1801

De formulis speciei *mxx+nyy* ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus

Leonhard Euler

DE FORMVLIS SPECIEI $mxx+nyy$ AD NVMEROS PRIMOS EXPLORANDOS IDONEIS, EARVMQVE MIRABILIBVS PROPRIETATIBVS.

Auctore

L. EVLERO.

Conv. Acad. exhib. die 16 Mart. 1778.

§. 1.

Hic praecipue reſpicio ad eam huiusmodi formularum proprietatem, qua conſtat omnes numeros, qui in tali forma $mxx+nyy$ duplici modo continentur, certe non eſſe primos, ſiquidem numeri m et n ambo fuerint poſitivi; ſi enim alter eorum eſſet negativus, utique evenire poſſet, ut idem numerus primus pluribus modis in tali formula contineretur. Veluti ſi $m=2$ et $n=-1$, in formula $2xx-yy$ numerus primus 7 pluribus adeo modis continetur, ſcilicet

I. Si $x=2$, $y=1$ II. Si $x=4$, $y=5$ III. Si $x=8$, $y=11$ atque adeo infinitis aliis modis hoc contingere poteſt.

§. 2

§. 2. Verum si ambo numeri m et n fuerint positivi, uti deinceps perpetuo supponemus, tum quoties quispiam numerus N duplici modo in formula $mxx+nyy$ continetur, ita ut sit $N = maa+nbb = mcc+ndd$, eius factores per hanc regulam satis facilem semper inveniri possunt. Formetur enim primo fractio $\frac{p}{q} = \frac{a+c}{b+d}$ ad minimos terminos reducenda; hincque formetur alia fractio $\frac{r}{s} = \frac{mpp}{nqq}$ pariter ad formam simplicissimam reducenda, quo facto erit $r+s$ factor numeri N, siquidem $r+s$ fuerit numerus impar, sin autem fuerit par, tum eius semissis $\frac{r+s}{2}$ factor erit numeri N; et quoniam ob ambiguitatem signi quatuor variationes locum habent, binae dabunt unum ipsius N factorem, binae reliquae vero alterum.

§. 3. Quo hoc clarius perspiciatur, sequens perpendamus exemplum. Consideremus formulam $7xx+3yy$, ubi $m=7$ et $n=3$, in qua numerus 391 duplici modo continetur, cum sit primo

$391 = 7.7^2 + 3.11^2$, tum vero etiam

$391 = 7.13^2 + 3.4^2$.

Hinc ergo erit $\frac{p}{q} = \frac{7+3}{11+4}$, cuius ergo quaterni valores erunt

I. $\frac{p}{q} = \frac{1}{3}$; II. $\frac{p}{q} = \frac{9}{17}$;

III. $\frac{p}{q} = \frac{1}{3}$; IV. $\frac{p}{q} = \frac{9}{17}$;

hinc iam porro deducantur sequentes fractiones:

I. $\frac{r}{s} = \frac{7}{3}\frac{1^2}{5^2} = \frac{21}{175}$; II. $\frac{r}{s} = \frac{7.9^2}{5.17^2} = \frac{567}{1445}$.

III. $\frac{r}{s} = \frac{7}{3}\frac{1^2}{3^2} = \frac{7}{27}$; IV. $\frac{r}{s} = \frac{7.9^2}{3.17^2} = \frac{567}{867}$.

Hic ergo prodit ubique $r+5$ numerus par, ideoque semis-

sem

fem capiendo ex primo et quarto oritur factor 23, at vero ex fecundo et tertio colligitur alter factor 17; revera autem eft $391 = 17 \cdot 23$.

§. 4. Contemplemur etiam fequens exemplum non parum memorabile, quo $m = 5$ et $n = 3$, atque in formula $5xx + 3yy$ numerus 512 duplici modo continetur cum fit primo $512 = 5 \cdot 1^2 + 3 \cdot 13^2$ et $512 = 5 \cdot 4^2 + 3 \cdot 12^2$, unde fit $\frac{p}{q} = \frac{4 \pm 1}{13 \pm 12}$, cuius quatuor valores funt

I. $\frac{p}{q} = \frac{1}{5}$; II. $\frac{p}{q} = \frac{5}{1}$;

III. $\frac{p}{q} = \frac{3}{25}$; IV. $\frac{p}{q} = \frac{3}{1}$;

unde fractiones $\frac{r}{s}$ fient:

I. $\frac{r}{s} = \frac{5 \cdot 1^2}{3 \cdot 5^2} = \frac{1}{15}$; II. $\frac{r}{s} = \frac{5 \cdot 5^2}{3 \cdot 1^2} = \frac{125}{3}$;

III. $\frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 25^2} = \frac{3}{125}$; IV. $\frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 1^2} = \frac{15}{1}$;

ergo formula $\frac{r+s}{2}$ ex primo et quarto dat factorem 8, e fecundo vero et tertio factorem 64, quorum productum ut que eft 512.

§. 5. Verum idem hic numerus 512 infuper du bus aliis modis in eadem formula $5xx + 3yy$ continetu priori fcilicet modo reperitur

$512 = 5 \cdot 8^2 + 3 \cdot 8^2$, pofteriori vero modo

$512 = 5 \cdot 10^2 + 3 \cdot 2^2$,

hinc ergo plures alios factores reperire licebit, id quod rum non eft, quia numerus 512 pluribus modis in du factores refolvi poteft. Veluti prima et poftrema refolu dant $\frac{p}{q} = \frac{10 \pm 1}{13 \pm 2}$, unde hae quatuor emergunt fractiones:

I. $\frac{p}{q} = \frac{11}{15}$; II. $\frac{p}{q} = \frac{11}{11}$;

III. $\frac{p}{q} = \frac{3}{5}$; IV. $\frac{p}{q} = \frac{9}{11}$;

unde pro $\frac{r}{s}$ ſequentes orientur fractiones:

I. $\frac{r}{s} = \frac{5 \cdot 11^2}{3 \cdot 15^2} = \frac{121}{135}$; II. $\frac{r}{s} = \frac{5 \cdot 1^2}{3 \cdot 1^2} = \frac{5}{3}$;

III. $\frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 5^2} = \frac{3}{5}$; IV. $\frac{r}{s} = \frac{5 \cdot 9^2}{3 \cdot 11^2} = \frac{135}{121}$;

unde factores ex $\frac{r+s}{2}$ oriundi erunt: alter 128, alter vero 4, quorum productum utique eſt 512.

§. 6. Cum igitur haec propoſitio ſit certiſſima: *Quod omnes numeri plus uno modo in eadem formula* $mxx+nyy$ *contenti non ſint primi ſed compoſiti, ideoque numeri primi unico tantum modo in tali formula contineri queant;* contemplemur huius propoſitionis inverſam, quae ita enunciabitur: *Quod omnes numeri compoſiti in formula* $mxx+nyy$ *contenti etiam plus uno modo in eadem contineantur, vel quod omnes numeri unico tantum modo in iſta formula contenti certe ſint primi.*

§. 7. Statim autem patet hanc propoſitionem inverſam in genere admitti non poſſe, cum innumerabiles caſus exhiberi queant, quibus numeri valde compoſiti in talibus formulis unico tantum modo continentur. Ita ſi $m = 7$ et $n = 2$, in formula $7xx + 2yy$ iſte numerus compoſitus 15 certe unico tantum modo continetur, ſcilicet quando $x = 1$ et $y = 2$. Quin etiam in eadem formula iſte numerus compoſitus $1807 = 13 \cdot 139$ unico tantum modo contineri deprehenditur, ſcilicet quando $x = 1$ et $y = 30$. Ex quo manifeſto apparet, iſtam propoſitionem inverſam, quod numeri unico tantum modo in tali formula $mxx + nyy$ contenti

etiam ſint numeri primi, in genere veritati non eſſe conſentaneam.

§. 8. Interim tamen plures caſus pro binis numeris m et n ita ſunt comparati, ut propoſitio illa inverſa egregie cum veritate conſentiat, inter quos notiſſimus eſt caſus, quo $m = 1$ et $n = 1$ et formula noſtra ſumma duorum quadratorum $xx + yy$; ſiquidem iam rigoroſe eſt demonſtratum, omnes numeros, qui unico tantum modo ſunt ſummae duorum quadratorum, ſemper etiam eſſe primos, dummodo fuerint impares, atque numeri x et y primi inter ſe, quae levis limitatio ſponte ſua patet. Atque hoc ipſo principio iam olim ſum uſus ad numeros praegrandes examinandos, utrum ſint primi nec ne. Statim enim atque oſtenſum fuerit numerum quantumvis magnum (imparem) unico tantum modo eſſe ſummam duorum quadratorum, etiam certum eſt eum eſſe primum.

§. 9. Eadem quoque indole praeditae ſunt ſequentes formulae ſimpliciores, veluti: $2xx+yy$; $3xx+yy$; $3xx+2yy$; $5xx+yy$; $5xx+2yy$; $5xx+3yy$; $6xx+yy$; $6xx+5yy$; etc. de quarum plerisque a Geometris iam demonſtratum, vel ſaltem obſervatum eſt, quod omnes numeri in quapiam earum unico tantum modo contenti etiam certe ſint primi, ſi modo pauciſſimi caſus, per ſe perſpicui, excipiantur; ſcilicet quando numeri vel ſunt pares, vel cum numeris m et n communem diviſorem recipiunt. Quin etiam in certis formulis evenire poteſt, ut adeo poteſtates binarii unico modo contineantur, veluti numerus 8 in formula $5xx+3yy$ et numerus 16 in formula $15xx+yy$, quibus ergo caſibus poteſtates binarii numeris primis aequivalere

lere ſunt cenſendae, propterea quod non diverſos factores involvunt.

§. 10. Hinc igitur intelligimus in formula $mxx+nyy$ ingens intercedere diſcrimen, cum aliae iſta ſint comparatae, ut omnes numeri unico modo in iis contenti recte pro primis haberi queant, dum aliae hac inſigni proprietate ſunt deſtitutae, quemadmodum in formula $7xx+2yy$ uſu venire iam ante obſervavimus. Quam ob rem cum iſtud diſcrimen non ſolum ſit maximi momenti, ſed etiam in ipſa natura harum formularum fundatum, plurimum conveniet, duas talium formularum claſſes conſtituere, atque a ſe invicem ſollicite diſtinguere, quandoquidem hic nobis propoſitum eſt inſignes atque adeo mirabiles proprietates prioris claſſis accuratius evolvere, quam ergo ſequenti definitione determinemus.

Definitio.

Quando numeri m et n ita ſunt comparati, ut omnes numeri unico modo in formula $mxx+nyy$ *contenti ſint vel ipſi primi, vel tantum binarium vel quempiam factorem numerorum m et n involvant, vel etiam certis caſibus ſint poteſtates binarii; tales formulas in ſequentibus formulas congruas appellabimus; ubi quidem per ſe perſpicuum eſt ambos numeros x et y inter ſe primos accipi debere.*

§. 11. Hic igitur probe tenendum eſt numeros ſemel tantum in tali formula congrua $mxx+nyy$ contentos non ſtatim pro primis eſſe habendos, propterea quod evenire poteſt, ut denotante p numerum primum quemcunque, iſti numeri etiam formam habeant vel $2p$, vel δp, exiſtente δ

diviſore producti mn. Hic autem poſterior caſus penitus ceſſat, quando numerus x primus ad n, ſimulque y primus ad m accipiatur. Deinde vero etiam iam obſervavimus, poteſtates quoque binarii unico tantum modo in certis formulis, veluti $5xx + 3yy$ contineri poſſe, quae tamen formula nihilominus pro congrua eſt habenda, cum omnes numeri impares ad $3 \cdot 5 = 15$ primi et unico modo in hac formula contenti ſemper revera ſint primi. Ita quia numerus 107 unico modo in iſta formula continetur, ſumendo ſcilicet $x = 4$ et $y = 3$, is recte pro primo haberi poteſt.

§. 12. Quoniam igitur in hoc iudicio non ſolum numeri primi ipſi p ſed etiam $2p$ et δp inſtar primorum ſpectari queant, denotante δ diviſorem quempiam numeri mn, quibus adeo certis caſibus etiam poteſtates binarii ad numerare licet; viciſſim ſequitur omnes reliquos numeros quos revera compoſitos vocemus, qui in tali formula contenta $mxx + nyy$ continentur, ſimul quoque plus quam uno modo in ea contineri debere. Veluti quia numerus $527 = 5 \cdot 10^2 + 3 \cdot 3^2$ non eſt primus, ſed factoribus conſtat $17 \cdot 31$, is inſuper alio modo in eadem formula continetur ſcilicet eſt $527 = 5 \cdot 2^2 + 3 \cdot 13^2$, atque ex hac duplici reſolutione per regulam ſupra datam factores numeri 527 ſequenti modo eruuntur. Cum primo ſit $\frac{p}{q} = \frac{10+2}{13+3}$, quatuor eius valores erunt $1^\circ.\ \frac{p}{q} = \frac{3}{4}$; $2^\circ.\ \frac{p}{q} = \frac{6}{5}$; $3^\circ.\ \frac{p}{q} = \frac{1}{2}$ $4^\circ.\ \frac{p}{q} = \frac{4}{5}$; unde porro altera fractio $\frac{r}{s} = \frac{mpp}{nqq}$ producit hos valores: $1^\circ.\ \frac{r}{s} = \frac{15}{16}$; $2^\circ.\ \frac{r}{s} = \frac{12}{5}$; $3^\circ.\ \frac{r}{s} = \frac{5}{12}$ et $4^\circ.\ \frac{r}{s} =$ unde aggregatum $r + s$ praebet duos factores 31 et 17.

§.

§. 13. Stabilita hac definitione formularum congruarum reliquas omnes hac insigni proprietate destitutas distinctionis gratia incongruas appellabimus easque hoc charactere designare licebit: quod etiam numeri revera compositi exhiberi queant, qui in talibus formulis unico tantum modo contineantur, veluti evenit in hac formula incongrua $7xx+5yy$, in qua iste numerus compositus $273=3.7.13$ unico tantum modo continetur, scilicet quando $x=2$ et $y=7$.

§. 14. Totum ergo negotium huc redit, ut regulam certam tradamus, cuius ope formulas congruas ab incongruis discernere liceat. Quoniam autem hic duo numeri m et n in considerationem sunt ducendi, universa haec quaestio ope sequentis theorematis ad considerationem unici numeri revocari potest.

Theorema.

Si formula $mxx+nyy$ est congrua, tum etiam haec formula $mnxx+yy$ erit congrua, ac viciſſim.

Demonstratio.

§. 15. Ponamus enim formulam $mxx+nyy$ esse congruam, alteram vero $mnxx+yy$ esse incongruam. Daretur igitur numerus revera compositus C unico tantum modo in hac formula contentus, qui sit $C=mnaa+bb$; hinc ergo foret $nC=mnnaa+nbb$ quoque unico modo, ideoque etiam unico modo in formula $mxx+nyy$ contineretur, existente scilicet $x=na$ et $y=b$; unde sequeretur formulam $mxx+nyy$ non esse congruam, contra hypothesin; unde necessario concludi oportet, quoties altera harum duarum

rum formularum fuerit congrua, neceſſario quoque alteram futuram eſſe congruam.

§. 16. Eodem modo etiam liquet, ſi altera harum formularum fuerit incongrua, etiam alteram talem eſſe futuram. Quare cum infra oſtendetur, hanc formulam $60xx+yy$ eſſe congruam, quoniam hic bini numeri m et n pluribus modis accipi poſſunt, haec ſola formula congrua etiam ſequentes omnes pariter congruas progignet: $30xx+2yy$; $20xx+3yy$; $15xx+4yy$; $12xx+5yy$ et tandem $10xx+6yy$.

§. 17. Hanc ob rem ad omnes formulas congruas conſtituendas ſufficiet omnes valores producti mn aſſignaſſe, cum deinde ex factoribus huiusmodi producti facillime omnes plane formulae congruae derivari queant.

Definitio.

Omnes numeros, quos loco producti mn aſſumere licet, ut formulae $mxx+nyy$ evadant congruae, in poſterum appellabimus numeros idoneos, vel etiam congruos, dum reliquos omnes incongruos vocabimus.

§. 18. Cum hoc idem argumentum iam nuper tractaverim, atque adeo omnes numeros idoneos, ſive congruos, exhibuerim, primo quidem hoc phoenomenon maxime mirandum ſe obtulit, quod multitudo iſtorum numerorum neutiquam in infinitum excreſcat, verum adeo non plures quam 65 huiusmodi numeros complectatur. Hos numeros, quoniam mihi propoſitum eſt plures proprietates eorum maxime memorabiles in medium afferre, ante omnia hic deſignemus.

Cata-

Catalogus
omnium numerorum idoneorum seu congruorum.

1.	1	23.	37	45.	177
2.	2	24.	40	46.	190
3.	3	25.	42	47.	210
4.	4	26.	45	48.	232
5.	5	27.	48	49.	240
6.	6	28.	57	50.	253
7.	7	29.	58	51.	273
8.	8	30.	60	52.	280
9.	9	31.	70	53.	312
10.	10	32.	72	54.	330
11.	12	33.	78	55.	345
12.	13	34.	85	56.	357
13.	15	35.	88	57.	385
14.	16	36.	93	58.	408
15.	18	37.	102	59.	462
16.	21	38.	105	60.	520
17.	22	39.	112	61.	760
18.	24	40.	120	62.	840
19.	25	41.	130	63.	1320
20.	28	42.	133	64.	1365
21.	30	43.	165	65.	1848
22.	33	44.	168		

§. 19. Maximus ergo numerus idoneus seu congruus est $1848 = 8.3.7.11$. qui ergo feliciſſimo ſucceſſu ad numeros primos explorandos adhiberi poterit. Si enim numerus quantumvis magnus N in forma $1848\,xx + yy$ contineatur, haud difficile erit inveſtigare, utrum inſuper alio modo in eadem

eadem formula contentus ſit, nec ne. Quodſi enim numerus unico modo contineri reperiatur, atque numerus y non ſolu primus fuerit ad x, ſed etiam ad ipſum 1848, tum tuto c cludere licebit, iſtum numerum N revera eſſe primum. H modo nuper plures numeros primos, ad multos milliones ex gentes, in medium protulimus, id quod multo minori lab praeſtari potuit, quam ſi, uti olim feci, ſumma binor quadratorum ad hunc finem uti vellemus. Talem autem eg gium uſum reliqui omnes numeri idonei maiores huius bulae praeſtabunt.

§. 20. Antequam autem in proprietates max memorabiles horum numerorum congruorum ſum inquiſitu conveniet praecipua momenta, quibus hi numeri innitun breviter exponere, quae ternis ſequentibus propoſitioni compleđi licet.

Propoſitio prima.

Nullus numerus minor quam $4mn$ plus uno n in formula $mnxx+yy$ contineri poteſt, niſi forte ſu quadratus; quia enim numerus minor ſupponitur quam 4 excluſo caſu $x=0$ pro numeris quadratis neceſſario debet $x=1$, atque adeo iſte numerus non niſi unico in hac formula contineri poteſt.

Propoſitio ſecunda.

Si numerus compoſitus, quantumvis magnus, u tantum modo in formula $mnxx+yy$ contineatur, tum per continuo multo minores numeri, pariter compoſiti, beri poſſunt unico etiam modo in hac forma contenti que tandem pervenietur ad numeros compoſitos mi

quam $4mn$. Huius propoſitionis veritatem non ita pridem demonſtravi.

Propoſitio tertia.

Si numerus mn ita fuerit comparatus, ut omnes numeri in formula $mn+yy$ contenti et minores quam $4mn$ ſint vel primi vel primis aequipollentes, tum iſte numerus mn certe erit idoneus et formula $mnxx+yy$ congrua. Quia enim nullus dabitur numerus compoſitus minor quam $4mn$ in iſta formula contentus, etiam nulli dabuntur numeri compoſiti, quantumvis magni, unico quoque tantum modo in eadem formula contenti, ſed omnes numeri unico tantum modo in ea contenti erunt vel primi, vel tanquam primi ſpectandi.

§. 21. Hinc facilis regula deducitur, cuius ope quoslibet numeros examinare licebit, utrum ſint congrui nec ne. Propoſito enim quocunque numero N, in formula $N+yy$ loco y ſucceſſive ſcribantur numeri 1, 2, 3, 4, 5, etc. donec perveniatur ad ſummam maiorem quam $4N$, atque ſi numeri hoc modo reſultantes fuerint vel primi p, vel etiam $2p$ vel δp (exiſtente δ diviſore numeri N) vel etiam poteſtates binarii, quibus adiungi oportet quadrata numerorum primorum, tum numerus iſte N erit idoneus et formula $Nxx+yy$ congrua; ſin autem hoc modo vel unicus numerus revera compoſitus occurrat, tum formula inter incongruas erit referenda.

§. 22. Illuſtremus hanc regulam exemplo numeri 48, unde addendo quadrata usque ad limitem $y=12$ orientur ſequentes numeri vel primi vel ut primi ſpectandi:

48	48
$+1 = 49 = pp$	$+ 7^2 = 97 = p$
$+2^2 = 52 = 4.13 = \delta p$	$+ 8^2 = 112 = 16.7 = \delta.p$
$+3^2 = 57 = 3.19 = \delta p$	$+ 9^2 = 129 = 3.43 = \delta.p$
$+4^2 = 64 = 16.4 = 2^\lambda$	$+10^2 = 148 = 4.37 = \delta.p$
$+5^2 = 73 = p$	$+11^2 = 169 = 13 = pp$
$+6^2 = 84 = 12.7 = \delta.p$	

Hinc ergo patet iſtum numerum utique eſſe idoneum, atque formulae, quae ex eo derivantur ſimul erunt congruae, quae ſunt $48xx + yy$ et $16xx + 3yy$, quandoquidem numeri pro m et n ſumendi inter ſe debent eſſe primi.

§. 23. Quamquam haec regula ad omnes caſus facile accommodari poteſt, tamen etiam alia dari poteſt regula maxime memorabilis, qua vera indoles numerorum idoneorum multo magis declaratur, quae ita ſe habet:

Regula condendi tabulam numerorum idoneorum.

§. 24. Ex ſerie omnium numerorum naturalium pro quolibet numero primo p excludantur numeri in hac forma contenti: $px - yy$, maiores quam $\frac{1}{4}pp$; praeter hos: $pp - yy$; quo facto pro ſingulis numeris primis p relinquentur numeri idonei. Notetur autem hic loco numeri primi 2 ſumi debere eius quadratum 4. Ita 1°. pro $p = 4$ excludi debent numeri formae $4x - 1 > 4$, praeter 15 et 7; numeri excludendi hinc erunt 11, 19, 23, 27, 31, 37, etc. 2°. Pro $p = 3$ excluduntur numeri $3x - 1$ maiores quam $\frac{9}{4}$, praeter 8 et 5; quare excludentur hi numeri: 11, 14, 17, 20, 23, 26, etc. 3°. Pro $p = 5$ excluduntur numeri formae $5x - 1, -4$ maiores quam $\frac{25}{4}$, praeter 24, 21, 16, 9; ergo excludendi ſunt

14,

14, 19, 29, 34, 39, etc. et 11, 26, 31, 36, 41, etc. 4°. Pro $p = 7$ excludi debent numeri formae $7x - 1, -4, -9 > \frac{49}{4}$, praeter 48, 45, 40, 33, 24, 13, unde numeri excludendi ſunt 20, 27, 34, etc. 17, 31, 38, 52, 59, etc. 19, 26, 47, 54, etc. 5°. Pro $p = 11$ excluduntur numeri $11x - 1$, $-4, -9, -16, -25 > \frac{121}{4} > 30$, praeter 120, 117, 112, 105, 96, 85, 72, 57, 40, 21, ſicque numeri excludendi erunt:

32, 43, 54, 65, 76, 87, 98, 109, 131, 142, etc.
51, 62, 73, 84, 95, 106, 128, 139, 150, etc.
35, 46, 68, 79, 90, 101, 123, 134, 145, etc.
39, 50, 61, 83, 94, 116, 127, 138, 149, etc.
41, 52, 63, 74, 107, 118, 129, 140, 151, etc.

hocque modo per omnes numeros primos eſt procedendum.

§. 25. Quamquam haec regula aliis innititur principiis, atque non parum discrepare videtur a criterio, quo numeri iſti idonei ab aliis numeris diſtinguuntur, tamen pulcherrimus conſenſus ubique deprehenditur. Praeterea vero etiam hi numeri tam egregiis proprietatibus ſunt praediti, quas adeo ex principiis plurimum diverſis demonſtrare licet, unde operae pretium erit iſtas proprietates in ſequentibus theorematibus ob oculos expoſuiſſe.

THEOREMATA,
quibus inſignes proprietates numerorum idoneorum demonſtrantur.

Theorema I.

In ordine numerorum idoneorum alii numeri quadrati non occurrunt, praeter 1, 4, 9, 16 et 25.

Demonſtratio.

§. 26. Si numerus idoneus eſt quadratum ii, formula congrua $iixx+yy$ utique erit ſumma duorum quadratorum. Conſideremus igitur numeros quoscunque compoſitos C, qui ſint ſummae duorum quadratorum, quod cum ſemper duplici modo evenire queat, ſtatuamus $C = aa+bb = cc+dd$, ac primo quidem ſit a numerus par $= 2f$, ut ſit $C = 4ff+bb$, ideoque b numerus impar, cuius quadratum cum ſemper ſit formae $4\alpha+1$, etiam ipe numerus C eandem habebit formam; unde evidens eſt, quadratorum cc et dd alterum par, alterum vero impar eſſe debere. Sit igitur $c = 2g$, eritque $C = 4gg+dd$; unde ſequitur, ſi numerus compoſitus C fuerit $= 4ff+bb$, eum quoque alio modo fore $C = 4gg+dd$; ex quo manifeſtum eſt quadratum 4 eſſe numerum idoneum.

§. 27. Ponamus nunc in eadem aequalitate $C = aa+bb = cc+dd$ numerum a eſſe multiplum ternarii, ſcilicet $a = 3f$, ut ſit $C = 9ff+bb$; et quia b ſupponitur primus ad a ideoque non diviſibilis per 3, eius quadratum bb habebit formam $3\alpha+1$, unde etiam ipſe numerus C eandem habebit formam $3\alpha+1$. Hanc autem formam altera expreſſio $cc+dd$ habere nequit, niſi alterum quadratorum cc et dd diviſibile ſit per 3, alterum vero non; ſi enim ambo non eſſent diviſibilia per 3, utrumque haberet formam $3\alpha+1$, ideoque eorum ſumma formam eſſet habitura $3\alpha+2$ diverſam ab illa. Ponatur igitur $c = 3g$, ita ut ſit $C = 9gg+dd$; unde patet, ſi numerus compoſitus habuerit formam $9ff+bb$, eum inſuper alio modo fore $9gg+dd$. Neceſſe igitur eſt ut quadratum 9 ſit numerus idoneus.

§. 28.

§. 28. Ponamus nunc esse $a = 4f$, ut sit $C = 16ff + bb$, atque demonstrandum est in altera forma $cc + dd$ vel c vel d etiam per 4 divisibile esse debere. Cum igitur numerus b sit impar, eius quadratum bb semper formam habet $8\alpha + 1$, eandemque ergo formam habebit numerus C, quam ergo formam quoque habere debet $cc + dd$; unde statim patet, alterum quadratum dd esse impar, ideoque formae $8\alpha + 1$, alterum vero cc par, atque adeo per 16 divisibile, sive $c = 4g$, ideoque $C = 16gg + dd$. Quare cum, si fuerit numerus compositus $C = 16ff + bb$, necessario quoque sit $C = 16gg + dd$, evidens est etiam quadratum 16 esse numerum idoneum.

§. 29. Sit porro $a = 5f$, ideoque $C = 25ff + bb$; et quia b divisionem per 5 non admittit, eius quadratum bb formam habebit $5\alpha + 1$ vel $5\alpha + 4$, ideoque ipse numerus C alterutram formam habere debet, quam ergo eandem formam habere debet $cc + dd$; unde statim patet, si neque c neque d divisibile esset per 5, summa $cc + dd$ formam foret habitura vel $5\alpha + 0$, vel $5\alpha + 2$, vel $5\alpha + 3$, quarum nulla congruit; unde sequitur, alterutrum numerorum c et d per 5 esse divisibilem. Sit igitur $c = 5g$, ideoque $C = 25gg + dd$; atque manifestum est, quoties numerus compositus C habuerit formam $25ff + bb$, semper insuper alio modo fore $C = 25gg + dd$, ideoque 25 esse numerum idoneum.

§. 30. Tale autem ratiocinium non ulterius extendi potest. Si enim ponamus $a = 6f$, ut sit $C = 36ff + bb$, quadratum bb necessario formam habebit $6\alpha + 1$, quae ergo forma etiam ipsi C convenit; verum pro altera forma $cc + dd$ non absolute necesse est, ut sit $c = 6g$: eadem enim forma

$6\alpha+1$ reſultare poteſt, ſumendo $c=2g$ et $d=6h+3$, ita ut horum numerorum alter per 2 alter vero per 3 ſit diviſibilis. Quia igitur g diviſionem per 3 admittere non debet, eius quadratum formam habebit $3\alpha+1$, ideoque cc formam $12\alpha+4$, ſive $6\alpha+4$; alterum vero quadratum dd formam habet $6\alpha+3$, quorum ergo quadratorum ſumma producit formam $6\alpha+1$, perinde ut ante. Quocirca cum, ſi fuerit $C=36ff+bb$, non neceſſe ſit ut etiam ſiat $C=36gg+dd$, hinc ſequitur numerum 36 non eſſe numerum idoneum; quod etiam criterium primo datum declarat, quoniam $36+7^2=85=5.17$. qui numerus revera eſt compoſitus et minor quam 4.36.

§. 31. Quo hoc clarius appareat, conſideremus caſum $a=7f$, ut ſit $C=49ff+bb$, ideoque b non diviſibile per 7, unde forma ipſius bb erit $7\alpha+1, 2, 4$, quod etiam de ipſo numero C valet. Videamus igitur num pro altera formula $cc+dd$ aliqua harum formarum reſultare poſſit, etiamſi neque c neque d per 7 ſumatur diviſibile, quo ergo caſu tam cc quam dd haberet formam vel $7\alpha+1$, vel $7\alpha+2$ vel $7\alpha+4$, ideoque eorum ſumma ad has formas perducit $7\alpha+1, 2, 3, 4, 5, 6$, hoc eſt omnes formas poſſibiles, in quibus ſuperiores tres formae utique continentur. Quare cum neutiquam neceſſe ſit, ut alter numerorum c et d etiam per 7 ſit diviſibilis, manifeſtum eſt etiam numerum 49 non eſſe idoneum; quod idem de numeris maioribus multo magis valebit, id quod etiam criterium noſtrum manifeſto declarat, cum ſit $49+6^2=5.17$, atque adeo $49+4^2=5.13$.

Theo-

Theorema II.

Si numerus idoneus fuerit formae $4\alpha - 1$ *tum etiam eius quadruplum* $4(4\alpha - 1)$ *erit numerus idoneus.*

Demonstratio.

§. 32. Sit brevitatis gratia $4\alpha - 1 = i$, ita ut pro quovis numero compoſito C fit $C = iaa + bb = icc + dd$. Iam ponamus eſſe $a = 2f$, ut prior forma evadat $C = 4iff + bb$, ubi ergo, ob b numerum imparem, quadratum bb habebit formam $4\alpha + 1$. Quia nunc i eſt numerus impar, alteruter numerorum c et d erit par, alter impar, unde duos caſus evolvi oportet. Sit primo $c = 2g$, et quia dd eſt formae $4\alpha + 1$, hoc utique congruit cum forma praecedente. Examinemus vero etiam alterum caſum, quo $d = 2h$. at cc impar, ideoque formae $4\alpha + 1$; cum igitur ſit $i = 4\alpha - 1$, numerus icc formam habebit $4\alpha - 1$, quae cum discrepet a forma priore $4iff + bb$, evidens eſt etiam numerum c parem eſſe debere. Sit igitur $c = 2g$, ut prodeat $C = 4igg + dd$, quam ob rem evictum eſt, ſi numerus compoſitus C formam habeat $4iff + bb$, neceſſario etiam alio modo proditurum eſſe $C = 4igg + dd$, ſicque evictum eſt etiam numerum $4i$ eſſe idoneum, ſiquidem fuerit $i = 4\alpha - 1$ numerus idoneus.

Corollarium.

§. 33. In tabula autem numerorum idoneorum ſupra allata alios numeros formae $4\alpha - 1$ non reperimus praeter 3, 7, 15, quorum etiam quadrupla 12, 28, 60 in eadem tabula reperiri videmus; quin etiam horum denuo quadrupla 48, 112, 240 etiam ibidem occurrunt, quemadmodum in ſequente theoremate demonſtrabimus.

Theo-

Theorema III.

Denotante i numerum imparem, ſi fuerit $4i$ numerus idoneus, tum etiam eius quadruplum $16i$ erit ſemper numerus idoneus.

Demonſtratio.

§. 34. Cum $4i$ ſit numerus idoneus, dabuntur numeri compoſiti C, ut ſit $C = 4iaa + bb = 4icc + dd$, ubi ergo numeri b et d erunt impares, ideoque eorum quadrata formae $8\alpha + 1$. Ponamus iam eſſe $a = 2f$, ut ſit $C = 16iff + bb$, qui numerus eſt formae $8\alpha + 1$. Quodſi iam c foret numerus impar, ob i numerum imparem, etiam icc erit impar, ideoque $4icc$ numerus formae $8\alpha + 4$, unde ob $dd = 8\alpha + 1$ forma poſterior foret $8\alpha + 5$, cum prior eſſet $8\alpha + 1$; ex quo ſequitur etiam numerum c neceſſario parem eſſe debere. Poſito igitur $c = 2g$, erit utique $C = 16iff + bb = 16igg + dd$, unde manifeſto ſequitur numerum $16i$ quoque eſſe idoneum.

Corollarium.

§. 35. Quando autem aſſumimus numerum $4i$ eſſe idoneum, neceſſe eſt ut etiam ipſe numerus i ſit idoneus, id quod in ſequente theoremate demonſtrabitur.

Theorema IV.

Si fuerit $\lambda\lambda i$ numerus idoneus ſemper etiam ipſe numerus i erit idoneus.

Demonſtratio.

§. 36. Quia $\lambda\lambda i$ eſt numerus idoneus, dabuntur numeri compoſiti C, ut ſit $C = \lambda\lambda iaa + bb = \lambda\lambda icc + dd$; ubi ſi

si ponamus $\lambda a = f$ et $\lambda c = g$, erit $C = i f f + b b = i g g + d d$, unde luculenter, liquet, etiam numerum i esse idoneum. Quoties igitur quispiam numerus idoneus per quadratum fuerit divisibilis, etiam facta divisione quotus erit numerus idoneus.

Theorema V.

Si habeatur numerus idoneus formae $3\alpha - 1$, etiam eius noncuplum semper erit numerus idoneus.

Demonstratio.

§. 37. Posito brevitatis gratia $3\alpha - 1 = i$, ut habeamus talem aequationem: $C = i a a + b b = i c c + d d$, sumamus $a = 3f$, ut sit $C = 9 i f f + b b$, ubi ergo, quia b primus ad a, quadrati $b b$ forma erit $3\alpha + 1$, ideoque ipse numerus C formae $3\alpha + 1$. Iam si in altera forma $i c c + d d$ numerus c non esset divisibilis per 3, foret $c c = 3\alpha + 1$, ideoque $i c c$ formae $3\alpha - 1$. Nunc autem alter numerus d vel erit per 3 divisibilis vel secus; priore casu, ob $d d = 3\alpha$, posterior forma foret $3\alpha - 1$; posteriore casu forma prodiret 3α. Quare cum prior forma sit $C = 3\alpha + 1$, cui neutra harum convenit, necesse est, ut numerus c sit per 3 divisibilis. Posito ergo $c = 3g$, habebimus $C = 9 i f f + b b = 9 i g g + d d$; unde manifestum est etiam numerum $9i$ esse idoneum, siquidem i fuerit numerus formae $3\alpha - 1$.

Corollarium.

§. 38. In tabula autem numerorum idoneorum alii numeri formae $3\alpha - 1$ non occurrunt, praeter hos tres: 2, 5, 8, quorum etiam noncupla 18, 45 et 72 in eadem tabula reperimus.

Theorema VI.

Si numerus impar formae $4\alpha + 1$ fuerit numerus id
neus, tum eius quadruplum $4(4\alpha + 1)$ in tabula numerorun
idoneorum occurrere nequit.

Demonſtratio.

§. 39. Poſito brevitatis gratia $4\alpha + 1 = i$ conſ
deremus hanc aequalitatem: $C = iaa + bb = icc + dd$
ubi ponamus $a = 2f$, ut ſit $C = 4iff + bb$. Iam niſi al
ſolute neceſſarium ſit, ut etiam c ſit numerus par, numer
$4i$ non erit idoneus. Conſideremus igitur caſum, quo c n
merus impar, eritque $cc = 4\alpha + 1$, ideoque icc form
$4\alpha + 1$; quare cum hoc caſu d ſit numerus par, poſteri
forma erit $4\alpha + 1$; unde patet neceſſe non eſſe, ut c ſit n
merus par, quod ipſum indicio eſt etiam numerum $4i$ n
eſſe idoneum.

Corollarium.

§. 40. Numeri autem formae $4\alpha + 1$, qui in noſt
tabula numerorum idoneorum occurrunt, ſunt 1, 5, 9, 1
21, 25, 33, 37, 45, 57, 85, 93, 105, 133, 165, 177, 25
273, 345, 357, 385, 1365, quorum etiam nullius quadr
plum in noſtra tabula deprehendimus, praeter unitatis, c
ius ratio eſt prorſus peculiaris.

Theorema VII.

Si inter numeros idoneos occurrat numerus imparit
par, ſive formae $4\alpha + 2$, tum etiam ſemper eius quadruplu
$4(4\alpha + 2)$ in eadem tabula reperietur.

Demonſtratio.

§. 41. Ponatur brevitatis gratia $4\alpha+2=i$, et conſideretur haec aequatio: $C=iaa+bb=icc+dd$, ac ponatur $a=2f$, quo facto, ſi etiam c neceſſario debet eſſe numerus par, evictum erit numerum $4i$ eſſe idoneum. Hic vero ante omnia notandum, quia i eſt numerus par, numeros b et d eſſe impares, eorumque ergo quadrata formae $8\alpha+1$, unde eorum differentia $bb-dd$ ſemper erit per octo diviſibilis. Cum igitur ſit $bb-dd=i(cc-4ff)$, neceſſe eſt ut hoc poſterius membrum diviſionem per 8 admittat; at vero prior factor i tantum per 2 dividi poteſt, unde patet alterum factorem $cc-4ff$ diviſibilem eſſe debere per 4, hincque ſequitur numerum c neceſſario parem eſſe debere. Sit igitur $c=2g$, ac ſi numerus compoſitus C habuerit formam $4iff+bb$, ſemper etiam alio modo erit $C=4igg+dd$; unde manifeſto ſequitur etiam numerum $4i$ eſſe idoneum, ſiquidem numerus $i=4\alpha+2$ talis fuerit.

Corollarium.

§. 42. Numeri autem impariter pares in tabula numerorum idoneorum occurrunt ſequentes: 2, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462, quorum etiam ſingulorum quadrupla revera in tabula noſtra reperiuntur.

Theorema VIII.

Denotante i numerum imparem, ſi fuerit $8i$ numerus idoneus, eius quadruplum $32i$ certe non erit numerus idoneus.

Demonſtratio.

§. 43. Poſito enim $C=8iaa+bb=8icc+dd$, ſi ponamus $a=2f$, ut prior formula fiat $C=32iff+bb$, vi-

deamus, num etiam neceſſario hinc ſequatur numerum c quoque parem eſſe debere. Primo igitur notetur numeros b et d eſſe impares, ideoque differentiam quadratorum $bb-dd$ diviſibilem per 8. Cum igitur ſit $bb-dd=8icc-32iff=8i(cc-4ff)$ quae forma ſponte eſt diviſibilis per 8, nulla neceſſitas adeſt, quod numerus c debeat eſſe par, conſequenter etiam numerus 32 non erit idoneus.

Corollarium.

§. 44. Quando numerus $8i$ eſt idoneus, tum etiam eius pars quarta $2i$ erit numerus idoneus. Ac ſi i denotet numerum imparem, modo ante vidimus etiam $8i$ eſſe numerum idoneum. Nunc autem intelligimus multiplicationem per 4 non ulterius locum habere poſſe, ita ut non ſolum $32i$, ſed etiam $128i$ et $512i$ etc. ex ordine numerorum idoneorum excludantur.

Theorema IX.

Denotante i numerum imparem, ſi fuerit $16i$ numerus idoneus, tum eius quadruplum $64i$ certe non erit numerus idoneus.

Demonſtratio.

§. 45. Poſito enim $C=16iaa+bb=16icc+dd$, ſi ponamus $a=2f$, ob $bb-dd$ diviſibile per 8, etiam forma $16i(cc-4ff)$ per 8 diviſibilis eſſe debet, quod cum ſponte eveniat, nulla neceſſitas urget, ut etiam numerus c par accipi debeat; ex quo ſequitur numerum $64i$ nunquam eſſe poſſe numerum idoneum.

Corol-

Corollarium.

§. 46. Quando hic assumimus numerum $16\,i$ esse idoneum, per se intelligitur etiam $4\,i$ et i esse numerum idoneum, quare cum multiplicatio per 4 ulterius locum non habeat, ex binis postremis theorematibus conficitur nullo plane dari numeros idoneos, qui per altiorem binarii potestatem quam quartam essent divisibiles. Vidimus autem tres tantum dari tales numeros per 16 divisibiles, scilicet 48, 112 et 240; nulli autem prorsus dantur, qui per 32, vel 64, vel altiorem potestatem essent divisibiles.

Theorema X.

Si i fuerit numerus idoneus formae cuiuscunque, sitque $i + a\,a = p\,p$, existente p numero primo, tum eius quadruplum $4\,i$ ex tabula numerorum idoneorum excluditur, existente $p\,p < 4\,i$.

Demonstratio.

§. 47. Quoniam $i + a\,a = p\,p$, erit $4\,i + 4\,a\,a = 4\,p\,p$. At sit $4\,i$ essetque numerus idoneus, tum forma $4\,i + x\,x$ esse deberet vel numerus primus, vel eius duplum vel quadratum, siquidem x fuerit primus ad $4\,i$. Iam sumatur $x = 2\,a - p$ qui certe ad $4\,i$ est primus, ac prodit $4\,i + xx = 4\,i + 4\,a\,a - 4\,a\,p + p\,p$, quae forma, ob $4\,i + 4\,a\,a = 4\,p\,p$, transit in hanc: $4\,i + x\,x = 5\,p\,p - 4\,a\,p = p\,(5\,p - 4\,a)$, quod cum non sit numerus primus, neque duplum, neque quadratum primi, evidens est numerum $4\,i$ idoneum non esse.

Scholion.

§. 48. Quemadmodum igitur initio demonstravimus, in tabula numerorum idoneorum nullos alios quadratos

tos occurrere, praeter 1, 4, 9, 16 et 25, ita ex demonſtrationibus ſequentibus concludere poſſumus ex hac tabula omnes excludi numeros diviſibiles per quadratos 4^2, 3^2, 5^2, 7^2, 11^2, etc. praeter paucos illos in tabula relatos, ſcilicet nulli occurrunt ibi numeri per 16 diviſibiles, praeter 16, 48, 112 et 240; tum vero nulli per 9 diviſibiles praeter 9, 18, 45 et 72; at vero per 25 ſolus ipſe numerus 25 adeſt; maiora autem quadrata penitus ex iſta tabula excluduntur, non ſolum ipſa, ſed ne quidem factores eſſe poſſunt ullius numeri idonei. Interim tamen quod in iſta tabula omnes plane numeri idonei occurrant, eorumque numerus non ultra 65 exſurgat, rigida demonſtratio etiamnunc deſideratur. Quia autem usque ad decies mille nulli alii ſe mihi obtulerunt, multo magis veriſimillimum videtur, poſt hunc terminum nullos praeterea exiſtere; id quod eo magis eſt notatu dignum, quod nulla adhuc in Analyſi talis numerorum ſeries occurrit, quae finito tantum terminorum numero conſtaret.

DE