

DE
FORMVLIS SPECIEI

$$mxx + nyy$$

AD NVMEROS PRIMOS EXPLORANDOS IDONEIS,
EARVMQVE MIRABILIBVS PROPRIETATIBVS.

Auctore

L. EVLERO.

Conv. Acad. exhib. die 16 Mart. 1773.

§. I.

Hic praecipue respicio ad eam huiusmodi formularum proprietatem, qua constat omnes numeros, qui in tali formula $mxx + nyy$ 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 $x = 2$ II. Si $x = 4$ III. Si $x = 8$
 $y = 1$ $y = 5$ $y = 11$ 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 quispian numerus N duplici modo in formula $m x x + n y y$ continetur, ita ut sit $N = m a a + n b b = m c c + n d d$, 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 $\frac{r}{s} = \frac{m p p}{n q q}$ 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, binæ dabunt unum ipsius N factorem, binæ reliquæ vero alterum.

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

$$391 = 7 \cdot 7^2 + 3 \cdot 11^2, \text{ tum vero etiam}$$

$$391 = 7 \cdot 1^2 + 3 \cdot 12^2.$$

Hinc ergo erit $\frac{p}{q} = \frac{7+3}{11+12}$, cuius ergo quaterni valores erunt

$$\text{I. } \frac{p}{q} = \frac{1}{3}; \quad \text{II. } \frac{p}{q} = \frac{6}{7};$$

$$\text{III. } \frac{p}{q} = \frac{1}{3}; \quad \text{IV. } \frac{p}{q} = \frac{6}{7};$$

hinc iam porro deducantur sequentes fractiones:

$$\text{I. } \frac{r}{s} = \frac{7 \cdot 7^2}{3 \cdot 11^2} = \frac{21}{121}; \quad \text{II. } \frac{r}{s} = \frac{1 \cdot 1^2}{3 \cdot 12^2} = \frac{1}{432};$$

$$\text{III. } \frac{r}{s} = \frac{7 \cdot 1^2}{3 \cdot 12^2} = \frac{7}{432}; \quad \text{IV. } \frac{r}{s} = \frac{6 \cdot 6^2}{7 \cdot 7^2} = \frac{21}{49}.$$

Hic ergo prodit ubique $r + s$ numerus par, ideoque semissem

I.

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

§. 4. Contemplemur etiam sequens 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 $\frac{p}{q} = \frac{4+1}{13+12}$, cuius quatuor valores sunt.

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

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

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

$$\text{I. } \frac{r}{s} = \frac{5 \cdot 1^2}{3 \cdot 13^2} = \frac{1}{15}; \quad \text{II. } \frac{r}{s} = \frac{5 \cdot 5^2}{3 \cdot 1^2} = \frac{125}{3};$$

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

ergo formula $\frac{r+s}{2}$ ex primo et quarto dat factorem 8, e secundo vero et tertio factorem 64, quorum productum utique est 512.

§. 5. Verum idem hic numerus 512 infuper duabus aliis modis in eadem formula $5xx + 3yy$ continetur priori scilicet modo reperitur

$$512 = 5 \cdot 8^2 + 3 \cdot 8^2, \text{ posteriori vero modo}$$

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

hinc ergo plures alios factores reperire licebit, id quod in sum non est, quia numerus 512 pluribus modis in duos factores resolvi potest. Veluti prima et postrema resoluunt dant $\frac{p}{q} = \frac{10+1}{13+2}$, unde hae quatuor emergunt fractiones:

I. $\frac{p}{q} = \frac{11}{13}$; 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. $\frac{r}{s} = \frac{5 \cdot 11^2}{3 \cdot 13^2} = \frac{121}{135}$; 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; contem-
 plemur 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 inver-
 sam 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
 Nova Acta Acad. Imp. Scient. Tom. XII. D etiam

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, ita 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

D 2

divi-

divisore producti $m.n.$ 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 $m.n.$, quibus adeo certis casibus etiam potestates binarii ar numerare licet; vicissim sequitur omnes reliquos numeros quos revera compositos vocemus, qui in tali formula congrua $mxx + nyy$ 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 quenti modo eruuntur. Cum primo sit $\frac{p}{q} = \frac{10+2}{13+3}$, quater eius valores erunt 1°. $\frac{p}{q} = \frac{3}{4}$; 2°. $\frac{p}{q} = \frac{6}{5}$; 3°. $\frac{p}{q} = \frac{1}{2}$ 4°. $\frac{p}{q} = \frac{4}{5}$; unde porro altera fractio $\frac{r}{s} = \frac{m \cdot p \cdot p}{n \cdot q \cdot q}$ producit h valores: 1°. $\frac{r}{s} = \frac{15}{16}$; 2°. $\frac{r}{s} = \frac{12}{5}$; 3°. $\frac{r}{s} = \frac{5}{12}$ et 4°. $\frac{r}{s} =$ 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 caractere 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 $273 = 3 \cdot 7 \cdot 13$ 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 fit $C = mnaa + bb$; 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 hypothefin; unde necessario concludi oportet, quoties altera harum duarum

rum

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 phaenomenon maxime mirandum se obtulit, quod multitudo istorum numerorum neutiquam in infinitum excreseat, verum adeo non plures quam 65 huiusmodi numeros compleatur. 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 $1848 = 8 \cdot 3 \cdot 7 \cdot 11$, qui ergo felicissimo successu ad numeros primos explorandos adhiberi poterit. Si enim numerus quantumvis magnus N in forma $1848xx + yy$ 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 solus primus fuerit ad x , sed etiam ad ipsum 1848, tum tuto concludere licebit, istum numerum N revera esse primum. Huiusmodi nuper plures numeros primos, ad multos milliones exegentes, in medium protulimus, id quod multo minori laborae praestari potuit, quam si, uti olim feci, summa binorum quadratorum ad hunc finem uti vellemus. Talem autem elegantium usum reliqui omnes numeri idonei maiores huiusmodi praestabunt.

§. 20. Antequam autem in proprietates maxime memorabiles horum numerorum congruorum sum inquisitione conveniet praecipua momenta, quibus hi numeri innituntur breviter exponere, quae ternis sequentibus propositionibus complecti licet.

Propositio prima.

Nullus numerus minor quam $4mn$ plus uno n in formula $m^2x^2 + y^2$ contineri potest, nisi forte sit quadratus; quia enim numerus minor supponitur quam $4mn$ excluso casu $x = 0$ pro numeris quadratis necessario debet $x = 1$, atque adeo iste numerus non nisi unico modo in hac formula contineri potest.

Propositio secunda.

Si numerus compositus, quantumvis magnus, tantum modo in formula $m^2x^2 + y^2$ contineatur, tum per continuo multo minores numeri, pariter compositi, dari possunt unico etiam modo in hac forma contenti, quae 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 quolibet 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:

$$\begin{aligned}
 &48 \\
 &+ 1 = 49 = pp \\
 &+ 2^2 = 52 = 4 \cdot 13 = \delta p \\
 &+ 3^2 = 57 = 3 \cdot 19 = \delta p \\
 &+ 4^2 = 64 = 16 \cdot 4 = 2^\wedge \\
 &+ 5^2 = 73 = p \\
 &+ 6^2 = 84 = 12 \cdot 7 = \delta \cdot p
 \end{aligned}$$

$$\begin{aligned}
 &48 \\
 &+ 7^2 = 97 = p \\
 &+ 8^2 = 112 = 16 \cdot 7 = \delta \cdot p \\
 &+ 9^2 = 129 = 3 \cdot 43 = \delta \cdot p \\
 &+ 10^2 = 148 = 4 \cdot 37 = \delta \cdot p \\
 &+ 11^2 = 169 = 13 = pp
 \end{aligned}$$

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 ferie 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, 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, ficque 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 apprehenditur. 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 $i i$, formula congrua $i i x x + y y$ utique erit summa duorum quadratorum. Consideremus igitur numeros quoscunque compositos C , qui sint summae duorum quadratorum, quod cum semper duplici modo evenire queat, statuamus $C = a a + b b = c c + d d$, ac primo quidem fit a numerus par $= 2 f$, ut fit $C = 4 f f + b b$, ideoque b numerus impar, cuius quadratum cum semper fit formae $4 a + 1$, etiam ipse numerus C eandem habebit formam; unde evidens est, quadratorum $c c$ et $d d$ alterum par, alterum vero impar esse debere. Sit igitur $c = 2 g$, eritque $C = 4 g g + d d$; unde sequitur, si numerus compositus C fuerit $= 4 f f + b b$, eum quoque alio modo fore $C = 4 g g + d d$; ex quo manifestum est quadratum 4 esse numerum idoneum.

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

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

§. 29. Sit porro $a = 5f$, ideoque $C = 25ff + b.b$; et quia b divisionem per 5 non admittit, eius quadratum $b.b$ formam habebit $5a + 1$ vel $5a + 4$, 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 $5a + 0$, vel $5a + 2$, vel $5a + 3$, quarum nulla congruit; unde sequitur, alterutrum numerorum c et d per 5 esse divisibilem. Sit igitur $c = 5g$, ideoque $C = 25gg + d.d$; atque manifestum est, quoties numerus compositus C habuerit formam $25ff + b.b$, semper insuper alio modo fore $C = 25gg + d.d$, ideoque 25 esse numerum idoneum.

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

$6a + 1$ 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 $3a + 1$, ideoque cc
 formam $12a + 4$, five $6a + 4$; alterum vero quadratum dd
 formam habet $6a + 3$, quorum ergo quadratorum summa pro-
 ducit formam $6a + 1$, perinde ut ante. Quocirca cum, si fue-
 rit $C = 36ff + bb$, non necesse sit ut etiam fiat $C = 36gg$
 $+ dd$, hinc sequitur numerum 36 non esse numerum idone-
 um; quod etiam criterium primo datum declarat, quoniam
 $36 + 7^2 = 85 = 5 \cdot 17$. qui numerus revera est compositus
 et minor quam $4 \cdot 36$.

§. 31. Quo hoc clarius appareat, consideremus ca-
 sum $a = 7f_2$ ut sit $C = 49ff + bb$, ideoque b non divisibile
 per 7, unde forma ipsius bb erit $7a + 1, 2, 4$, quod etiam
 de ipso numero C valet. Videamus igitur num pro altera for-
 mula $cc + dd$ aliqua harum formarum resultare possit,
 etiam si neque c neque d per 7 sumatur divisibile, quo ergo
 casu tam cc quam dd haberet formam vel $7a + 1$, vel
 $7a + 2$ vel $7a + 4$, ideoque eorum summa ad has formas
 perducit $7a + 1, 2, 3, 4, 5, 6$, hoc est omnes formas pos-
 sibiles, in quibus superiores tres formae utique continen-
 tur. Quare cum nequaquam necesse sit, ut alter numerorum c
 et d etiam per 7 sit divisibilis, manifestum est etiam nu-
 merum 49 non esse idoneum; quod idem de numeris maio-
 ribus multo magis valebit, id quod etiam criterium nostrum
 manifesto declarat, cum sit $49 + 6^2 = 5 \cdot 17$, atque adeo $49 +$
 $4^2 = 5 \cdot 13$.

Theo

Theorema II.

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

Demonstratio.

§. 32. Sit brevitatis gratia $4a - 1 = i$, 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 $4a + 1$. Quia nunc i est numerus impar, alteruter numerorum c et d erit par, alter impar, unde duos casus evolvendi oportet. Sit primo $c = 2g$, et quia dd est formae $4a + 1$, hoc utique congruit cum forma praecedente. Examinemus vero etiam alterum casum, quo $d = 2h$, at cc impar, ideoque formae $4a + 1$; cum igitur sit $i = 4a - 1$, numerus icc formam habebit $4a - 1$, quae cum discrepet a forma priore $4iff + bb$, evidens est etiam numerum c parum esse debere. Sit igitur $c = 2g$, ut prodeat $C = 4igg + dd$, quam ob rem evidum est, si numerus compositus C formam habeat $4iff + bb$, necessario etiam alio modo proditurum esse $C = 4igg + dd$, sicque evidum est etiam numerum $4i$ esse idoneum, siquidem fuerit $i = 4a - 1$ numerus idoneus.

Corollarium.

§. 33. In tabula autem numerorum idoneorum supra allata alios numeros formae $4a - 1$ 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 $4i$ fit 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 $8a + 1$. Ponamus iam esse $a = 2f$, ut sit $C = 16iff + bb$, qui numerus est formae $8a + 1$. Quodsi iam c foret numerus impar, ob i numerum imparem, etiam icc erit impar, ideoque $4icc$ numerus formae $8a + 4$, unde ob $dd = 8a + 1$ forma posterior foret $8a + 5$, cum prior esset $8a + 1$; ex quo sequitur etiam numerum c necessario parem esse debere. Posito igitur $c = 2g$, erit utique $C = 16igg + dd$, unde manifesto sequitur numerum $16i$ quoque esse idoneum.

Corollarium.

§. 35. Quando autem assumimus numerum $4i$ esse idoneum, necesse est ut etiam ipse numerus i fit 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 $C = \lambda\lambda ia a + bb = \lambda\lambda icc + dd$; ubi

si ponamus $\lambda a = f$ et $\lambda c = g$, erit $C = iff + bb = igg + dd$, 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 $3a - 1$, etiam eius noncuplum semper erit numerus idoneus.

Demonstratio.

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

Corollarium.

§. 38. In tabula autem numerorum idoneorum alii numeri formae $3a - 1$ 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 $4a + 1$ fuerit numerus idoneus, tum eius quadruplum $4(4a + 1)$ in tabula numerorum idoneorum occurrere nequit.

Demonstratio.

§. 39. Posito brevitatis gratia $4a + 1 = i$ consideremus hanc aequalitatem: $C = iaa + bb = icc + da$ ubi ponamus $a = 2f$, ut sit $C = 4iff + bb$. Iam nisi absolute necessarium sit, ut etiam c sit numerus par, numerus $4i$ non erit idoneus. Consideremus igitur casum, quo c numerus impar, eritque $cc = 4a + 1$, ideoque icc forma $4a + 1$; quare cum hoc casu d sit numerus par, posterior forma erit $4a + 1$; unde patet necesse non esse, ut c sit numerus par, quod ipsum indicio est etiam numerum $4i$ non esse idoneum.

Corollarium.

§. 40. Numeri autem formae $4a + 1$, qui in nostra tabula numerorum idoneorum occurrunt, sunt 1, 5, 9, 17, 21, 25, 33, 37, 45, 57, 85, 99, 105, 133, 165, 177, 257, 273, 345, 357, 385, 1365, quorum etiam nullius quadruplum in nostra tabula deprehendimus, praeter unitatis, eius ratio est prorsus peculiaris.

Theorema VII.

Si inter numeros idoneos occurrat numerus imparis par, sive formae $4a + 2$, tum etiam semper eius quadruplum $4(4a + 2)$ in eadem tabula reperietur.

Demonstratio.

§. 41. Ponatur brevitatis gratia $4a+2=i$, et consideretur haec aequatio: $C=iaa+bb=icc+dd$, ac ponatur $a=2f$, quo facto, si etiam c necessario debet esse numerus par, evistum 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 $8a+1$, unde eorum differentia $bb-dd$ semper erit per octo divisibilis. Cum igitur sit $bb-dd=i(cc-4ff)$, neceffe 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 $i=4a+2$ 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 $16i$ esse idoneum, per se intelligitur etiam $4i$ 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 $i + aa = pp$, existente p numero primo, tum eius quadruplum $4i$ ex tabula numerorum idoneorum excluditur, existente $pp < 4i$.

Demonstratio.

§. 47. Quoniam $i + aa = pp$, erit $4i + 4aa = 4pp$. At sit $4i$ esset numerus idoneus, tum forma $4i + xx$ esse deberet vel numerus primus, vel eius duplum vel quadratum, siquidem x fuerit primus ad $4i$. Iam sumatur $x = 2a - p$ qui certe ad $4i$ est primus, ac prodit $4i + xx = 4i + 4aa - 4ap + pp$, quae forma, ob $4i + 4aa = 4pp$, transit in hanc: $4i + xx = 5pp - 4ap = p(5p - 4a)$, quod cum non sit numerus primus, neque duplum, neque quadratum primi, evidens est numerum $4i$ 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 exurgat, rigida demonstratio etiam nunc 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 Analyfi talis numerorum series occurrit, quae finito tantum terminorum numero constaret.
