m \pm 1$; $60m \pm 7$; $60m \pm 11$; $60m \pm 17$.

Theorema 55.

Omnes diuisores primi numerorum huius formae $aa - 21bb$ sunt vel 2 vel 3 vel 7 vel in his formis continentur:

		quae reuocantur ad has
$84m \pm 1$;	$84m \pm 5$	$42m \pm 1$
$84m \pm 25$;	$84m \pm 41$	$42m \pm 5$
$84m \pm 37$;	$34m \pm 17$	$42m \pm 17$

Theo-

Theorema 56.

Omnes diuisores primi numerorum huius formae $aa - 33bb$ sunt vel 2 vel 3, vel 11 vel in his formulis continentur:

		quae reuocantur ad has
$132m \pm 1$;	$132m \pm 17$	$66m \pm 1$
$132m \pm 25$;	$132m \pm 29$	$66m \pm 17$
$132m \pm 35$;	$132m \pm 65$	$66m \pm 25$
$132m \pm 49$;	$132m \pm 41$	$66m \pm 29$
$132m \pm 37$;	$132m \pm 31$	$66m \pm 31$

Theorema 57.

Omnes diuisores primi numerorum huius formae $aa - 35bb$ sunt vel 2 vel 5 vel 7 vel in his formulis continentur:

$140m \pm 1$;	$140m \pm 9$;	$140m \pm 59$
$140m \pm 29$;	$140m \pm 19$;	$140m \pm 31$
$140m \pm 13$;	$140m \pm 23$;	$140m \pm 67$
$140m \pm 43$;	$140m \pm 33$;	$140m \pm 17$

Theorema 58.

Omnes diuisores primi numerorum huius formae $aa - 30bb$ sunt vel 2 vel 3 vel 5 vel in his formulis continentur

$120m \pm 1$;	$120m \pm 13$;	$120m \pm 49$
$120m \pm 37$;	$120m \pm 7$;	$120m \pm 29$
$120m \pm 17$;	$120m \pm 19$;	

Theorema 59.

Omnes diuisores primi numerorum huius formae $aa - 105bb$ sunt vel 2 vel 3 vel 5 vel 7 vel continentur in his formulis

		quae reuocantur ad has
$420m \pm 1$;	$420m \pm 13$	$210m \pm 1$
$420m \pm 169$;	$420m \pm 97$	$210m \pm 13$
$420m \pm 23$;	$420m \pm 121$	$210m \pm 23$
$420m \pm 107$;	$420m \pm 131$	$210m \pm 41$
$420m \pm 109$;	$420m \pm 157$	$210m \pm 53$
$420m \pm 59$;	$420m \pm 73$	$210m \pm 59$
$420m \pm 101$;	$420m \pm 53$	$210m \pm 73$
$420m \pm 151$;	$420m \pm 137$	$210m \pm 79$
$420m \pm 89$;	$420m \pm 103$	$210m \pm 89$
$420m \pm 79$;	$420m \pm 187$	$210m \pm 97$
$420m \pm 41$;	$420m \pm 113$	$210m \pm 101$
$420m \pm 209$. ;	$420m \pm 197$	$201m \pm 103$

Annotatio 13.

Numerorum ergo in formula $aa-Nbb$ contentorum diuisores primi omnes sunt vel 2., vel diuisores numeri N vel in eiusmodi formulis $4Nm \pm \alpha$ comprehenduntur. Quodsi enim $4Nm+\alpha$ fuerit forma diuisorum, tum quoque $4Nm-\alpha$ erit diuisorum forma: secus atque in formulis $aa+Nbb$, quarum si $4Nm+\alpha$ fuerit diuisor tum $4Nm-\alpha$ nullum vnquam praebere potest diuisorem eiusdem formulae.

Annotatio 14.

Posita ergo $4Nm \pm \alpha$ pro forma diuisorum generali numerorum in hac expressione $aa-Nbb$ contentorum, littera α plerumque plures significabit numeros; inter quos vnitas semper continetur, tum vero quia hic de diuisoribus primis sermo est inter valores ipsius α nullus erit numerus

merus par nec vllus diuisor numeri N. Deinde etiam manifestum est, omnes valores ipsius α ita ordinari posse, vt fiat minores quam $2N$. Si enim sit $4Nm+2N+b$ diuisor, tum posito $m-1$ loco m, diuisor erit $4Nm-(2N-b)$. Erunt ergo valores ipsius α numeri impares primi ad N, minores quam $2N$, horumque numerorum omnium imparium et primorum ad N et minorum, quam $2N$, semissis tantum praebebit idoneos valores ipsius α, reliqui exhibebunt formulas, in quibus plane nullus continetur diuisor. Perpetuo scilicet totidem habebuntur formulae diuisorum, quot sunt contrariae, solo excepto casu, quo $N=1$.

Annotatio 15.

Quod ad numerum valorum ipsius α pro formula diuisorum $4Nn\pm\alpha$ attinet, quoniam ob signum ambiguum quaeuis formula est duplex, hic quoque eadem valebit regula, quam supra annot. 6. dedi. Sic in vltimo theoremate, quo erat $N=105=3, 5, 7$, numerus valorum ipsius α erit $=2, 4, 6=48$, seu cum quaeuis formula sit gemina, numerus formularum sit 24, quot etiam exhibuimus.

Annotatio 16.

Sicut autem vnitas perpetuo inter valores ipsius α reperitur, ita etiam quiuis numerus quadratus, qui sit primus ad $4N$, valorem idoneum pro α suppeditabit. Posito enim $b=2c$, formula $aa-Nbb$ abit in $aa-4Ncc$ seu $4Ncc-aa$, ex quo patet quemuis numerum quadratum aa, qui sit primus ad $4N$, exhibere valorem idoneum pro α, sumendo scilicet residuo, quod in diuisione ipsius aa per

4 N

4N remanet. Simili modo ponendo $b = 2c + 1$, formula $Nbb - aa$ abit in $4N(cc + c) + N - aa$, vnde etiam omnes numeri $N - aa$ seu $aa - N$, qui quidem sint primi ad $4N$, idoneos valores pro α praebebunt. Deinde quoque notandum est, si sint x, y, z, valores ipsius α, tum quoque x^{μ}, y^{ν}, z^{ξ} itemque omnia producta, quae ex numeris x, y, z eorumue potestatibus quibuscunque resultant, valores ipsius α esse exhibitura; vnde cognito vno vel aliquot valoribus ipsius α facili negotio omnes reperiuntur.

Annotatio 17.

Quo autem clarius appareat, cuiusmodi valores littera α perpetuo sit habitura, tabulam sequentem adiicere visum est, similem eius, quae annot. 9. habetur.

Erit scilicet	si fuerit
$\alpha = 3$	$N = 3n + 1$
$\alpha \neq 3$	$N = 3n - 1$
$\alpha = 5$	$N = 5n \begin{cases} +1 \\ -1 \end{cases}$
$\alpha \neq 5$	$N = 5n \begin{cases} +2 \\ -1 \end{cases}$
$\alpha = 7$	$N = 7n \begin{cases} +1 \\ +2 \\ -3 \end{cases}$
$\alpha \neq 7$	$N = 7n \begin{cases} -1 \\ -2 \\ +3 \end{cases}$
$\alpha = 11$	$N = 11n \begin{cases} +1 \\ -2 \\ +3 \\ +4 \\ +5 \end{cases}$
$\alpha \neq 11$	$N = 11n \begin{cases} -1 \\ +2 \\ -3 \\ -4 \\ -5 \end{cases}$

$\alpha = 13$

$$\alpha = 13 \;\Big|\; N = 13n \begin{cases} +1 \\ -1 \\ +3 \\ -3 \\ +4 \\ -4 \end{cases}$$

$$\alpha = 13 \;\Big|\; N = 13n \begin{cases} +2 \\ -1 \\ +5 \\ -5 \\ +6 \\ -6 \end{cases}$$

Annotatio 18.

Ex hac igitur tabula numeri primi, qui idoneos valores pro α praebeant, facile dignofci fimulque inepti reiici poffunt. Propofito fcilicet numero primo p, omnes numeri quadrati in huiusmodi formulis $pn + \theta$: comprehendi poffunt, quae prodeunt ponendo pro θ numeros quadratos, feu refidua, quae ex diuifione quadratorum per p remanent. Quare fi N fuerit huiusmodi numerus $pn + tt$, tum inter formas diuiforum $4Nm \pm \alpha$ formulae $aa - Nbb$ feu $Nbb - aa$, habebitur $\alpha = p$, fin autem numerus N non contineatur in forma $pn + tt$, tum nullus numerus in formula hac $4Nm \pm p$ contentus poterit effe diuifor vllius numeri huius formae $aa - Nbb$.

Annotatio 19.

Si fuerit N numerus impar formae $4n + 1$ tum expreffionis $aa - Nbb$ diuiforum formae $4Nm \pm \alpha$ ad duplo pauciores reduci poffunt, ita vt exhiberi poffint hoc modo: $2Nm \pm \alpha$. Hoc fcilicet cafu, fi $4Nm \pm \alpha$ fuerit forma diuiforum, tum quoque $4Nm \pm (2N - \alpha)$ erit diuiforum forma, fic cum cafu $N = 13$, vna diuiforum formulae $aa - 13bb$ forma effet $52m \pm 3$, erit quoque $52m \pm 23$ forma diuiforum.

Annotatio. 20.

Sin autem fuerit N vel numerus impariter par, vel numeru impar formae $4n-1$ tum ista formarum diuidentium reductio ad duplo pauciores non succedit. Scilicet si hoc casu formulae $aa-Nbb$ fuerit $4Nm\pm\alpha$ diuisorum forma, tum $4Nm\pm(2N-\alpha)$ talis non erit, hoc est: nullus numerus in forma $2(2m\pm1)N\pm\alpha$ contentus erit diuisor vllius numeri huiusmodi $aa-Nbb$. Posito ergo $\alpha=tt$, erit

$$(2(2m\pm1)N\pm tt)u = aa-Nbb.$$

Vnde consequimur sequens.

Consectarium.

Nullus numerus in hac forma $2abc\pm c\pm b$ contentus vnquam potest esse quadratus, si quidem fuerit a numerus impar, et b numerus seu impariter par, seu impar huius formae $4n-1$.

Scholion 2.

Huiusmodi formulae magis speciales, quae nunquam quadrata fieri queant, innumerabiles superioribus deduci possunt. Consideremus enim priorum formam $aa+Nbb$, sitque $4Nm+A$ eiusmodi formula, vt nullus numerus in ea contentus possit esse diuisor formae $aa+Nbb$. Erit ergo $aa+Nbb=(4Nm+A)u$, denotante hoc signo $=$ aequationem impossibilem, ex quo oritur $aa=4Nmu+Au-Nbb$. Sit $b=Ac$ fiet $aa=4Nmu+Au-NAAcc$. Ponatur porro $u=NAcc+d$, eritque $aa=4NNAmcc+4Nmd+Ad$. Sit $d=4NNn$ erit $aa=16N^3mn+4NNAmcc+4NNAn$. Diuidatur haec

haec formula per quadratum $4NN$ ac ponatur $c = 1$ eritque $4Nmn + Am + An$ formula, quae nunquam poterit esse quadratum, si quidem forma $aa + Nbb$ non possit diuidi per vllum numerum in hac formula $4Nm + A$ contentum. Ex superioribus ergo theorematis colligimus nullum numerum, qui in vna sequentium expressionum contineatur, fieri posse quadratum.

$4mn - (m+n)$	$4mn + 3(m+n)$
$8mn - (m+n)$	$8mn + 7(m+n)$
$8mn - 3(m+n)$	$8mn + 5(m+n)$
$12mn - (m+n)$	$12mn + 11(m+n)$
$12mn - 7(m+n)$	$12mn + 5(m+n)$
$20mn - (m+n)$	$20mn + 19(m+n)$
$20mn - 3(m+n)$	$20mn + 17(m+n)$
$20mn - 7(m+n)$	$20mn + 13(m+n)$
$20mn - 9(m+n)$	$20mn + 11(m+n)$
$24mn - (m+n)$;	$24mn + 23(m+n)$
$24mn - 5(m+n)$;	$24mn + 19(m+n)$
$24mn - 7(m+n)$;	$24mn + 17(m+n)$
$24mn - 11(m+n)$;	$24mn + 13(m+n)$
$28mn - (m+n)$;	$28mn + 27(m+n)$
$28mn - 9(m+n)$;	$28mn + 19(m+n)$
$28mn - 11(m+n)$;	$28mn + 17(m+n)$
$28mn - 15(m+n)$;	$28mn + 13(m+n)$
$28mn - 23(m+n)$;	$28mn + 5(m+n)$
$28mn - 25(m+n)$;	$28mn + 3(m+n)$.

cet.

Notandum autem est in formulis alterius columnae numeros m et n respectu coefficientis ipsius $m+n$ primos esse oportere. Hanc restrictionem requirit ea conditio, quam initio stabilinibiliuimus, vt in forma $aa+Nbb$ numeri a et b ſint inter ſe numeri primi: niſi enim haec conditio obſeruetur, quilibet numerus poſſet eſſe diuiſor iſtius formae. Ceterum hac conditione obſeruata ex praecedentibus perſpicuum eſt, ſi $4Nmn-A(m+n)$ quadratum eſſe nequeat, tum quoque hanc latius patentem $4Nmn-A(m+n)\pm 4Np(m+n)$ quadratum eſſe non poſſe.

Scholion 3.

Contemplemur iam expreſſionem $aa-Nbb$ cuius nullus diuiſor contineatur in formula hac $4Nm\pm A$. Erit ergo $aa-Nbb=4Nmu\pm Au$ ſeu $aa=4Nmu+NAA\pm Au$. Ponatur $NA\pm u=d$, ſeu $u=\pm d\mp NA$, eritque $aa=\pm 4Nmd\mp 4NNAm+Ad$, ſit $d=\pm 4NNn$ fietque $16N^2mn\mp 4NNAm\pm 4NNAn=aa$, vnde patet nullum numerum contentum in hac formnla $4Nmn\pm A(m-n)$ quadratum eſſe poſſe. Neque ergo etiam vllus numerus in hac expreſſione $4Nmn\pm A(m-n)\pm 4Np(m-n)$ contentus quadratum eſſe poterit, ſi modo conditio ante memorata obſeruetur, vt a et b ſint numeri inter ſe primi. Hinc itaque ex theorematis poſterioribus deducuntur ſequentes formulae, quae nunquam numeros quadratos praebere poſſunt.

$$8mn\pm 3\,(m-n), \quad 8mn\pm 5\,(m-n)$$
$$12mn\pm 5\,(m-n); \quad 12mn\pm 7\,(m-n)$$
$$20mn\pm 3\,(m-n); \quad 20mn\pm 17\,(m-n)$$
$$20mn\pm 7\,(m-n); \quad 20mn\pm 13\,(m-n)$$
$$24mn\pm 7\,(m-n); \quad 24mn\pm 17\,(m-n)$$
$$24mn\pm 11\,(m-n); \quad 24mn\pm 13\,(m-n)$$

$$28mn \pm 5\,(m-n); \quad 28mn \pm 23\,(m-n)$$
$$28mn \pm 11\,(m-n); \quad 28mn \pm 17\,(m-n)$$
$$28mn \pm 13\,(m-n); \quad 28mn \pm 15\,(m-n)$$

cet.

attendenti autem facile patebit ambos numeros m et n reſpectu coefficientis ipſius $(m-n)$ primos eſſe debere: alioquin enim, ſi verbi gratia in formula $12mn \pm 5(m-n)$ poneretur $m = 5p$ et $n = 5q$, prodiret $12.25pq \pm 25(p-q)$, neque adeo haec formula $12pq \pm (p-q)$ quadratum eſſe poſſet, quod tamen eſt falſum.