1783

De criteriis aequationis $fxx + gyy = hz^2$, utrum ea resolutionem admittat nec ne?

Leonhard Euler

Multiplicetur per $d\Phi \,\text{fin.}\, \Phi^{-2n} \,\text{cof.}\, \Phi$ et integretur, erit

$$\int d\Phi \,\text{fin.}\, \Phi^{-2n} \,\text{fin.}\, 2n\Phi = \frac{n}{1(1-n)} \,\text{fin.}\, \Phi^{2-2n}$$
$$+ \frac{n(1-n)(1+n)}{1.2.3(2-n)} 2^2 \,\text{fin.}\, \Phi^{4-2n} + \text{etc.}$$

Statuatur pariter, integratione abfoluta, $\text{fin.}\, \Phi = \frac{1}{2}$, feu $\Phi = 30°$, ac prodibit feries $Q = 2^{1-2n} \int d\Phi \,\text{fin.}\, \Phi^{-2n} \,\text{fin.}\, 2n\Phi$. Quocirca feriei propofitae fumma ita exprimetur, vt fit

$$s = 2^{2n+1} \int d\Phi \,\text{fin.}\, \Phi^{2n-1} \,\text{cof.}\, (1-2n)\Phi$$
$$+ 2^{2-2n} \int d\Phi \,\text{fin.}\, \Phi^{-2n} \,\text{fin.}\, 2n\Phi$$

et quia haec fumma iam aliunde eft cognita, habebitur

$$\frac{\pi}{\text{fin.}\, n\pi} = 4\int d\Phi \,\text{cof.}\, (1-2n)\Phi (2 \,\text{fin.}\, \Phi)^{2n-1}$$
$$+ 4\int d\Phi \,\text{fin.}\, 2n\Phi (2 \,\text{fin.}\, \Phi)^{-2n}.$$

Corollarium 1.

§. 58. Si ponatur $2n = \frac{1-\lambda}{2}$, erit $1 - 2n = \frac{1+\lambda}{2}$, qua pofitione noftra aequatio fit concinnior, eritque

$$\frac{\pi}{\text{fin.}\, \frac{1-\lambda}{4}\pi} = 4\int \frac{d\Phi \,\text{cof.}\, \frac{1+\lambda}{2}\Phi}{(2 \,\text{fin.}\, \Phi)^{\frac{1+\lambda}{2}}} + 4\int \frac{d\Phi \,\text{fin.}\, \frac{1-\lambda}{2}\Phi}{(2 \,\text{fin.}\, \Phi)^{\frac{1-\lambda}{2}}} = \frac{\pi \sqrt{2}}{\text{cof.}\, \frac{\lambda\pi}{4} - \text{fin.}\, \frac{\lambda\pi}{4}}$$

pofito poft integrationem $\Phi = 30°$.

Corollarium 2.

§. 59. Simili modo fumto λ negatiue, erit

$$\frac{\pi}{\text{fin.}\, \frac{1+\lambda}{4}\pi} = 4\int \frac{d\Phi \,\text{cof.}\, \frac{1-\lambda}{2}\Phi}{(2 \,\text{fin.}\, \Phi)^{\frac{1-\lambda}{2}}} + 4\int \frac{d\Phi \,\text{fin.}\, \frac{1+\lambda}{2}\Phi}{(2 \,\text{fin.}\, \Phi)^{\frac{1+\lambda}{2}}} = \frac{\pi \sqrt{2}}{\text{cof.}\, \frac{\lambda\pi}{4} + \text{fin.}\, \frac{\lambda\pi}{4}}$$

vbi quidem notaffe iuuabit, omnibus cafibus, quos euoluere licet, eundem harum formularum integralium valorem actu reperiri, quem hic exhibuimus.

DE CRITERIIS AEQVATIONIS

$$fxx + gyy = hz^2$$

VTRVM EA RESOLVTIONEM ADMITTAT NEC NE?

§. 1.

Notum eft huiusmodi aequationem, pro varia relatione, quae inter numeros f, g et h intercedit, modo effe poffibilem modo impoffibilem, fiquidem pro x, y et z numeros rationales accipi oportet, atque adeo integros, quia fracti facillime ad integros reuocarentur. Ita notum eft hanc aequationem: $xx + yy = 2zz$ effe poffibilem; hanc vero: $xx + yy = 3zz$ impoffibilem. Quando autem litterae f, g et h maiores tenent valores, iudicium, vtrum aequatio fit poffibilis nec ne, difficulter inftituitur; in maximis vero numeris vix fufcipiendum videtur. Hic igitur conftitui in certa criteria inquirere, ex quibus iudicare liceat, vtrum haec aequatio fit poffibilis nec ne, quantumuis magni fuerint numeri f, g et h.

§. 2. Ante omnia autem fequentia notaffe iuuabit:

I°. Numeros f, g et h non folum integros affumo, fed etiam non-quadratos, neque etiam per quadratum diuifibiles; si enim numerus f haberet factorem quadratum, is in quadrato xx inuolui posset, quod etiam de reliquis tenendum.

II°. Praeterea hos numeros aeque negatiuos ac positiuos assumere licet; et quia aequatio ita semper disponi potest, vt membra fxx et hzz obtineant valores positiuos, solum membrum gyy relinquitur, quod vel positiuum vel negatiuum esse poterit.

III°. Numeros f et g tamquam primos inter se spectamus: si enim haberent communem diuisorem d; vel numerus h eundem habere deberet, quo casu ille per diuisionem tolleretur; vel quantitas z per d esset diuisibilis. Vnde si loco z scribamus dv, nostra aequatio ad hanc formam reduceretur: $fxx + gyy = dhvv$, ita vt nunc f et g futuri sint primi inter se.

IV°. Denique notandi sunt casus maxime obuii, quibus aequatio nostra fit possibilis. *Primo* scilicet hoc euenit si fuerit vel $h = f$, vel $h = g$: illo enim casu foret $y = 0$ et $z = x$, hoc vero $x = 0$ et $z = y$. Tum vero etiam casus satis obuius erit, si fuerit $h = f + g$, quia ei satisfieret, sumendo $z = x = y$. Minus obuii autem erunt casus, quibus $h = faa + gbb$; foret enim tum $x = a$, $y = b$ et $z = 1$.

§. 3. Primum autem inuestigabo, datis numeris f et g, cuiusmodi numeri pro h locum habere queant, vt aequatio fiat possibilis. Quare quum hic h vt numerum incognitum spectemus, aequationem nostram hac forma referamus: $fxx + gyy = hzz$, vt iam idoneos valores pro

dratum, is de reliquis
s ac positi- disponi po- s positiuos, sitiuum vel
se specta- ; vel nu- per diui- diuisibilis, l hanc for- vt nunc f
quibus ae- i fuerit vel et $z = x$, casus satis , sumendo , quibus et $z = 1$.
numeris f leant, vt numerum forma re- os valores pro

pro littera s inuestigari oporteat, quibus aequatio fiat possibilis, et quidem omnes qui hoc praestent, quem in finem sequentia Theoremata adiungo.

Theorema I.

Si casu $s = h$ possibilis fuerit aequatio $fxx + gyy = hzz$, ita vt litterae x, y, z iam sint cognitae, si vero insuper habeatur haec aequatio: $pp + fg.qq = krr$, tum nostra aequatio quoque erit possibilis casu $s = hk$.

Demonstratio.

Multiplicentur enim hae duae aequationes in se, et prodibit haec noua aequatio:

$$hkrrzz = (fxx + gyy)(pp + fgqq)$$
$$= f(px \pm gqy)^2 + g(py \mp fqx)^2.$$

Quare si statuamus

$$rz = Z,\ px \pm gqy = X \text{ et } py \mp fqx = Y,$$

nascitur haec aequatio propositae omnino similis:

$$fX^2 + gY^2 = hkZ^2.$$

Corollarium 1.

§. 4. Quodsi ergo litteres p et q ita assumere liceat, vt k obtineat factorem h, scilicet $k = hl$, tum ob $s = hhl$ nouus valor idoneus erit $s = l$, quoniam quadratum hh omittere licet.

Corollarium 2.

§. 5. Quemadmodum igitur ex illo valore idoneo $s = h$ erutus est alius $s = hk$, siue $s = l$, ita ex hoc simifimili modo alius nouus valor, puta $s = m$, hincque denuo nouus $s = n$ erui poterit; atque hanc determinationem in infinitum continuare licebit. Ita ex cafu quocunque cognito innumerabiles alii deriuari poterunt.

Corollarium 3.

§. 6. Si eueniat vt numeri b et k communem habeant diuiforem d, tum nouus valor fk factorem habebit dd, qui ergo expungi poterit. Hoc modo continuo ad minores numeros idoneos pro s peruenire licebit, donec tandem ad cafum obuium perducamur.

Corollarium 4.

§. 7. Hinc fi adhuc fuerimus incerti, vtrum b fit valor idoneus ipfius s, hoc autem modo procedendo perueniamus tandem ad cafum obuium, tuto concludere poterimus, etiam cafum $b = k$ effe poffibilem. Sin autem hoc nullo modo fuccedat, vel tandem in minoribus numeris ad eiusmodi cafum perueniatur, cuius impoffibilitas patefcat, etiam valor ipfe $b = k$ pro impoffibili erit habendus.

Theorema 2.

Si pro noftra aequatione tres innotefcant cafus poffibiles $s = b$, $s = b'$ et $s = b''$, tum etiam valor idoneus erit $s = b.b'.b''$.

Demonftratio.

§. 8. Quum igitur habeantur tres huiusmodi aequationes, quae fint:

hincque denuo
minationem in
cunque cogni-
dr
k communem
Fa factorem habe-
do continuo ad
vt icebit, donec
qu
tal
i, vtrum b fit
rocedendo per-
concludere po-
qu 1. Sin autem
Tl noribus nume-
poffibilitas pa-
libili erit ha-
b,
be
co fcant cafus pos-
valor idoneus
litt
$s =$ res huiusmodi
pl
I. fa

$$\text{I. } faa + gbb = b.cc$$
$$\text{II. } fAA + gBB = b'.CC$$
$$\text{III. } f.\alpha\alpha + g.\beta\beta = b''.\gamma\gamma,$$

ducatur prima in fecundam, et productum erit

$$bb'.ccCC = (faa + gbb)(fAA + gBB)$$
$$= (faA \pm gbB)^2 + fg(aB \mp bA)^2.$$

Faciamus nunc

$$cC = r \text{ et } faA \pm gbB = p \text{ et } aB \mp bA = q,$$

vt hoc productum fiat

$$pp + fgqq = bb'rr$$

quod denuo multiplicatum in tertiam aequationem dabit tale productum:

$$bb'b''rr\gamma\gamma = (f\alpha\alpha + g\beta\beta)(pp + fgqq)$$
$$= f(p\alpha \pm gq\beta)^2 + g(p\beta \mp fq\alpha)^2$$

quae forma cum plane conueniat cum propofita, veritas Theorematis eft manifefta, et cafus $s = bb'b''$ erit poffibilis.

Corollarium 1.

§. 9. Ex cognitis ergo tribus valoribus idoneis b, b', b'', quartus facile inuenitur. Ac fi forte illi terni habeant diuifores communes, hoc modo ad nouos valores continuo minores pertingere licebit.

Corollarium 2.

§. 10. Si ergo hunc nouum valorem indicemus littera b''', tum etiam valores idonei erunt $s = bb'b'''$, $s = bb''b'''$; $s = b'b''b'''$; ex quibus porro fimili modo plures alii deduci poffunt.

Co-

Corollarium 3.

§. 11. Quando autem hi noui valores per quadrata, vti praecepimus, deprimuntur, continuo iidem casus cogniti recurrent. Quum enim sit $b''' = b\,b'\,b''$, forma $b\,b'\,b''$ reducitur ad b'', haec vero: $b\,b''\,b'''$ ad b', et $b'\,b''\,b'''$ ad b, ita vt reuera vnus tantum casus nouus hoc modo reperiatur.

Theorema III.

Si aequationi nostrae $fxx + gyy = szz$ satisfaciat casus $s = b$, tum quoque omnes isti valores satisfacient:

$$s = 4fg + b;\; s = 8fg + b;\; s = 12fg + b;\; s = 16fg + b;\ \text{etc.}$$

quin etiam, si b fuerit numerus satis magnus, isti:

$$s = b - 4fg;\; s = b - 8fg;\; s = b - 12fg;$$

et in genere $s = b \pm 4nfg$, dummodo hi numeri fuerint primi.

§. 12. Huius elegantissimi Theorematis demonstratio adhuc desideratur, postquam a pluribus iam dudum frustra est inuestigata; cuius rei difficultas manifesto in hoc est sita: quod omnes hi numeri tum demum quaesito satisfaciant, quando sunt numeri primi. Quando enim sunt compositi euenire potest, vt non satisfaciant, etiamsi non semper a scopo aberrent. Quum autem hic tantum valeant numeri primi, probe notandum est, numeros negatiuos, qui ex formula $s = b - 4fg$ resultare possunt, non pro primis esse habendos. Quocirca plurimum is praestitisse erit censendus,

fendus, inuenire er quan casus forma i b', et nouus finitum rum pr numero z fatises fatis- fit possi forma: +b; etc. etiam t meri su fuerint Hos aut quadrat stratum, nstratio sium a ustra est bit sum est sita: composi sfaciant, mum p ompositi merorum emper a mulae f t numequi ex) primis erit cen- § satisfieri fendabit fo Euleri O

cui successerit demonstrationem huius Theorematis inuenire.

Corollarium 1.

§. 13. Quum hoc modo saltem ascendendo in infinitum progredi liceat, etiam multitudo valorum idoneorum pro s eo vsque augeri poterit, quo vsque Tabula numerorum primorum fuerit constructa.

Corollarium 2.

§. 14. Ita quum haec aequatio: $xx + yy = zz$, sit possibilis vbi est $f = 1$, $g = 1$ et $s = b = 1$, haec forma: $4n + 1$, quatenus scilicet praebet numeros primos, etiam totidem valores idoneos pro s suppeditabit, qui numeri sunt

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc.

Hos autem numeros omnes ipsos aequari summae duorum quadratorum, iam dudum rigorosissime a me est demonstratum, vnde eo minus de demonstratione reliquorum casuum desperare fas est. His igitur omnibus casibus licebit sumere $z = 1$. Interim tamen hinc etiam numeros compositos pro s inuenire licet, dum per Theorema primum producta ex binis vel pluribus horum ipsorum numerorum etiam pro s valebunt, quoniam binae illae formulae $fxx + gyy$ et $pp + fgqq$ hoc casu congruunt.

Corollarium 3.

§. 15. Quia aequationi $2xx + 3yy = szz$, satisfieri potest casu $s = 341$, alios casus idem praestantes dabit formula $341 \pm 24n$, quoties scilicet prodierint numeri

meri primi. Hinc ergo descendendo oriuntur sequentes valores:

341, 317, 293, 269, 197, 173, 149, 101, 53, 29, 5.

Hi autem omnes numeri ipsi iam in forma $1.xx + 3yy$ continentur, ita vt possit esse $z = 1$.

Scholion.

§. 16. Hoc Theoremate, quasi demonstratum esset, praemisso, pro quouis casu numerorum f et g omnes plane valores idonei litterae s facile inueniri poterant. Ad hoc autem ostendendum, duos casus separatim tractari oportet: priorem, quo $f = 1$, atque idcirco primi termini primi Theorematis inter se conueniunt; alterum vero, quo f non est vnitas. Vnde primo aequationem $xx + gyy = szz$ euoluemus.

Problema 1.

Proposita aequatione $xx + gyy = szz$, inuenire omnes valores idoneos pro s, quibus haec aequatio euadit possibilis.

Solutio.

§. 17. Hic statim euidens est valorem idoneum fore $s = g$; tum enim fit $x = 0$ et $y = z$. Etsi enim $4g$; $9g$; $16g$; etc. aeque satisfaciant, tamen omnes per quadratum depressi redeunt ad g. Verum sumto $y = 0$, omnes numeri quadrati pro s prodeunt, quos igitur omnes ad vnitatem reducere liceret. Sed quia praeter hos ipsos numeros etiam iidem, numeris $4ng$ siue aucti siue minuti satisfaciunt, quatenus scilicet prodeunt numeri primi, haec

haec quadrata hic negligere non licet. Iis autem tantum quadratis indigemus, quae ad numerum $4g$ fuerint primi, quia aliter nulli numeri primi inde emergerent; quamobrem statim omnia quadrata paria hinc excluduntur, et iis tantum imparibus locus conceditur, quorum radices ad numerum g fuerint primi. Semper ergo hic occurrit vnitas, tum vero etiam nouem, nisi g sit per 3 diuisibilis, porro etiam 25, nisi g diuisorem habeat 5, etc. Quando autem haec quadrata excedunt numerum $4g$, eorum loco scribantur residua ex diuisione per $4g$ remanentia. Ponamus ergo hinc prodire formulas:

$4ng + 1$; $4ng + a$; $4ng + b$; $4ng + c$; $4ng + d$; etc.

vbi scilicet a, b, c, d, ea residua, quae ex quadratis per $4g$ diuisis resultant. Verum praeter hos casus alius est obuius $s = 1 + g$, siquidem g fuerit numerus par; sin autem fuerit impar, sumatur $s = 4 + g$, vt scilicet habeatur numerus ad $4g$ primus. Tum vero quia per Theorema primum producta ex binis numeris satisfacientibus etiam satisfaciunt, habebimus insuper istas formulas, loco $1 + g$ vel $4 + g$ scribendo h:

$$s = 4ng + h;\ 4ng + ah;\ 4ng + bh;$$
$$4ng + ch;\ 4ng + dh;\ \text{etc.}$$

quos omnes valores coniunctim ita ob oculos constituamus:

$$s = 4ng + \begin{pmatrix} 1, & a, & b, & c, & d, & \text{etc.} \\ h, & ah, & bh, & ch, & dh, & \text{etc.} \end{pmatrix}$$

Quae omnes formulae eatenus valent, quatenus numeros primos producunt, hocque modo omnes plane numeri primi idonei reperientur; compositi autem nulla plane laborant difficultate, quum nascantur ex duobus pluribusue nu-

numeris primis idoneis. Quin etiam ipsum numerum g, eiusque producta per numeros iam inuentos, annumerari oportet.

Corollarium 1.

§. 18. Quia veritas huius solutionis nondum plane est euicta, casus aliquos obuios consideremus, quos semper in aliqua superiorum formularum contineri deprehendemus. Ita casus $s = 1 + 4g$ continetur in formula $4ng + 1$, et $s = 1 + 9g$ continetur in formula $4ng + b$, si fuerit $b = 1 + g$; at si $b = 4 + g$, in ea continebitur $s = 4 + 9g$. Similique modo res se habet in formulis $1 + 16g$; $1 + 25g$; $1 + 36g$; vel $4 + g$; $4 + 9g$; $4 + 25g$; etc. vbi eos casus, qui numeros primos producere nequeunt, excludimus.

Corollarium 2.

§. 19. Haec solutio aeque locum habet, siue g sit numerus positiuus, siue negatiuus. At quia hoc posteriori casu, in formulis inuentis littera b obtinet valorem negatiuum, loco terminorum b, ab, bb, cb etc. eorum complementa ad numerum $4g$ scribantur.

Corollarium 3.

§. 20. Casu quo g est numerus negatiuus, si iam fuerint inuentae formulae superiores, quae valent pro formula $xx - gyy$, si ibi signa mutentur, siue loco numerorum $1, a, b, c, d$, etc. scribantur eorum complementa ad $4g$, tum illae inseruient huic aequationi:

$$gyy - xx = szz.$$

Scho-

erum g, eius-
ari oportet.
nondum pla-
us, quos sem-
eri deprehen-
in formula
ula $4ng + b$,
ea continebi-
et in formu-
g; $4 + 9g$;
rimos produ-
bet, siue g sit
hoc posteriori
alorem nega-
eorum com-
atiuus, si iam
lent pro for-
loco nume-
plementa ad
Scho-

Scholion.

§. 21. Haec autem maxime illustrabuntur et facilius in vsum vocari poterunt, si plura exempla adiungamus, quibus etiam natura numerorum aliaeque abstrusae proprietates clarius perspicientur.

Exemplum 1.

Sit $g = 1$ et aequatio proposita $xx + yy = szz$, atque hic pro valoribus ipsius s vnica habetur formula $4n + 1$. Casus autem $1 + g = 2$, quia ad $4g$ non est primus, generali formulae innecti nequit; interim tamen seorsim praebet numerum idoneum $= 2$. Pro numeris igitur primis satisfacientibus praeter 2 habemus superiorem seriem:

1, 5, 13, 17, 29, 37, 41, etc.

et producta ex quocunque horum praebebunt omnes numeros compositos satisfacientes. At pro casu $g = -1$, seu aequatione $xx - yy = szz$, praeter formam $4n + 1$, ex quadratis ortam, formula $4 + g = 3$ dabit insuper hanc: $4n + 3$. Sicque omnes numeri primi in alterutra harum duarum formularum: $4n + 1$ et $4n + 3$ erunt contenti, ideoque omnes plane numeri primi hoc casu sunt idonei, quippe quos omnes in differentiam duorum quadratorum resoluere licet. Hinc quidem 2 excluditur, quoniam differentia duorum quadratorum esse nequit, attamen valorem pro s dari potest, siquidem pro z sumatur numerus par. Nam $2 \cdot 4$ vtique est $9 - 1$.

Exemplum 2

§. 22. Sit nunc $g = 2$ et proposita haec forma: $xx + 2yy = szz$, vbi quum sit $4g = 8$, quadrata imparia

paria 1, 9, 25, etc. omnia reducuntur ad eandem formam $8n+1$; at casus $1+g=h=3$ insuper dat hanc formam: $8n+3$, sicque omnes numeri primi hac specie referentur: $8n+(1,3)$, quibus accedit insuper $s=g=2$, sicque omnes hi numeri primi sunt

1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, etc.

At si sit $g=-2$, pro formula $xx-2yy=szz$ reperitur $s=8n+(1,7)$, quibus annumerari debet -2, atque hinc vicissim pro aequatione $2yy-xx=szz$, erit $s=8n+(7,1)$. Iidem ergo numeri pro his duobus posterioribus casibus valent.

Exemplum 3.

§. 23. Pro formula $xx+3yy=szz$ secundum praecepta data prodit $s=12n+(1,7)$, et insuper numerus solitarius 3. Pro formula autem $xx-3yy=szz$ reperitur $s=12n+(1)$.

Exemplum 4.

Pro formula $xx+5yy=szz$, reperitur $s=20n+(1,9)$, cum numero s; at pro formula $xx-5yy=szz$ reperitur $s=20n+(1,9)$, cum numero $-s$.

Exemplum 5.

Pro formula $xx+6yy=szz$ reperitur $s=24n+(1,7)$, vna cum numero 6; pro formula autem $xx-6yy=szz$ colligitur $s=24+(1,19)$, vna cum numero -6, vbi numeri ± 6 tamquam primi sunt spectandi, etiamsi in se sint compositi.

Scho-

eandem for- per dat hanc mi hac specie uper $s=g=2$,
9, 97, etc.
szz reperi- ebet -2, at- $=szz$, erit is duobus po-
szz secun- 7), et insuper $x-3yy=szz$
eritur $s=20n$ $x-5yy=szz$ $-s$.
eritur $s=24n$ ormula autem 19), vna cum rimi sunt spe-
Scho-

Scholion.

§. 24. Plura huiusmodi exempla non eucluimus, quum calculus satis sit perspicuus, sed potius Tabulam sequentem adiungimus, in qua pro quauis formula $xx+gyy=szz$, primo formam numerorum primorum pro s exhibebimus, deinde vero ipsos numeros primos vsque ad centum; quibus cognitis omnia producta, tam ex binis quam pluribus numeris primis, pro valore litterae s satisfaciunt:

$xx+yy=szz$	$s=4n+1$ cum 2
Num. primi	1, 2, 5, 13, 17, 29, 37, 41, etc.
$xx-yy=szz$	$s=4n+(1,3)$
Num. primi	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, etc.
$xx+2yy=szz$	$s=8n+(1,3)$ cum 2
Num. primi	2; 1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97
$xx-2yy=szz$	$s=8n+(1,7)$ cum -2
Num. primi	-2; 1, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97
$xx+3yy=szz$	$s=12n+(1,7)$ cum 3
Num. primi	3; 1, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, etc.
$xx-3yy=szz$	$s=12n+1$ cum solitario -3
Num. primi	-3; 1, 13, 37, 61, 73, 97
$xx+5yy=szz$	$s=20n+(1,9)$ cum numero 5
Num. primi	5; 1, 29, 41, 61, 89, etc.
$xx-5yy=szz$	$s=20+(1,9,11,19)$ cum numero -5
Num. primi	-5; 1, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, etc.
$xx+6yy=szz$	$s=24n+(1,7)$ cum numero 6
Num. primi	6; 1, 7, 31, 73, 79, 97, etc.
$xx-6yy=szz$	$s=24n+(1,19)$ cum -6
Num. primi	-6; 1, 19, 43, 67, 73, 97, etc.

$xx+$

$xx+7yy=szz$	$s=28n+(1,11,23,9,25,15)$ cum numero 7
Num. primi	7; 1, 11, 23, 29, 37, 43, 53, 67, 71, 79,
$xx-7yy=szz$	$s=28n+(1,9,25)$ cum -7
Num. primi	-7; 1, 29, 37, 43, 83, etc.
$xx+10yy=szz$	$s=40n+(1,9,11,19)$ cum 10
Num. primi	10; 1, 11, 19, 41, 59, 89, etc.
$xx-10yy=szz$	$s=40n+(1,9,31,39)$ cum -10
Num. primi	-10; 1, 31, 41, 71, 79, 89, etc.
$xx+11yy=szz$	$s=44n+\begin{pmatrix}1,9,25,5,37,\\15,3,23,31,27\end{pmatrix}$ cum 11
Num. primi	$+11$; 1, 3, 5, 23, 31, 37, 47, 53, 59, 67, 71, 89, 97
$xx-11yy=szz$	$s=44n+(1,9,25,5,37)$ cum -11
Num. primi	-11; 1, 5, 37, 53, 89, 97, etc.

Problema 2.

Propofita aequatione $fxx+gyy=szz$, inuenire omnes numeros primos, qui pro s valores idoneos praebent, quibus haec aequatio euadit poffibilis.

Solutio.

§. 25. Sit b valor quicunque idoneus pro z, et per Theorema nondum demonftratum patet, omnes numeros primos in hac formula contentos: $4nfg+b$, pariter pro s valere; ex quo manifeftum eft, iftum valorem b ad $4fg$ primum effe debere. Talis autem valor facile inuenitur. Si enim ambo numeri f et g fuerint impares, capi poterit $b=4f+g$, fiue $b=f+4g$; fin autem numerorum f et g alter fuerit par, alter impar, valor idoneus habetur $b=f+g$. Quo autem alii infoper numeri primi, atque adeo omnes, pro s obtineantur, confideretur formula $pp+fgqq=krr$, atque in problemate praecedente iam affignauimus omnes primos pro k valentes, qui fint $4nfg+(1, a, b, c, d, \text{etc.})$; nunc hae duae aequationes ducantur in fe et iam oftendimus prodire huiusmodi formam: $bkrrzz$, fiue $bkZ^2=fX^2+gY^2$, quocirca productum bk etiam dabit valorem idoneum pro s; vnde perfpicuum eft, omnes numeros primos pro s idoneos contineri debere in hac forma generali:

$$s=4nfk+(b, ab, bb, cb, db, \text{etc.}).$$

Cognitis autem numeris primis pro s valentibus, qui noftrae aequationi $fxx+gyy=szz$ fatisfaciunt, fi infuper omnes numeri primi pro k adhibendi innotefcant, qui fint A, B, C, D, etc., tum producta priorum pro s inuentorum in fingulos, vel binos, vel ternos etc. horum pofteriorum praebebunt etiam valores idoneos pro s, hocque adeo modo facile erit infinitos valores litterae x exhibere.

Corollarium 1.

§. 26. Si eueniat vt primus valor pro b inuentus fit quadratus, tum, quia is iam in ordine numerorum $1, a, b, c, d$, etc. continetur, iidem valores pro s locum habebunt, qui pro k funt affignati.

Corollarium 2.

§. 27. Sin autem numerus b in ordine $1, a, b, c, d$ non contineatur, tum nullo modo fieri poterit, vt valores pro s et k inter fe conueniant, fed omnes a fe inuicem difcrepabunt.

Exem-

Exemplum 1.

§. 28. Proposita sit aequatio $2xx + 3yy = szz$, vbi $f = 2$ et $g = 3$ primus autem valor $b = 5$. Tum ergo consideretur aequatio $pp + 6qq = krr$, et vidimus valores primos pro k contineri in hac formula: $24n + (1, 7)$. His igitur numeris $1, 7$ in $b = 5$ ductis, omnes numeri primi pro s in hac formula continentur: $24n + (5, 11)$, qui sunt: $5, 11, 29, 53, 59, 83$, etc.

Pro aequatione $2xx - 3yy = szz$, vbi $f = 2$ et $g = -3$, valor cognitus habetur $b = -1$, siue $b = 23$; at aequationi $pp - 6qq = krr$, pro k inuenta est formula $24n + (1, 19)$, vnde omnes numeri primi pro s fiunt: $24n + (5, 23)$, quae formula praebet hos numeros primos:

$5, 23, 29, 47, 53, 71$, etc.

Verum pro hac aequatione $3xx - 2yy = szz$, vbi $f = 3$ et $g = -2$, valor b fit $= 1$; et quia formula $pp - 6qq = krr$ eadem est quae ante, iidem etiam numeri primi pro s in formula $24n + (1, 19)$ continentur, hincque ipsi numeri primi: $24n + (5, 23)$, qui igitur fient: $5, 23, 29, 47, 53, 71$, etc.

Exemplum 2.

§. 29. Proposita aequatione $2xx + 5yy = szz$, vbi $f = 2$ et $g = 5$, primus valor b fit $= 7$, et quia aequationi $pp + 10qq = krr$, conuenit formula

$40.n + (1, 9, 11, 19)$,

pro valoribus primis ipsius s habebimus

$s = 40.n + (7, 23, 37, 13)$,

ergo ipsi numeri primi erunt

$7, 13, 23, 37, 47, 53$, etc.

At

At proposita aequatione $2xx - 5yy = szz$, fit statim $b = -3$; et quia pro aequatione $pp - 10qq = krr$ inuenimus formulam $40.n + (1, 9, 31, 39)$, numeri primi quaesiti continebuntur in hac formula:

$40.n + (37, 13, 27, 3)$

ergo ipsi numeri primi erunt:

$3, 13, 37, 43, 53, 67, 83$, etc.

Denique pro formula $5xx - 2yy = szz$, ob $b = 3$, ex iisdem numeris k numeri quaesiti pro s sunt:

$40.n + (37, 13, 27, 3)$.

Scholion 1.

§. 30. Quae hactenus iam tradita hisque exemplis illustrata sunt, omnes numeros primos pro s satisfacientes suppeditant, qui in se inuicem multiplicati, vti praecepimus, dant numeros compositos aeque satisfacientes. Neque vero hinc semper omnes plane numeri compositi pro s idonei obtinentur; sed dantur casus, quibus praeterea alii numeri primi in valores compositos ipsius s ingrediuntur. Caussa huius rei in eo consistit, quod in inuestigatione superiori numeros pares statim exclusimus, qui tamen, cum aliis numeris primis iuncti, quaesito satisfacere possunt. Ad hos ergo eruendos ponamus statim $s = 2b$, vt sit

$\frac{fxx + gyy}{2} = bzz$.

Quod si iam haec formula $\frac{fxx + gyy}{2}$ praebeat numerum imparem, siue productum ex impari in quadratum par, ex eo statim infinitos alios valores pro b elicere licet. Sit enim α eiusmodi numerus impar, et quum pro forma

xx

$xx + fgyy = szz$ omnes valores primi ipsius s in hac forma contineantur: $4fg + (1, a, b, c, d, \text{etc.})$, omnes numeri primi idonei pro nostra littera b in hac forma continebuntur:

$$4fg + (a, aa, ab, ac, ad \text{ etc.})$$

qui si fuerint diuersi ab iis, quos ante sumus affecuti, etiam infiniti alii habebuntur numeri primi, qui in compositionem numeri s ingredi possunt. Singuli enim isti numeri, quos litteris A, B, C, D, designemus, per 2 multiplicati, ideoneos praebent valores pro s, qui ergo erunt: $2a$, $2b$, $2c$, $2d$, etc. Et quia producta ex binis eorum etiam satisfaciunt, hinc nascentur numeri impares, ab, ac, ad, bc bd, cd, etc. Ita in exemplo $xx - 3yy = szz$, formula $\frac{zz - 1yy}{2}$ statim dat -1. Quum ergo pro hoc casu inuenta sit formula $s = 12n + 1$, pro valoribus ipsius b habebimus formulam $12n - 1$, siue $12n + 11$, quae praebet hos numeros primos:

$$11, 23, 47, 59, 71, 83,$$

qui duplicati omnes etiam satisfaciunt, atque etiam producta ex eorum binis, tum vero etiam producta ex his in singulos eorum, quos ante iam assignauimus; hocque pacto multitudo valorum compositorum vehementer augetur. Hoc praecipue iis casibus vsu venit, vbi formulae supra inuentae ex paucioribus membris constabant. Pro formula autem $xx + 7yy = szz$, eius dimidium $\frac{zz + 7yy}{2}$ praebet 4, siue $1 = a$, qui valor quum iam in formula supra data contineatur, hinc noui valores non oriuntur. At vero formula $\frac{zz - 7yy}{2}$ praebet $a = -3$, ideoque valores pro b erunt $28 . n + (25, 1, 9)$, qui numeri iam antea occurrunt. Hoc ergo probe obseruare oportet eum, qui etiam omnes nu-

s s in hac
nun mnes nu-
rit, c forma
affecuti,
tur in com-
mo enim isti
eo : is, per 2
tant qui ergo
Qua ex binis
mea impares,
iusn $x - 3yy$
prae ium ergo
num , pro va-
aditu $12n + 11$,
lior
tiam pro-
ta ex his
s nu ; hocque
rum iter auge-
inter formulae
s − f ant. Pro
ula supra
At vero
c. d, res pro b
tum occurrunt.
fa + im omnes
eritqu nu-

meros compositos pro s satisfacientes inuestigare voluerit, vnde huic negotio immorari superfluum foret.

Scholion 2.

§. 31. Quamtumuis autem haec egregia videantur, vtique hic erit dolendum, quod nondum firmis demonstrationibus sunt munita, cuius rei ratio potissimum in eo sita videtur, quod formulae pro s inuentae eatenus tantum valent, quatenus numeros primos suppeditant. Quamquam autem omnes labores a me suscepti spem meam fefellerunt, tamen spero, conatus meos iis, qui huiusmodi speculationibus delectantur, non fore ingratos, praecipue quia iam memoratam illam difficultatem circa numeros primos de medio sustuli, ita vt nunc sine dubio aditus ad illa numerorum mysteria non mediocriter facilior reddi videatur.

Propositio 1.

§. 32. Si fuerit $fxx + gyy = szz$, existente s numero primo, tum si omnia quadrata per hunc numerum s diuidantur et residua ex singulis enata notentur, inter ea semper occurret $-fg$, siue sublata negatione, $s - fg$.

Demonstratio.

Sint residua illa ex diuisione per s orta, $1, a, b, c, d$, etc. ac praebeat quadratum xx residuum a, quadratum vero yy residuum b, atque euidens est numerum $fa + gb$ per s fore diuisibilem. Sit ergo $fa + gb = \lambda s$, eritque $gb = \lambda s - fa$, ideoque $bg^2 = \lambda gs - fga$. Quum iam

iam omne residuum, in quadratum ductum, iterum inter residua occurrat, siquidem infra s deprimatur, prodeat inde residuum c, ita vt sit $c = \lambda g s - f g a$, et multiplo ipsius s sublato $c = - f g a$, siue $c = s - f g a$, et quia hoc aeque valet de omnibus residuis, loco a sumentes vnitatem habebimus: $c = - f g$, siue $c = s - f g$.

Corollarium 1.

§. 33. Si ergo satisfaciat valor $s = b$, quia formula $4 n f g + b$, si fuerit numerus primus, etiam satisfaciat pro s, si per hunc numerum omnia quadrata diuidantur, inter residua certo occurret $- f g$.

Corollarium 2.

§. 34. Sit ille diuisor $= D$, et quia datur quadratum, quod sit $p p$, vnde nascitur residuum $- f g$, manifestum est formulam $p p + f g$ diuisibilem fore per diuisorem D.

Corollarium 3.

§. 35. Hic autem iam manifesto inuoluitur difficilis illa conditio numeri primi, quia ordo residuorum hic memoratus locum non habet, nisi D sit numerus primus. Fieri enim vtique posset, vt $- f g$ non inter residua occurreret, si diuisor non esset primus.

Propositio 2.

§. 36. Si quadrata diuidendo per quemcunque numerum primum $D = 2 P + 1$ inter residua occurrat numerus r, tunc

tunc eius potestas r^P per D diuisa vnitatem relinquet; et viciſſim, si $r^P - 1$ diuisorem habeat D, numerum r inter residua reperiri necesse est.

Demonstratio.

Quum diuisor D ponatur $2 P + 1$, omnium numerorum ipso minorum multitudo est $2 P$, quorum quia semissis tantum in residua ingreditur, multitudo residuorum erit P. Deinde etiam certum est, si inter residua occurrat numerus r, tum quoque omnes eius potestates ibidem occurrere debere, quemadmodum simplicissima $r^0 = 1$ inest. Quocirca potestas r^P necessario non nouum residuum praebere potest. Atque hinc rite concluditur, inde ipsum primum residuum 1 prodire debere, sicque constat propositam potestatem r^P, per numerum primum D diuisam, residuum relinquere $= 1$. Quod ad inuersionem propositionis attinet, perpendamus, formulam $r^{2P} - 1$ perpetuo diuisibilem esse per $2 P + 1$; ex quo sequitur, vel formulam $r^P - 1$, vel $r^P + 1$ diuisibilem esse debere. Omnes ergo numeri pro r sumti, quibus formula posterior $r^P + 1$ fit diuisibilis, ex ordine residuorum excluduntur, atque illi tantum, qui formulam $r^P - 1$ diuisibilem producunt, relinquuntur, quorum numerus quum sit P, sequitur omnes numeros r fore residua.

Corollarium 1.

§. 37. Quum primus diuisor fuerit $= b$, ponamus $b = 2 p + 1$, et quia $r = - f g$, sequitur, formulam $(- f g)^p - 1$ per $b = 2 p + 1$ esse diuisibilem, seu fore $r^p = 1 + m (2 p + 1)$. Quum deinde etiam diuisor esse pos-

possit $b + 4nfg$, dummodo fuerit numerus primus, ob $b = 2p + 1$ faciamus

$$D = 2p + 1 + 4nfg = 2P + 1,$$

ita vt sit $P = p + 2nfg$, atque etiam haec potestas:

$$(-fg)^P = (-fg)^{p+2nfg}$$

vnitate minuta per diuisorem $2p + 1 + 4nfg$ euadet diuisibilis.

Corollarium 2.

§. 38. Quocirca totum negotium huc redit, vt, ponendo breuitatis gratia $-fg = r$, ostendatur, si formula $r^p - 1$ fuerit diuisibilis per $2p + 1$, tum etiam hanc formulam: $r^{p+2nr} - 1$, fore diuisibilem per $2p + 1 + 4nr$, siquidem numerus $2p + 1 + 4nr$ fuerit numerus primus.

Corollarium 3.

§. 39. Si ponamus $r = -1$, euidens est formulam $-1^p - 1$, diuidi non posse per $2p + 1$, nisi p sit numerus par. Sit ergo $p = 2q$ et $4q + 1$ numerus primus, tum certe inter residua reperietur $4q$. Sit quadratum, vnde hoc residuum nascitur $= vv$, et $vv + 1$ diuisibile erit per $4p + 1$. Ita ex his rationibus facillime patet, semper dari summam duorum quadratorum diuisibilem per numerum $4q + 1$, id quod alias per multas demum ambages ostendi solet.

§. 40. Missis autem his, quae principiis nondum satis corroboratis innituntur, per certa principia in indolem huiusmodi aequationum: $fxx + gyy = szz$, accuratius inquiramus. Ac primo quidem iam rigorose mon-

strai … mus, ob
sumto
etiam
misso … tas:
euadet
tum …
merum
dit, vt,
formula
anc for-
per b, … $+ 4nr$,
ductum … imus.
ita, vt
x et y
sponte … rmulam
t nume-
primus,
vnde … m, vnde
habebit … r $4p+1$.
haec fo … summam
Hoc v … $q + 1$,
conseq … solet.
b, in …
nondum
in indo-
z, accu-
tantum … se mon-
tionem … strai-
Eule

strauimus, si haec aequatio possibilis fuerit casu $s = b$, tum sumto numero k, ita vt sit $pp + fgqq = krr$, fore etiam $s = bk$ valorem idoneum pro s. Hoc igitur praemisso ad sequentia progrediamur.

Theorema I.

§. 41. Si aequatio $fxx + gyy = bzz$ fuerit possibilis, tum semper assignari potest talis formula: $tt + fg$, per numerum b diuisibilis, ita vt numerus t minor sit quam $\frac{1}{2}b$.

Demonstratio.

Quum formula illa $fxx + gyy$ diuisibilis sit per b, si ea ducatur in formulam $fpp + gqq$, etiam productum per b erit diuisibile. Sumantur ergo numeri p et q ita, vt sit $py - qx = 1$, id quod semper fieri potest, nisi x et y habeant communem diuisorem, qui autem casus hinc sponte excluditur; tum autem productum illud erit

$$(fpx + gqy)^2 + fg,$$

vnde sumto $t = fpx + gqy$ formula $tt + fg$ diuisorem habebit b. Hic autem ponamus $t = t' \pm \lambda b$, atque tum haec formula $t't' + fg$, etiamnunc per b erit diuisibilis. Hoc vero modo t' infra semissem numeri b deprimetur, consequenter certo dabitur formula $tt + fg$ diuisibilis per b, in qua t non excedit semissem ipsius b.

Corollarium 1.

§. 42. Haec eadem proprietas numeri b, quia tantum a producto fg pendet, aeque patet ad hanc aequationem: $xx + fgyy = bzz$. Quin etiam, si productum

 fg

fg in duos alios factores ζ et η resolui queat, ea lem conditio locum habet, vt aequatio $\zeta xx + \eta yy = bzz$ sit possibilis.

Corollarium 2.

§. 43. Quoties ergo numerus b fuerit diuisor formulae $tt + fg$, inde non semper concludi potest, aequationem $fxx + gyy = bzz$ esse possibilem, sed plus inde inferri nequit, quam dari formulam affinem $\zeta xx + \eta yy$ aequalem termino bzz, dummodo fuerit $\zeta\eta = fg$.

Corollarium 3.

§. 44. Quia $t < \frac{1}{2}b$ formula $tt + fg$, minor erit quam $\frac{1}{4}bb + fg$, quae ergo si diuidatur per b, quotus minor erit quam $\frac{1}{4}b + \frac{fg}{b}$.

Corollarium 4.

§. 45. Vicissim ergo etiam patet, si nulla detur huiusmodi formula per b diuisibilis, tum etiam neque hanc aequationem: $fxx + gyy = bzz$, neque vllam aliam adfinem $\zeta xx + \eta yy = bzz$ esse possibilem, si scilicet fuerit $\zeta\eta = fg$. Ad hoc ergo examinandum sufficit eos tantum casus euoluisse, quibus $t < \frac{1}{2}b$.

Theorema 2.

§. 46. Si aequatio $fxx + gyy = bzz$ fuerit possibilis, tum semper numerum b', minorem quam b, exhibere licet, ita vt haec aequatio: $fxx + gyy = b'zz$, sit possibilis.

Demon-

eat, ea lem
$yy = bzz$
diuisor for-
test, aequa-
ed plus in-
$\zeta xx + \eta yy$
$= fg$.
minor erit
b, quotus
nulla detur
neque hanc
n aliam ad-
scilicet fue-
eos tantum
it possibilis,
ibere licet,
possibilis.
Demon-

Demonstratio.

Si ponamus formulam $tt + fg = k$, supra iam demonstrauimus, etiam hanc formam: $fxx + gyy = bkzz$ esse possibilem. Modo autem vidimus pro t dari valorem adeo minorem quam $\frac{1}{2}b$, quo formula $tt + fg$ habeat factorem b. Sit ergo alter factor b' ideoque $k = bb'$ et $bk = b'b^2$, et deleto quadrato bb, vtpote in quadrato zz inuoluendo, oritur aequatio quoque possibilis:

$$fxx + gyy = b'zz, \text{ vbi } b' < \frac{1}{4}b + \frac{fg}{b}.$$

Corollarium 1.

§. 47. Quantuscunque ergo fuerit numerus b', hoc modo continuo ad minores valores b', b'', etc. peruenire licebit, donec tandem numeri prodeant tam parui, qui vlteriorem diminutionem non admittunt. Quia enim $b' < \frac{1}{4}b + \frac{fg}{b}$, vtique b' excedere debebit $\frac{fg}{b}$; vnde manifestum est, quo minor numerus b fuerit redditus, vlteriorem diminutionem retardari, atque adeo penitus sisti.

Corollarium 2.

§. 48. Si, dum hoc modo pro b continuo minores valores eruuntur, tandem perueniatur ad valorem vel f, vel g, hinc certo concludere poterimus, aequationem propositam esse possibilem, quandoquidem ista: $fxx + gyy = fzz$ casum maxime obuium inuoluit, scilicet $y = 0$ et $z = x$. Sin autem nullo modo deducamur ad f vel g, sed ad alium numerum ζ, diuisorem ipsius fg, indicio id erit, non ipsam aequationem propositam, sed aliam adfinem, scilicet $\zeta xx + \eta yy = bzz$ esse possibilem; vnde si tandem adeo

Gg 2 per-

perueniretur ad vnitatem, tum aequatio $xx + fgyy = bzz$ foret possibilis.

Problema.

§. 49. Proposita aequatione $fxx + gyy = bzz$, inuestigare, vtrum ea sit possibilis nec ne?

Solutio.

Quia hic tres numeri proponuntur, f, g et b, aequatio ita exhibeatur, vt numerus b eorum sit maximus, quandoquidem hic perinde est, vtrum termini aequationis sint positiui, an negatiui. Tum sumatur formula $tt + fg$, et examen instituatur, vtrum, pro t numeris minoribus quam $\frac{1}{2}b$ sumendis, haec formula fiat diuisibilis per b nec ne? Casu posteriore statim pronunciare poterimus, aequationem propositam esse possibilem; priore autem casu loco b nanciscemur alium numerum minorem b' simili modo examini subiiciendum, donec tandem vlterior diminutio non habeat locum. Et si inter hos valores occurrat f vel g, certum hoc erit indicium, aequationem propositam esse possibilem; sin autem ad alium numerum ζ, diuisorem producti fg, perueniamus, tum concludemus, aequationem $\zeta xx + \eta yy = bzz$ esse possibilem, existente $\zeta\eta = fg$. Quodsi autem neutrum vsu veniat, tum in valore minimo in locum b succedente acquiescamus, qui sit b', et nunc aequationem $fxx + gyy = b'zz$ ita disponamus, vt litterarum f et g maior, puta g, ad dextram referatur hoc modo: $b'zz - fxx = gyy$, et nunc loco g simili modo quaerantur g', donec perueniatur ad g' siue ipsi b' siue ipsi f aequalem, quo casu propositum nostrum itidem erit euic-

euictu $+ fgyy = bzz$
troduc
quatio
tanden
cium : $+ gyy = bzz$,
taediof onuntur, f, g
omnes us b eorum sit
laborei vtrum termini
cipio m sumatur for-
n, pro t nume-
rmula fiat diui-
im pronunciare
ssibilem; priore
puta m ierum minorem
mo ta ec tandem vlte-
faltem iter hos valores
deincep m, aequationem
ipsum um numerum ζ,
operati oncludemus, ae-
xistente $\zeta\eta = fg$.
alore minimo in
et nunc aequa-
$3xx$ - ius, vt littera-
ob $f =$ eratur hoc mo-
tur t pr g simili modo
manife siue ipsi b' siue
dit $b' =$ um itidem erit
vt for euic-

euictum. At si ne hoc quidem facile patescat, loco g introducamus valorem exiguum inde ortum g', et nunc aequatio $b'zz - g'yy = fxx$ simili modo tractetur; sicque tandem ad ternos numeros f', g', b' peruenietur, vt indicium nulla amplius difficultate laborare possit.

Corollarium 1.

§. 50. Si numerus b fuerit praegrendis, vtique taedioso calculo erit opus, antequam formulae $tt + fg$ omnes casus vsque ad $t = \frac{1}{2}b$ exigantur; vix autem talem laborem quisquam suscipiet. Admisso autem superiore principio statim valor iste b infra $4fg$ deprimetur.

Corollarium 2.

§. 51. Si ingens ille numerus b habeat factores, puta m et n, hic labor non parum subleuabitur, dum primo talis valor pro t inuestigatur, vt formula $tt + fg$ saltem diuisibilis fiat vel per m, vel per n; neque enim deinceps difficile erit casum elicere, quo ista formula per ipsum numerum b fiat diuisibilis. De caetero tota haec operatio exemplis clarius illustrabitur.

Exemplum 1.

§. 52. Examinanda proponatur haec aequatio: $3xx + 5yy = 1007zz$. Sumatur ergo formula $tt + 15$, ob $f = 3$ et $g = 5$, et quia $b = 1007 = 19 \cdot 53$, quaeratur t primo ita vt $tt + 15$ saltem diuisorem obtineat 19, quod manifesto fit sumendo $t = 2$; tum enim fit $k = 19$ et sic prodit $b' = 53$, sublato quadrato 19^2. Nunc porro quaeratur t, vt formula $tt + 15$ diuisorem nanciscatur 53, quod fit

si

si $t = 12$, ita vt iam habeamus $k = 159 = 3 . 53$, ideoque $b' k = 3 . 53^2$, sicque $b'' = 3$, qui numerus, quum aequalis sit ipsi f, indicat nostram formulam esse possibilem.

Exemplum 2.

§. 53. Proponatur haec aequatio: $2xx + 7yy = 23 . zz$. Hic $f = 2$, $g = 7$ et $b = 23$. Sumatur $k = tt + 14$, qui numerus fit diuisibilis per 23, sumendo $t = 3$. Erit autem $k = 23 . b$, ideoque $bk = 23^2$; vnde intelligimus, hanc aequationem: $xx + 14yy = zz$ esse possibilem; neque vero hinc sequitur propositam esse impossibilem, quum fieri possit vt vtraque simul locum habeat. Videamus ergo an haec forma: $2xx + 7yy = zz$ sit possibilis, quod quidem manifestum est, sumendo $x = 1$, $y = 1$ et $z = 3$. Sed tamen regula nostra vtamur, et quia est $b' = 1$, sumendo $t = 2$ erit $k = 18 = 2 . 3^2$, hinc $b' k = 2 . 3^2$, ideoque $b'' = 2$ hoc est $b'' = f$; sicque patet etiam ipsam propositam aequationem esse possibilem.

Corollarium.

§. 54. Quum ergo hoc casu vtraque forma $fxx + gyy = bzz$ et $xx + fgyy = bzz$ sit possibilis, operae pretium erit in eos casus inquirere, quibus vtraque formula $fxx + gyy$ et $xx + fgyy$ eidem termino bzz aequalis esse possit. Hoc autem manifesto eueniet, quando fieri poterit $fxx + gyy = uu + fgvv$, quod si euenire possit, infiniti certe exhiberi poterunt casus, inter quos dabitur vnus, quo $v = 0$. Illud igitur euenit, quoties euadere potest $fxx + gyy = uu$, id quod nostro exemplo manifesto fit.

Exem-

Exemplum 3.

§. 55. Proponatur aequatio $xx + 6yy = 145 zz = 5 . 29 . zz$. In formula ergo $k = tt + 6$ sumamus $t = 2$, vt fiat $k = 2 . 5$, ideoque $bk = 2 . 5^2 . 29$, sicque $b' = 2 . 29$. Nunc sumatur t ita, vt k fiat per 29 diuisibile, quod euenit sumendo $t = 9$: fiet enim $k = 87 = 3 . 29$, ergo $b' k = 2 . 3 . 29^2$ et $b'' = 6 . = g$, consequenter nostra aequatio est vtique possibilis.

Exemplum 4.

§. 56. Proponatur aequatio: $3xx + 7yy = 89 . zz$. Hic est $f = 3$, $g = 7$ et $b = 89$, ideoque $k = tt + 21$. Quaeratur ergo t, vt illa formula diuisibilis fiat per 89. Ponamus in hunc finem $tt + 84 = 89 . n$. Hic enim loco 21 scribere liceret $21 . uu$ in genere, atque hic sumsimus $u = 2$, vt etiam hunc casum illustramus. Quum autem nullum quadratum sit formae $3n + 2$, pro numero n excluduntur valores 1, 4, 7, 10, et in genere $3\alpha + 1$. Deinde excluduntur omnes numeri impariter pares 2, 6, 10, 14, etc. et quia omnia quadrata sunt formae vel $5\alpha + 3$, vel $5\alpha + 4$, pro n etiam excluduntur hi numeri: 3, 4, 8, 9, 13, 14, et in genere $5\alpha + 3$ et $5\alpha + 4$. His exclusis pro n remanent examinandi hi numeri: 5, 11, 12, 15, 17, 20, 21, 27, 32, 35, 36, 41, quos ergo successiue in aequatione $tt = 89 . n - 84$, loco n substitui oportet. At vero primus valor $n = 5$ statim praebet quadratum, vnde $k = 5 . 89$ et $b' = 5$. Nunc autem k per 5 fiet diuisibile sumendo $t = 1$, vnde fit $k = 5 . 17$ et $b'' = 17$. Quia ergo neque ad 3, neque ad 7 peruenimus, sumto $b' = 5$ examinemus aequationem $5zz - 3xx = 7yy$, atque iam tota ope-

operatio est mutanda, dum habemus $f = 5$, $g = -3$ et $b = 7$, quocirca, posito $k = tt - 15$, sumamus $t = 1$, vt fiat $k = -2.7$, vnde fit $b' = -2$, ita vt nunc aequatio examinanda sit haec $5zz - 3xx = -2yy$, siue $3xx - 2yy = 5zz$, vbi $f = 3$, $g = -2$ et $b = 5$. Sumto ergo $k = tt - 6$, fiat $t = 1$ erit $k = -5$ et $b' = -1$, ergo peruenimus ad hanc aequationem: $3xx - 2yy = -zz$, siue $2yy - zz = 3xx$, vbi habemus $f = 2$, $g = -1$, $b = 3$. Erit ergo $k = tt - 2$, quod quum nullo modo fieri possit, omnes istae aequationes ideoque et ipsa proposita sunt impossibiles.

Exemplum 5.

§. 57. Sit proposita aequatio $3xx + 7yy = 178zz$, vbi vt antea $f = 3$, $g = 7$, at $b = 178 = 2.89$, duplo maior quam casu praecedente. Posito ergo $k = tt - 21$, ex praecedente patet pro t sumi debere 23. Posito igitur $tt = 81.n - 21$ pro n relinquuntur numeri:

5, 8, 9, 14, 18, 20, 24, 29, 30, 33, 38, 44.

Reperitur autem $n = 14$, vnde fit $t = 35$, sicque erit $k = 14.89$, hincque $b' = 2.14 = 4.7$, ideoque $b' = 7$, qui numerus quum ipsi numero g sit aequalis, indicat aequationem nostram esse possibilem.

Problema.

§. 58. Postquam aequatio $fxx + gyy = bzz$ methodo praecedente possibilis fuerit inuenta, dum tandem valores ex b inuenti perducti fuerint ad f, siue ad g, determinare ipsa quadrata xx et yy, quibus aequatio euadit possibilis.

Solu-

Solutio.

Quia solutio praecedens ad sequentes formulas est perducta:

$$k = aa + fg = bb'; \quad k' = bb + fg = b'b'';$$
$$k'' = cc + fg = b''b'''; \text{ etc.}$$

habebimus $bk = b^2 b' = b'.\square$, hincque $bk^2 = b'k\square$. Simili modo reperiemus

$$b'.\square = b''k', \text{ item } b''.\square = b'''k''; \text{ etc.}$$

Sit nunc $b''' = f$, erit $b'' = f.k''$, hinc $b'\square = f.k''.k'$, ac tandem $b.\square = fk.k'.k''$, consequenter habebimus $b\square$ hoc est

$$bzz = f(aa + fg)(bb + fg)(cc + fg)(dd + fg) \text{ etc.}$$

quod productum manifesto reducitur ad $f(A^2 + fgB^2)$, ita vt hinc fiat $bzz = fA^2 + ffgB^2$, quocirca nanciscimur $x = A$ et $y = fB$, sicque Problema est resolutum.