1802

De variis modis numeros praegrandes examinandi, utrum sint primi necne?

Leonhard Euler

DE VARIIS MODIS NUMEROS PRAEGRANDES EXAMINANDI, UTRUM SINT PRIMI NEC NE?

Auctore *L. EVLERO*.

Conventui exhibuit die 16 Mart. 1778.

§. 1.

Cum nimis molestum et operosum esset, hoc examen principia vulgaria instituere, dum scilicet divisio tent per omnes numeros primos radice quadrata numeri prop minoribus: plurimum interesit ejusmodi methodos trad quarum ope hoc negotium multo facilius et brevius ex diri queat. Tales autem methodi innituntur potissimum quenti propositioni: *Si numerus* N *duplici modo conti tur in tali formula*: $\alpha xx + \beta yy$, *vbi* α *et* β *sunt numeri quicunque, tum certum est, illum numerum* N *non esse mum, atque adeo eius divisores facile investigari poterunt*

§. 2. Ponamus igitur numerum quemcunque proposit N duplici modo in hac formula $\alpha xx + \beta yy$ contineri, primo quidem esse $N = \alpha aa + \beta bb$, tum vero et $N = \alpha AA + \beta BB$. Jam a priori aequatione per BB mu plicata auferatur altera per bb multiplicata, vt obtinea haec aequatio: $N(B^2 - bb) = \alpha(aaB^2 - A^2bb)$, quae factores ita referri potest:

$$N(B + b)(B - b) = \alpha(aB + Ab)(aB - Ab),$$

vn

[illegible]as patet, numerum N primum esse non posse, sed [illegible] communem factorem habere, tam cum formula $aB + Ab$ [illegible] cum formula $aB - Ab$, quandoquidem istae formu[illegible] diversae sunt a prioribus $B + b$ et $B - b$.

§. 3. Quo haec conclusio clarius perspiciatur, eam aliquot exemplis illustremus. Sit scilicet $N = 77$, qui numerus duplici modo in forma $5xx + 2yy$ continetur; primo enim est $N = 5 \cdot 1^2 + 2 \cdot 6^2$, tum vero etiam $N = 5 \cdot 3^2 + 2 \cdot 4^2$, sicque habebimus $a = 1$, $b = 6$, $A = 3$ et $B = 4$, hincque $aB + Ab = 22$; cum quo numero numerus propositus N factorem habet communem 11. Altera formula fit $aB - Ab = 14$, cum quo numero numerus N factorem communem habet 7. Sicque jam nacti sumus factores numeri propositi N, qui sunt 7 et 11.

§. 4. Sit numerus propositus 703, qui duplici modo in forma $7xx + 3yy$ continetur; primo enim est

$$N = 7 \cdot 2^2 + 3 \cdot 15^2, \text{ tum vero est etiam}$$
$$N = 7 \cdot 10^2 + 3 \cdot 1^2.$$

Prior formula dat 52, cujus numeri cum 703 maximus communis divisor est 19; at vero numerus 703 cum altera formula 148 divisorem habet communem 37. Est vero utique $703 = 19 \cdot 37$. Hoc etiam inde facilius patet, quod sit $152 = 8 \cdot 19$, unde, quia 8 nullum factorem ipsius 703 continet, necesse est ut 19 ejus sit factor. Simili modo cum $148 = 4 \cdot 37$; ob eandem rationem necesse est ut 37 sit factor numeri 703.

§. 5. Consideremus numerum majorem 12091 duplici modo in forma $7xx + 11yy$ contentum. Hic cum sit

$$1^0)\quad 12091 = 7 \cdot 40^2 + 11 \cdot 9^2,$$
$$\text{tum vero etiam}\quad 2^0)\quad 12091 = 7 \cdot 4^2 + 11 \cdot 33^2,$$

hinc

hinc forma examinanda $40 \cdot 30 \pm 4 \cdot 9$, quae per 12 div[...] dat 110 ± 3. Nunc autem eſt 113 primus, ideoque fa[...] numeri propoſiti; deinde etiam 107 pariter eſt primus, p[...] pterea etiam factor; revera autem eſt $12091 = 113 \cdot 10$[...]

Theorema I.

Si fuerit tam $N = \alpha a^2 + \beta b^2$ *quam* $N = \alpha A^2 + \beta$[...] *tum formulae* $aB + Ab$, *et* $aB - Ab$ *praebent facto*[...] *numeri* N, *poſtquam ſcilicet per numeros, qui factores* [...] *nequeunt ipſius* N, *fuerint diviſae.*

§. 6. Poſſunt vero etiam ex binis reſolutionibus [...] pra exhibitis numeri N aliis modis factores inveſtigari, [...] licet a priori ducta in αA^2 ſubtrahatur, poſterior ducta [...] βbb, vt prodeat

$$N(\alpha A^2 - \beta B^2) = (\alpha\alpha a^2 A^2 - \beta\beta b^2 B^2)$$
$$= (\alpha a A + \beta b B)(\alpha a A - \beta b B)$$

vnde patet, ambas has formulas factores continere numeri [...] id quod per ſuperiora exempla etiam illuſtremus.

§. 7. In exemplo §. 3 erat

$$77 = 5 \cdot 1^2 + 2 \cdot 6^2,$$
et $$77 = 5 \cdot 3^2 + 2 \cdot 4^2,$$

vnde colligitur forma $5 \cdot 1 \cdot 3 \pm 2 \cdot 6 \cdot 4$, quae per 3 [...] preſſa fit $5 \cdot 1 \pm 4 \cdot 4$. Hinc oriuntur iſti duo numeri 21 et [...] quorum prior per 3 diviſus dat 7.

Exemplum §. 4. allatum erat $703 = 7 \cdot 2^2 + 3 \cdot 1$[...] et $703 = 7 \cdot 10^2 + 3 \cdot 1^2$, vnde forma oritur $7 \cdot 2 \cdot 10 \pm 3 \cdot 1$[...] quae per 5 depreſſa dat 28 ± 9, ideoque tam 37 quam [...] ſunt factores numeri propoſiti 703 ſupra inventi.

Terti[...]

Tertium exemplum §. 5. erat $12091 = 7 \cdot 40^2 + 11 \cdot 9^2$, $12091 = 7 \cdot 4^2 + 11 \cdot 33^2$, unde oritur haec formula: $7 \cdot 40 \cdot 4 \pm 11 \cdot 9 \cdot 33$, ex qua pro ſigno ſuperiori oritur 4387, qui numerus cum numero propoſito diviſorem habet communem 107. Deinde pro ſigno inferiori fit 2147, qui cum numero propoſito diviſorem habet communem 113, ut ante.

Theorema II.

Si fuerit tam $N = \alpha aa + \beta bb$ quam $N = \alpha A^2 + \beta B^2$, tum etiam tam iſta formula $\alpha a A + \beta b B$, quam $\alpha a A - \beta b B$, cum numero propoſito N communem habebit diviſorem, unde ejus factores innoteſcent.

§. 8. Hinc autem deducuntur aliae formulae imprimis memorabiles, quae cum ipſo numero N communes habebunt factores. Additis enim binis illis formulis, vt habeatur $2N = \alpha(aa + A^2) + \beta(bb + B^2)$, huc addatur formula ante inventa bis ſumpta $2\alpha a A \pm 2\beta b B$, vel etiam ſubtrahatur; quoniam enim cum ipſo numero N communem habet factorem, idem factor communis in membro dextro contineri debebit. Hoc modo obtinebitur

$$2N \pm 2\alpha a A \pm 2\beta b B = \alpha(a \pm A)^2 + \beta(b \pm B)^2,$$

quae forma ideo eſt notabilis, quia ipſi formae propoſitae eſt ſimilis, et quia quatuor variationes in illa locum habent, totidemque modis etiam factores numeri propoſiti aſſignari poterunt.

§. 9. Quodſi ambae formulae $a \pm A$ et $b \pm B$ habeant factorem communem, quoniam is in N contineri nequit, eum ſtatim e medio tolli conveniet. Veluti ſi haec fractio $\frac{a \pm A}{b \pm B}$ reducatur ad hanc formam ſimpliciſſimam $\frac{p}{q}$, tum iſta formula $\alpha pp + \beta qq$ factorem numeri propositi praebebit, quippe qui erit communis divisor hujus ipsius formulae cum numero proposito N.

§. 10. Illustremus etiam hanc methodum per exempla supra allata, in quorum primo erat

$77 = 5 \cdot 1^2 + 2 \cdot 6^2$ et

$77 = 5 \cdot 3^2 + 2 \cdot 4^2$, unde formetur fractio

$\frac{p}{q} = \frac{3 \pm 1}{6 \pm 4}$, atque formula $5pp + 2qq$ dabit divisorem ipsius 77. Hinc autem erit 1°) $\frac{p}{q} = \frac{2}{5}$, tum vero formula $5 \cdot 4 + 2 \cdot 25$ per 10 depressa, dat $2 + 5 = 7$.

2°) fit $\frac{p}{q} = 2$, hincque $20 + 2 = 2 \cdot 11$.

3°) fit $\frac{p}{q} = \frac{1}{5}$, hincque formula $5 \cdot 1 + 2 \cdot 25$, per 5 depressa dat $1 + 2 \cdot 5 = 11$. Tandem erit 4°) $\frac{p}{q} = 1$ et formula $5 \cdot 1 + 2 \cdot 1 = 7$.

§. 11. Simili modo pro secundo exemplo, quo erat

$703 = 7 \cdot 2^2 + 3 \cdot 15^2$ et

$703 = 7 \cdot 10^2 + 3 \cdot 1^2$, habebimus

$\frac{p}{q} = \frac{10 \pm 2}{15 \pm 1}$ et formula $7pp + 3qq$ dabit factorem numeri 703. Hinc fit 1°) $\frac{p}{q} = \frac{3}{4}$ et factor $7 \cdot 9 + 3 \cdot 16$, per ternarium depressa, erit $7 \cdot 3 + 16 = 37$. Porro 2°) fit $\frac{p}{q} = \frac{6}{7}$ et formula $7 \cdot 36 + 3 \cdot 49$, per $7 \cdot 3$ depressa, dat factorem 19. Jam 3°) fit $\frac{p}{q} = \frac{1}{2}$, unde formula $7 \cdot 1 + 3 \cdot 4$ dat factorem 19. Tandem 4°) fiet $\frac{p}{q} = \frac{4}{7}$, unde formula $7 \cdot 16 + 3 \cdot 49$, per 7 depressa, praebet factorem 37.

§. 12. Tertium denique exemplum erat

$12091 = 7 \cdot 40^2 + 11 \cdot 9^2$ et

$12091 = 7 \cdot 4^2 + 11 \cdot 33^2$, ex quo fit

$\frac{p}{q} = \frac{40 \pm 4}{33 \pm 9}$ et formula $7pp + 11qq$ dabit: 1°) $\frac{p}{q} = \frac{22}{21}$; hinc formula $7 \cdot 22^2 + 11 \cdot 21^2$, per $7 \cdot 11$ depreſſa, dabit factorem 107. Erit 2°) $\frac{p}{q} = \frac{11}{6}$, hinc forma $7 \cdot 11^2 + 11 \cdot 6^2$, per 11 depreſſa, dat factorem 113. Porro fit 3°) $\frac{p}{q} = \frac{6}{7}$, hinc formula $7 \cdot 6^2 + 11 \cdot 7^2$, per 7 depreſſa, praebet factorem 113. Tandem erit 4°) $\frac{p}{q} = \frac{3}{2}$, unde formula $7 \cdot 3^2 + 11 \cdot 2^2$ ſtatim dat factorem 107.

Theorema III.

***Si fuerit tam** $N = \alpha aa + \beta bb$ quam $N = \alpha A^2 + \beta B^2$, **hincque** formetur fractio $\frac{p}{q} = \frac{a \pm A}{b \pm B}$; tum iſta formula $\alpha pp + \beta qq$ ſemper continebit factorem numeri propoſiti N, **qui** ſcilicet vel ipſe ſe prodit, vel facta diviſione ſive per α, **ſive per** β, ſive per $\alpha\beta$, quandoque etiam per alium numerum ſimpliciſſimum 2, ejusve poteſtatem.*

Demonſtratio.

§. 13. Cum ſit $\alpha aa + \beta bb = \alpha A^2 + \beta B^2$, erit $\alpha(aa - A^2) = \beta(BB - bb)$, hincque $\frac{a + A}{B + b} = \frac{\beta(B - b)}{\alpha(a - A)}$. Sit nunc $\frac{p}{q}$ fractio ſimpliciſſima huic vtrique formulae aequalis, ac pro priore ponatur $a + A = mp$ et $B + b = mq$, pro poſteriore vero ſit $\beta(B - b) = \alpha\beta np$ et $\alpha(a - A) = \alpha\beta nq$, unde ergo fiet $B - b = \alpha np$ et $a - A = \beta nq$. Ex his quatuor aequalitatibus definiantur numeri a, A et b, B, qui erunt $a = \frac{mp + \beta nq}{2}$; $A = \frac{mp - \beta nq}{2}$; $B = \frac{mq + \alpha np}{2}$ et $b = \frac{mq - \alpha np}{2}$. Cum nunc ſit $N = \alpha aa + \beta bb$, reperietur facta ſubſtitutione

$$N = \tfrac{1}{4}\,\alpha(mp + \beta nq)^2 + \tfrac{1}{4}\,\beta(mq - \alpha np)^2$$

ſive

fiue per factores

$$N = \tfrac{1}{4}\,\alpha\,(mmpp + \beta\beta nnqq) + \tfrac{1}{4}\,\beta\,(mmqq + \alpha\alpha nnpp),$$

quae forma reducitur ad hoc productum:

$$\tfrac{1}{4}\,(mm + \alpha\beta nn)\,(\alpha pp + \beta qq).$$

Unde patet formulam $\alpha pp + \beta qq$ continere diuiforem nume
fimul vero etiam patet quotum hinc ortum effe formae $mm + \alpha\beta$

§. 14. Evidens autem eft in hac demonftratione li
ras α et β fupponi pofitivas; fi enim altera effet nega
evenire poffet, vt factor inventus $\alpha pp + \beta qq$ abiret in
tatem, id quod unico exemplo oftendiffe fufficiet, quo
$7 = 2 \cdot 8^2 - 1 \cdot 11^2$ et $7 = 2 \cdot 22^2 - 1 \cdot 31^2$. Hic ergo
$N = 7$, ideoque numerus primus; tum vero $\alpha = 2$; $\beta =$
$a = 8$; $b = 11$; $A = 22$ et $B = 31$, unde fit
$\frac{p}{q} = \frac{22 \pm 8}{31 \pm 11}$, ita ut quatuor fractiones hinc ortae fint 1°) $\frac{p}{q}$
2°) $\frac{p}{q} = \frac{3}{2}$; 3°) $\frac{p}{q} = \frac{1}{3}$; et 4°) $\frac{p}{q} = \frac{7}{10}$, ergo formulae $2pp$
valores erunt 1°). 1, 2°). 14, qui poftremus, per 2
preffus, dat 7; 3°). 7. et 4°). 2, qui poftremus redigitur a
Evidens autem eft litteras a et A; b et B pro lubitu
pofitive quam negative accipi poffe.

Theorema IV.

*Si duo numeri M et N ejusdem formae $\alpha xx + \beta y$
fe invicem multiplicentur, productum MN femper erit fo
$\alpha\beta xx + yy$, idque duplici modo.*

Demonftratio.

§. 15. Si enim ponamus $M = \alpha pp + \beta qq$ et $N = \alpha rr +$
tum facta multiplicatione reperitur $MN = \alpha\alpha pprr + \beta\beta q$
$\alpha\beta ppss + \alpha\beta qqrr$, quod productum manifesto reducitur ad h
formam:

M

$MN = \alpha\beta(ps \pm qr)^2 + (\alpha pr \mp \beta qs)^2$, hoc eſt ad formam $\alpha\beta xx + yy$, exiſtente $x = ps \pm qr$ et $y = \alpha pr \mp \beta qs$; unde ſimul patet, hanc reſolutionem ſemper duplici modo fieri poſſe.

Theorema V.

Si duo numeri M *et* N, *quorum alter* M *ſit formae* $\alpha xx + \beta yy$, *alter vero* N *formae* $\alpha\beta xx + yy$, *in ſe invicem ducantur, productum* MN *ſemper erit formae* $\alpha xx + \beta yy$, *idque duplici modo.*

Demonſtratio.

§. 16. Si enim ponamus $M = \alpha pp + \beta qq$ et $N = \alpha\beta rr + ss$, facta multiplicatione reperitur $MN = \alpha\alpha\beta pprr + \beta qqss + \alpha\beta\beta qqrr + \alpha ppss$, quod productum manifeſto reducitur ad hanc formam: $MN = \alpha(\beta qr \pm ps)^2 + \beta(\alpha pr \mp qs)^2$, ideoque eſt formae $\alpha xx + \beta yy$, exiſtente $x = \beta qr \pm ps$ et $y = \alpha pr + qs$, quae ergo reſolutio, ob ſigna ambigua, ſemper duplici modo inſtitui poteſt.

§. 17. Hic animadvertiſſe juvabit, binas formulas $\alpha xx + \beta yy$ et $\alpha\beta xx + yy$ arctiſſimo vinculo inter ſe eſſe conjunctas, quod etiam inde patet, quod alteram in alteram facillime convertere liceat. Si enim in priore formula ponatur $x = \beta z$, ea abit in $\beta(\alpha\beta zz + yy)$; ac in altera ſi ponatur $y = \alpha v$, tum ea accipiet hanc formam: $\alpha(\beta xx + \alpha vv)$. Infra autem multo clarius patebit, ambas iſtas formulas paribus proprietatibus eſſe praeditas, ita vt, quod de una demonſtrabitur, id etiam de altera locum habere queat.

§. 18. Cum igitur demonſtratum ſit, omnes numeros, qui duplici modo in tali forma $\alpha xx + \beta yy$ continentur, certe

non

non eſſe primos, atque adeo eorum factores ſemper aſſignan
poſſe: nunc quaeſtio maximi momenti ſe offert, num om
nes numeri, qui unico tantum modo in tali formula conti
nentur, etiam ſemper pro primis haberi queant? Hoc au
tem pendet a natura formulae $\alpha xx + \beta yy$, ſive a numeri
α et β, quorum duo genera conſtitui debent. Dantur enim
ejusmodi valores pro his litteris, vt omnes numeri, qu
unico modo in tali formula continentur, certe futuri ſin
primi; praeterea vero etiam dantur ejusmodi valores pr
α et β, vbi talis concluſio falleret, cujusmodi eſt haec fo
mula $7xx + 2yy$, quae ſumpto $x = 1$ et $y = 2$ dat num
rum compoſitum 15, qui tamen unico tantum modo in ha
formula continetur.

§. 19. Cum igitur nobis ſit propoſitum hinc meth
dum certam deducere, numeros praemagnos examinand
utrum ſint primi, nec ne: manifeſtum eſt ad hunc ſcopu
formulas tantum prioris generis $\alpha xx + \beta yy$ adhibe
poſſe, de quibus ſcilicet certi ſumus, omnes numero
qui in iis unico tantum modo contineantur, etiam reve
eſſe primos. Hanc ob rem nobis ante omnia in certa cri
ria inquirere juvabit, quibus tales formulae dignoſci quea
a formulis poſterioris generis, in quibus etiam numeri com
ſiti unico tantum modo contineri poſſunt, quas ergo form
las ab hoc inſtituto penitus excludi oportet; quam ob r
accuratius diſcrimen inter has duplicis generis formulas p
ſcrutari conveniet.

Theorema VI.

Si in formula $\alpha xx + \beta yy$ unico modo contineatur
merus compoſitus mp, *exiſtente* $m > 2$, *tunc etiam innumer*

alii ejusmodi numeri compositi exhiberi possunt, qui etiam unico tantum modo in hac formula contineantur.

Demonstratio.

§. 20. Hic ante omnia probe tenendum est, non solum numeros α et β inter se primos esse debere, sed etiam numeros x et y inter se primos esse accipiendos, atque adeo ita, vt insuper numerus x primus sit ad β, et y ad α; quibus notatis patet, etiam factores m et p ad quatuor numeros α, β, x et y, primos esse futuros.

§. 20. Ponamus igitur esse $mp = \alpha aa + \beta bb$, ac primum observo pluribus modis aliud productum mq exhiberi posse, quod unico modo in formula affini $\alpha\beta xx + yy$ contineatur. Sit enim $mq = \alpha\beta \partial\partial + cc$, ut hinc fiat

$$\beta\partial\partial mp - \alpha\alpha mq = \beta\beta bb\partial\partial - \alpha\alpha cc, \text{ ideoque}$$

$$m(\beta\partial\partial p - \alpha\alpha q) = (\beta b\partial + \alpha c)(\beta b\partial - \alpha c),$$

unde si numeri ∂ et c ita accipiantur, vt vel $\beta b\partial + \alpha c$ vel $\beta b\partial - \alpha c$ per m fiat divisibilis, tum hinc etiam valores idonei pro q reperientur. Sit enim $\beta b\partial + \alpha c = \delta m$, erit $\beta\partial\partial p - \alpha\alpha q = \delta(\beta b\partial - \alpha c)$, ideoque $q = \frac{\beta\partial\partial p - \delta(\beta b\partial - \alpha c)}{\alpha\alpha}$, unde sufficiet minimum valorem ipsius q accipere, ita vt certi esse queamus numerum mq unico modo in formula $\alpha\beta xx + yy$ contineri; quod vel inde patet, si sumpto $a = 1$ et $\partial = 1$ fuerit $mp = \alpha + \beta bb$, tum vero q ita sumatur, vt sit $mq < 4\alpha\beta$. Tum enim evidens est productum mq plus uno modo in formula $\alpha\beta xx + yy$ certe non contineri, quia sumpto $x = 2$ haec formula jam habitura esset valorem majorem.

§. 21. Ducantur nunc in se invicem binae illae formulae, ac reperietur

$$mmpq = \alpha(aacc + \beta\beta bb\partial\partial) + \beta(bbcc + \alpha\alpha aa\partial\partial),$$

quae

quae forma transformari potest in hanc: $mm\,pq = \alpha(\alpha c \pm \beta b \partial)^2 +$ $\beta(bc \mp \alpha a \partial)^2$, unde per mm dividendo colligitur

$$pq = \alpha\left(\frac{\alpha c \pm \beta b d}{m}\right)^2 + \beta\left(\frac{bc \mp \alpha a d}{m}\right)^2$$

vbi quidem signa ambigua duplicem resolutionem innue- videntur; verum hic probe obseruandum est, alteram tantum in numeris fractis subsistere, ideoque a nostro instituto es- removendam. Si enim signa superiora praebeant nume- integros, inferiora dabunt fractiones: nam si summa duorum numerorum A + B per m fuerit divisibilis, neque vero nu- meri A et B seorsim hanc divisionem admittant, tum ce- differentia A — B non erit divisibilis, solo casu excep- quo $m = 2$.

§. 22. Cum igitur productum pq unico modo in in- gris (de quibus solis hic agitur) in formula $\alpha xx + \beta yy$ co- tineatur, simili modo ex hoc producto pq alia nova p- ducta derivari poterunt, quae pariter unico tantum mo- in nostra formula contineantur.

Theorema VII.

Quodsi productum quantumvis magnum pq *unico tan- modo in formula $\alpha xx + \beta yy$ contineatur, tunc etiam mu- hujusmodi producta exhiberi poterunt, quae pariter u- tantum modo contineantur.*

Demonstratio.

§. 23. Ponamus enim esse $pq = \alpha ff + \beta gg$, atque forma comparetur cum modo ante inventa $\alpha\left(\frac{\alpha c \pm \beta b \partial}{m}\right)^2 + \beta\left(\frac{bc \mp \alpha a \partial}{m}\right)^2$, vbi quidem signa superiora tan- valeant, hincque deducemus $f = \frac{\alpha c + \beta b d}{m}$ et $g = \frac{c - \alpha a d}{m}$ quibus duabus aequationibus semper pluribus modis quatuor litterae a, b, c et ∂ definiri poterunt, unde igitur eum modum eligi conveniet, qui pro m minimum producat valorem, qui quidem semper major erit quam 2.

§. 24. Ex his duabus formis deducatur primo fractio $\frac{f}{g} = \frac{ac + \beta b d}{bc - \alpha a d}$, unde derivetur fractio $\frac{c}{\partial} = \frac{\alpha a f + \beta b g}{f b - a g}$. Hic jam pro litteris a et b ejusmodi valores quaerantur, vt numerator et denominator hujus fractionis minimum acquirat divisorem communem, hincque numeri c et ∂ ad minimos valores reducantur.

§. 25. Hoc autem sequenti modo haud difficulter praestari poterit. Ponamus Δ esse minimum communem divisorem harum duarum formularum: I. $\alpha a f + \beta b g$ et II. $b f - a g$, eritque etiam Δ hujus formulae inde formatae $a\,(\alpha f f + \beta g g)$ minimus divisor; hincque patet pro Δ sumi posse factorem quendam formae $\alpha f f + \beta g g$; unde cum hujus formulae factores sint p et q, sumatur $\Delta = p$, et fractio nostra statim per Δ deprimi poterit, unde porro etiam numeri c et ∂ innotescent, quibus inventis sponte se prodit numerus $m = \frac{\alpha c + \beta b d}{f}$.

§. 26. Plurimum juvabit hoc exemplo illustrare formulae $7xx + 2yy$, ita vt sit $\alpha = 7$ et $\beta = 2$, in qua formula istud productum $59 \cdot 131 = 7729$ unico modo continetur, scilicet si $x = 19$ et $y = 51$. Habemus igitur $p = 59$; $q = 131$; $f = 19$ et $g = 51$, unde deducetur fractio $\frac{c}{\partial} = \frac{7 \cdot 19\, a + 2 \cdot 51\, b}{19\, b - 51\, a}$.

§. 27. Nunc a et b ita accipi poterunt, vt communis divisor numeratoris ac denominatoris euadat $\Delta = 59$; atque adeo sufficit soli denominatori hunc divisorem dedisse.

Pona-

Ponamus igitur $19b - 51a = 59n$, eritque $19b = 59n + 51a$, consequenter $b = 3a + 3n + \frac{2n-6a}{19}$. Ponatur nunc $\frac{n-3a}{19} = A$, vt fit $b = 3a + 3n + 2A$, et cum inde fiat $n - 3a = 19A$, erit $3a = n - 19A$, ideoque $a = -6A + \frac{n-A}{3}$. Ponatur porro $\frac{n-A}{3} = B$, erit $A = n - 3B$, ideoque $a = -6n + 19B$ ac denique $b = -13n + 51B$.

§. 28. Vt iam litterae a et b quam minimae reddan-tur, sumatur $B = 0$ et $n = -1$, et denominator evadet $= -5$; tum erit $a = 6$ et $b = 13$, unde fiet nostra fractio $\frac{c}{\partial} = \frac{6 \cdot 7 \cdot 19 - 2 \cdot 13 \cdot 51}{-59} = -\frac{2124}{59} = -36$, ideoque $c = 36$ et $\partial = -1$, unde reperitur $m = 10$.

§. 29. Nunc igitur nacti sumus novum productum minus $mp = 10 \cdot 59$, quod etiam in nostra forma $7xx + 2yy$ con-tinetur, quae si fuerit $7ff + 2gg$, erit $f = 6$ et $g = 13$. Eri igitur $\frac{f}{g} = \frac{6}{13} = \frac{ac - 2b\partial}{bc - 7a\partial}$, unde reperitur $\frac{c}{\partial} = \frac{7 \cdot 6a + 2 \cdot 13b}{6b - 13a}$. Su-mantur nunc a et b ita, ut denominator $6b - 13a$ diviso-rem admittat 10, quod fit sumto $a = 2$ et $b = 6$; fiet enim $\frac{c}{\partial} = 24$, ideoque $c = 24$ et $\partial = 1$, unde fit $m = 10$, vt ante ideoque $7aa + 2bb = 10 \cdot 10$.

§. 30. En ergo novum productum $10 \cdot 10$, pro quo $f = 2$ et $g = 6$. Statuatur igitur $\frac{f}{g} = \frac{2}{6} = \frac{ac - 2b\partial}{bc - 7a\partial}$, und reperitur $\frac{c}{\partial} = \frac{7 \cdot 2a + 2 \cdot 6b}{2b - 6a} = \frac{7a + 6b}{b - 3a}$. Sumatur ergo $a = -2$ et b qui numeri, per 2 depressi, dant $a = -1$, et $b = 2$, hincque $\frac{c}{\partial} =$ ideoque $c = 1$ et $\partial = 1$, ex quo reperitur $m = 3$, unde $7aa + 2bb = 3 \cdot 5$, quod sine dubio est minimum productu

Al

Alia demonstratio ejusdem theorematis.

§. 31. Cum productum pq unico modo in forma illa $\alpha xx + \beta yy$ contineatur, sit $pq = \alpha ff + \beta gg$, atque evidens est factores p et q non in eadem forma contineri, quia alioquin productum duplicem resolutionem admitteret. Consideretur nunc factor minor, qui sit q, atque formula generalis $\alpha xx + \beta yy$ infinitis modis per q divisibilis fieri potest, sumendo $x = nf \pm \mu q$ et $y = ng \pm \nu q$. Prodibit enim

$$\alpha(nnff \pm 2\mu nfq + \mu\mu qq) + \beta(nngg \pm 2\nu gq + \nu\nu qq)$$

quae formula, ob $nn(\alpha ff + \beta gg) = nnpq$, abit in

$$q(nnp \pm \alpha(2\mu nf + \mu\mu q) \pm \beta(2\nu ng + \nu\nu q);$$

ubi litterae μ, ν et n facile ita accipi possunt, ut posterior factor, qui sit r, multo minor evadat quam q, ita ut jam habeamus productum qr, existente $r < q$. Tum vero simili modo ex hoc producto aliud denuo minus elici poterit, quod sit $= rs$, existente $s < r$; atque hac ratione mox perveniri poterit ad productum minimum, si modo in qualibet operatione valores ipsarum x et y minimi reddantur.

§. 32. Haec clariora evadent, si ad exemplum propositum applicentur, quo erat $pq = 7 \cdot 19^2 + 2 \cdot 51^2 = 7729$, ubi ergo $p = 131$ et $q = 59$. Cum igitur hic sit $f = 19$ et $g = 51$, valores generales erunt: $x = 19n - 59\mu$ et $y = 51n - 59\nu$, qui pluribus modis multo minores reddi possunt quam f et g. Veluti sumptis n, μ et $\nu = 1$, fiet $x = -40$ et $y = -8$, qui numeri, per 8 depressi, evadunt $x = -5$ et $y = -1$, unde prodit $7xx + 2yy = 59 \cdot 3$, ideoque $r = 3$. Nunc ergo cum sit $f = 5$ et $g = 1$, novi valores erunt $x = 5n - 3\mu$ et $y = n - 3\nu$ unde valores minimi, per 2

de-

depreffi, erunt $x = 1$ et $y = 1$; quare productum minimum resultat $7 + 2 = 3 \cdot 3$; unde facile intelligitur, quomodo pro quovis cafu operationes fint inftituendae.

§. 33. Totum hoc ratiocinium fimili modo inftitu poteft pro formula $\alpha\beta xx + yy$, ita vt, fi numeri quantum vis magni compofiti in ea femel tantum contineantur, ex iis continuo minores reperiri queant, quae pariter unico tantum modo in hac formula contineantur. Atque adeo ha operationes eo vsque continuare licebit, donec ad numero compositos perveniatur, qui fint minores quam $4\alpha\beta$. Quod etiam praecedente exemplo illuftrari poteft; quandoquidem numerus $59 \cdot 131$ etiam unico modo in formula $14xx + y$ continetur, exiftente $x = f = 6$ et $y = g = 85$, unde nov valores erunt $x = 6n - 59\mu$ et $y = 85n - 59\nu$. Ja hic notetur litteras n et ν femper ita accipi poffe, vt fi $x = 1$: pofito enim $6n - 59\mu = 1$, erit $n = 10\mu + \frac{\mu+}{6}$ Capiatur ergo $\mu = 1$, eritque $n = 10$ et $x = 1$, tum ve $y = 850 - 59\nu$, cujus valor minimus prodit ex $\nu = 1$ unde fit $y = 24$. Adepti igitur fumus hanc formam: $14 \cdot 1^2 + 24^2 = 59 \cdot 10$. Eadem autem forma factorem h bebit 10, fi fumatur $y = 24 - 10\nu = 4$, unde refultat p $14 \cdot 1^2 + 4^2 = 30 = 10 \cdot 3$, qu ductum adhuc minus eft quam $4\alpha\beta$. Quodfi enim fuerit num rus compositus $pq < 4\alpha\beta$, hic cafus locum habere quit, nifi fuerit $x = 1$, unde y etiam datum fortietur lorem. Hinc viciffim manifefto fequitur, fi nullus nume compofitus minor quam $4\alpha\beta$ in formula $\alpha\beta xx + yy$ co tineatur, tales etiam in numeris maximis non dari; con quenter quoties quispiam numerus in tali formula un tantum modo continetur, tum certo concludere poterim ill illum numerum eſſe primum; unde ſequens problema maximi momenti reſolvere licebit.

PROBLEMA.

Propoſitae formulae cujuscunque $\alpha xx + \beta yy$ *naturam perſcrutari, utrum numeri unico modo in ea contenti tuto concludi queant eſſe primi, an vero iſta concluſio fallere queat, quippe quo poſteriori caſu tales formulas a propoſito noſtro excludi oportet.*

Solutio.

§. 34. Primo ex iis, quae ſunt allata, ſatis intelligitur, hanc formulam eadem proprietate praeditam eſſe atque ejus affinem $\alpha\beta xx + yy$. Sicque totum judicium eo redit, vtrum omnes numeri ſemel tantum in hac formula contenti tuto pro primis haberi queant, nec ne? Ad hanc quaeſtionem decidendam ſufficiet examinaſſe, vtrum dentur numeri compoſiti minores quam $4\alpha\beta$, qui in hac formula contineantur. Si enim tales numeri occurrant, non ſolum haec formula $\alpha\beta xx + yy$, ſed etiam illa $\alpha xx + \beta yy$ a propoſito noſtro eſt excludenda: contra autem, ſi nulli tales numeri compoſiti occurrant, vtraque formula ad numeros primos explorandos tuto vti licebit; quandoquidem omnes numeri vnico modo contenti certe futuri ſunt primi.

§. 35. Hinc igitur ſtatim, quia nulli alii numeri, niſi minores quam $4\alpha\beta$, in judicium ingrediuntur, ponatur $x = 1$, vt habeatur formula $\alpha\beta + yy$, vbi ipſi y nullos alios valores tribui opus eſt, niſi qui ſint ad $\alpha\beta$ primi. Reliquis igitur

igitur exclusis ipsi y successive tribuantur tales valores, donec numeri resultantes terminum $4\alpha\beta$ excedant.

§. 36. Jam nihil reliquum est, nisi vt numeri hoc modo prodeuntes examinentur, vtrum sint primi, an vero compositi; si enim unicus compositus occurrat, eam formulam statim excludi oportebit. Hic autem probe est tenendum, numeros quadratos in hoc judicio inter compositos numerari non debere, propterea quod si fuerit $\alpha\beta + yy = kk$, idem quadratum insuper alio quoque modo in formula illa $\alpha\beta xx + yy$ continetur, scilicet quando $x = 0$ et $y = k$; quamobrem, quoties in his evolutionibus numeri quadrati occurrent, ii non compositis numeris, sed primis accenseri debebunt *).

§. 37. Hanc regulam illustremus exemplo formulae $7xx + 2yy$, vbi $\alpha = 7$ et $\beta = 2$, ita vt formula $14 + yy$ sit examinanda. Hic ergo valores ipsi y tribuendi primo debent esse impares, neque per 7 divisibiles, idque tantum eo vsque, quamdiu numeri prodeuntes non superabunt terminum $4 \cdot 14 = 56$. Hoc examen sequenti modo commode repraesentabitur;

$14 + 1$;	3^2,	5^2
15,	23,	39
c.	p.	c.

vbi

*) Praeterea vero si etiam numeri pares prodeant, quoniam supra §. 21 vidimus, ex valoribus litterae m vnitatem et binarium excludi: hinc si p sit numerus primus, in hac investigatione, praeter ipsum numerum p, etiam ejus quadratum pp, simulque ejus duplum $2p$, vt primi spectari debebunt; praeterea etiam omnes potestates binarii pro primis spectari debent.

vbi numeri compoſiti littera c, primi vero littera p deſignentur. Hinc igitur patet, a noſtro inſtituto excludi debere non ſolum formulam $14xx + yy$, ſed etiam $7xx + 2yy$.

§. 38. Simili modo examinetur formula $11xx + yy$, atque in formula $11 + yy$ ipſi y tribuantur valores ad 11 primi, vsque ad terminum 44, quod ergo examen ita referetur:

$$\frac{11 + 1;\ 2^2.\ 3^2.\ 4^2.\ 5^2.}{12.\ 15.\ 20.\ 27.\ 36}$$
$$c\quad c\quad c\quad c\quad c$$

Quoniam igitur hic omnes numeri reſultantes ſunt compoſiti, hunc numerum 11 maxime excludi oportet.

Examinetur nunc numerus 13, vtrum excludi debeat, nec ne, quod examen ita inſtituetur:

$$\frac{13 + 1;\ 2^2.\ 3^2.\ 4^2.\ 5^2.\ 6^2}{14.\ 17,\ 22,\ 29,\ 38,\ 49}$$
$$2p\quad p,\quad p\quad p,\quad p,\ pp$$

Hic ergo nulli numeri compoſiti occurrunt, unde numerus 13 ad claſſem numerorum idoneorum referri debebit.

Examinetur numerus 30, vtrum ſit idoneus, an vero excludi debeat, qui calculus ita ſe habebit:

$$\frac{30 + 1^2.\ 7^2}{31.\ 79}$$
$$p\quad p$$

Quia ergo hic etiam nullus numerus compoſitus prodit, numerus 30 in claſſe numerorum idoneorum locum habebit.

Exami-

Examinetur numerus 43, et calculus ita ſe habebit:

$$\frac{43 + 1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2,\ 9^2,\ 10^2,\ 11^2,}{44,\ 47,\ 52,\ 59,\ 68,\ 79,\ 92,\ 107,\ 124,\ 143,\ 164,}$$
$$c,\ p,\ c,\ p,\ c,\ p,\ c,\ p,\ c,\ p,\ c$$

Hinc ergo patet, hunc numerum 43 ex claſſe numerorum idoneorum excludi debere.

Examinetur nunc ſimili modo numerus $210 = 2.3.5.7$, ita vt ipſi y valores ad 210 primos tribui oporteat usque ad terminum 840

$$\frac{210 + 1;\ 11^2;\ 13^2;\ 17^2;\ 19^2;\ 23^2}{211,\ 331,\ 379,\ 499,\ 571,\ 739}$$
$$p,\ p,\ p,\ p,\ p,\ p$$

Cum igitur omnes numeri prodeuntes ſint primi, numerus iſte 210 pro idoneo eſt habendus, ex quo plures formulae ſequentes formari poſſunt:

1. $210\,xx + yy$
2. $105\,xx + 2yy$
3. $70\,xx + 3yy$
4. $42\,xx + 5yy$
5. $30\,xx + 7yy$
6. $35\,xx + 6yy$
7. $21\,xx + 10yy$
8. $14\,xx + 15yy$

quae omnes formulae ita ſunt comparatae, vt omnes numeri, qui in quapiam earum ſemel tantum continentur, certe futuri ſint numeri primi.

§. 39. Poſtquam igitur hoc modo numeri ad inſtitutum noſtrum inepti fuerint excluſi, reliqui numeri, quos idoneos appellemus, ordine in tabulam referantur, quam usque ad terminum 3000 continuare licuit; atque adeo adhuc dubium videtur, num majores numeri idonei reperiri queant.

TABULA

numerorum idoneorum.

1	13	37	85	177	357
2	15	40	88	190	385
3	16	42	93	210	408
4	18	45	102	232	462
5	21	48	105	240	520
6	22	57	112	253	760
7	24	58	120	273	840
8	25	60	130	280	1320
9	28	70	133	312	1365
10	30	72	165	330	1848
12	33	78	168	345	

Hic ſcilicet maximus numerus idoneus eſt 1848, ex his factoribus compoſitus: 8 . 3 . 7 . 11; neque poſt hunc ullum alium majorem mihi quidem invenire licuit, poſtquam iſtum laborem vsque ad 3000, et ultra, ſum exſecutus. Operae autem pretium erit in confirmationem hujus tanti numeri probationem adiungere.

1848		1848	
+ 1	1849 = 43^2 = pp	+ 37^2	3217 — p
+ 5^2	1873 — p	41^2	3529 — p
13^2	2017 — p	43^2	3697 — p
17^2	2137 — p	47^2	4057 — p
19^2	2209 = 47^2 = pp	53^2	4657 — p
23^2	2377 — p	59^2	5329 = 73^2 = pp
25^2	2473 — p	61^2	7417 — p
29^2	2689 — p		
31^2	2809 = 53^2 = pp		

§. 40. Diſtinctio igitur talium formularum $\alpha xx + \beta yy$ in duas claſſes maxime eſt memorabilis, et in ipſa rei natura fundata, quarum claſſium prior omnes tales formulas complectitur, in quibus omnes numeri ſemel tantum contenti tuto pro primis haberi queant, quarum criterium in hoc conſiſtit, vt productum $\alpha\beta$ in ſuperiore tabula numerorum idoneorum reperiatur, cujus generis ſimpliciores formae ſunt $xx + yy$; $2xx + yy$; $3xx + yy$, quarumque proprietas iſta jam pridem a Geometris eſt agnita, et demonſtrata. Ad alteram vero claſſem referendae ſunt reliquae formae $\alpha xx + \beta yy$, in quibus etiam numeri compoſiti unico tantum modo contenti eſſe poſſunt, quarum criterium in hoc conſiſtit, quod productum $\alpha\beta$ non in ſuperiori tabula occurrit, cujusmodi formae ſimpliciores ſunt $5xx + 4yy$; $7xx + 2yy$; $7xx + 5yy$; $11xx + yy$ etc. Quantum autem hinc ſubſidium oriatur, ad numeros praegrandes examinandos, vtrum ſint primi, nec ne, in ſingulari diſſertatione fuſius oſtendi.

ADDI-

ADDITAMENTUM.

De numeris idoneis inveſtigandis.

§. 41. Tabula numerorum idoneorum huic diſſertationi inſerta eo magis eſt notatu digna, quod non ſolum omnes numeros hujus naturae usque ad 2 millia exhibeat, ſed etiam vltra hunc terminum nulli prorsus hujusmodi numeri occurrere videantur. Cum enim hanc inveſtigationem vsque ad 4 millia eſſem proſecutus, in toto hoc intervallo ne vnicus quidem numerus idoneus ſe mihi obtulerat; unde ſequitur, ab hoc termino vsque ad 16000 nullos certe dari numeros idoneos per 4 diviſibiles; eorum enim partes quartae in praecedente intervallo reperiri deberent. Neutiquam autem probabile eſt ibi numeros vel impares vel impariter pares exiſtere; ex ſola enim inſpectione ſuperioris tabulae manifeſto patet iſtos numeros continuo magis fieri compoſitos, ſiquidem vltimus hujus tabulae numerus primus eſt 37; numerus vero, qui tantum duobus conſtat factoribus, eſt 253. Hinc igitur maxime veriſimile eſt in tabula noſtra omnes plane numeros idoneos contineri.

§. 42. Cum iſti numeri ſumma attentione ſint digni, operae pretium erit eorum proprietates accuratius perpendiſſe. In hoc autem negotio imprimis attendiſſe juvabit, quaenam numerorum genera ex hac tabula excludantur. Quemadmodum enim numeri primi reperiuntur, dum ex ordine omnium numerorum omnes, qui ſunt compoſiti, delentur, ita etiam numeri idonei relinquuntur, poſtquam omnes ineptos deleverimus; numerorum igitur genera, quae excludi oportet, hic ante oculos conſtituamus.

I. Primum genus numerorum excludendorum in hac forma continetur: $4n+3$. Si enim primum quadratum 1 addatur, prodit $4(n+1)$, ideoque numerus compositus, solis casibus exceptis, quibus $(n+1)$ est potestas binarii, uti evenit, si fuerit vel $n=0$; vel $n=1$; vel $n=3$; vel $n=7$. Hanc ob rem ex ordine omnium numerorum excludi debent numeri formae $4n+3$ praeter hos tres minimos, 3, 7 et 15.

II. Excludi etiam debent numeri in hac forma contenti: $3n+2$, quia addito quadrato 1 prodit $3(n+1)$, ideoque numerus compositus, nisi fuerit vel $n=0$, quo casu numerus fit revera primus; vel $n=1$, quo casu prodit numerus $2 \cdot 3$ pro primo habendus, ob formam pq; vel $n=2$, quo casu prodit numerus $3 \cdot 3$ formae pp, pariter pro primo habendus. Hinc ergo ex ordine omnium numerorum excludi debent omnes numeri formae $3n+2$, praeter hos tres: 2, 5 et 8.

III. Excludi debent omnes numeri in hac forma contenti: $5n+4$. Addita enim 1 prodit $5(n+1)$, numerus compositus, exceptis casibus $n=0$; $n=1$ et $n=4$. Quamobrem ex ordine omnium numerorum excludi debent omnes numeri formae $5n+4$, praeter hos tres: 4, 9, 24; reliqui scilicet omnes, qui sunt 19, 29, 34, 39, etc. debent deleri;

IV. Excludi debent numeri formae $5n+1$, quia addito quadrato 4 prodit numerus $5(n+1)$, pro composito habendus, nisi fuerit vel $n=0$; vel $n=1$; vel $n=4$; quamobrem ex ordine omnium numerorum excludi debent omnes numeri formae $5n+1$, praeter hos tres, 1, 6, 21, quibus adiungi oportet casus $n=3$, quoniam ad

nume-

numerum 16 quadratum 4 addi non convenit; ficque numeri hinc expungendi erunt 11, 26, 31, 36, 41, 46, etc. NB. Si binae pofteriores conditiones conjungantur, excludi debent numeri definentes in 1, 4, 6 et 9, exceptis minoribus 1, 4, 6, 9, 21 et 24.

V. Ob numerum primum 7 excludi debent numeri formae $7n+6$, quia addito quadrato 1 prodit numerus compofitus $7(n+1)$ exceptis cafibus, $n=0$; $n=1$ et $n=6$. Unde ex ordine omnium numerorum excludi debent omnes numeri formae $7n+6$, exceptis his tribus: 6, 13, 48; ita vt deleri debeant numeri 20, 27, 34, 41, 55, 62 etc.

VI. Ob eundem numerum 7 etiam excludi debet forma $7n+5$, quia addito quadrato 9 prodit forma $7(n+2)$, qui eft numerus compofitus; nifi fuerit $n=0$ et $n=5$. Infuper vero etiam excipiuntur cafus $n=1$; $n=4$; $n=7$ et $n=10$, quippe quibus forma $7n+5$ diviforem habet 3, ideoque quadratum 9 eo addi non conveniet; quam ob rem expungi debent omnes numeri $7n+5$, praeter hos: 5, 12, 33, 40.

VII. Ob eundem numerum 7 excludi debent numeri formae $7n+3$, quia addito quadrato 4 prodit forma $7(n+1)$, ideoque numerus compofitus, praeter cafus $n=0$; $n=1$ et $n=6$. Praeterea vero etiam intelligitur, non nifi ad numeros impares quadratum 4 addi poffe; hinc ergo excludi debent omnes numeri in forma $7n+3$ contenti, praeter iftos: 3, 10, 24, 45. NB. Ob numerum ergo 7 omnes numeri in quapiam harum trium formarum $7n+2$, $7n+5$, $7n+6$, contenti excludi debent, praeter 3, 5, 6, 10, 12, 13, 24, 40, 45 et 48.

VIII. Deinde ob numerum primum 11 excludi debet forma $11n+10$, quia addito 1 prodit $11(n+1)$, ideoque numerus

merus

merus compositus, praeter casus $n = 0$; $n = 1$ et $n = 10$; unde omnes numeri hujus formae deleri debent, praeter 10, 21, 120.

IX. Ob eundem numerum 11 excludi debet forma $11n + 8$, quia addito quadrato 25 prodit forma $11(n + 3)$, quae semper est numerus compositus, praeter casum $n = 8$, quo prodit 11^2. Deinde etiam considerari debet, casibus, quibus haec forma $11n + 8$ factorem habet 5, additionem quadrati 25 locum non habere. Hinc ergo omnes numeri formae $11n + 8$ excludi debent, praeter hos: 8, 30, 85.

X. Ob eundem numerum 11 excludi debet forma $11n + 7$, quoniam addito quadrato 4 prodit $11(n + 1)$, numerus compositus, praeter casus $n = 0$, $n = 1$ et $n = 10$; unde prodeunt numeri 7, 18 et 117, quorum postremus, ob alias rationes, scilicet ob formam $7n + 5$, jam est exclusus. Praeterea vero casus, quibus $11n + 7$ est numerus par, additionem quadrati 4 non patiuntur; ergo omnes numeri formae $11n + 7$ deleri debent, praeter 7, 18, 40.

XI. Ob eundem numerum 11 excludi debet forma $11n + 6$, cui quadratum 16 additum producit $11(n + 2)$, ideoque numerus compositus, praeter $n = 0$ et $n = 9$, hoc est praeter numeros 6 et 105. Sicque deleri debent omnes numeri formae $11n + 6$, praeter 6 et 105, quibus adiungi oportet insuper pares numeros 28 et 72, quippe qui additionem quadrati 16 non admittunt.

XII. Ob eundem numerum 11 restat forma $11n + 2$, cui quadratum 9 additum dat $11(n + 1)$, unde oritur exclusio $n = 0$; $n = 1$ et $n = 10$, praeterquam quod numeri hujus formae per 3 divisibiles additionem hujus quadrati non patiuntur; consequenter omnes numeri $11n + 2$ sunt expun-

expungendi, praeter 2, 13, 112, quibus adiungi oportet numeros hujus formae per 3 divifibiles, qui funt 24, 57. NB. Ob numerum igitur primum 11 habentur quinque numerorum formae, quos deleri oportet, fcilicet 11 $n+2$, 11 $n+6$, 11 $n+7$, 11 $n+8$, 11 $n+10$, praeter fcilicet paucos certos numeros, qui ob fingulares rationes relinqui debent.

§. 43. Simili modo etiam fequentes numeri primi evolvi poffent, quod autem nimis foret prolixum. Contenti autem effe poffumus pro fingulis eas formas notaffe, quas excludi oportet: hae autem formae excludendae funt fequentes:

1° $4n+3$
2° $3n+2$
3° $5n+1, 4$
4° $7n+3, 5, 6$
5° $11n+2, 6, 7, 8, 10$
6° $13n+1, 3, 4, 9, 10, 12$
7° $17n+1, 2, 4, 8, 9, 13, 15, 16$
8° $19n+2, 3, 8, 10, 12, 13, 14, 15, 18$
9° $23n+5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22$
10° $29n+1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.$

§. 44. Numeri autem in his formis contenti ideo excludi debent, quia femper quadratum addere licet, ita ut fumma per ipfum illum numerum primum fit divifibilis. Ita numerus $29n+13$ ideo excluditur, quia addito quadrato 16 prodit fumma $29(n+1)$ per 29 divifibilis. Quo igitur ftatim hujusmodi quadrata addenda obtineantur, fuperiores formae pro fingulis numeris primis fequenti modo commode repraefentari poffunt:

4 n +

$4n+$	$\sqrt{\Box}$
$+3$	1, 3

$3n+$	$\sqrt{\Box}$
$+2$	1, 2

$5n+$	$\sqrt{\Box}$
$+4$	1, 4
$+1$	2, 3

$7n+$	$\sqrt{\Box}$
	1, 6
$+3$	2, 5
$+5$	3, 4

$11n+$	$\sqrt{\Box}$
	1, 10
$+7$	2, 9
2	3, 8
6	4, 7
8	5, 6

$13n+$	$\sqrt{\Box}$
$+12$	1, 12
9	2, 11
4	3, 10
10	4, 9
1	5, 8
3	6, 7

$17n+$	$\sqrt{\Box}$
16	1, 16
13	2, 15
8	3, 14
1	4, 13
9	5, 12
15	6, 11
2	7, 10
4	8, 9

$19n+$	$\sqrt{\Box}$
18	1, 18
15	2, 17
10	3, 16
3	4, 15
13	5, 14
2	6, 13
8	7, 12
12	8, 11
14	9, 10

$23n+$	$\sqrt{\Box}$
$+22$	1, 22
19	2, 21
14	3, 20
7	4, 19
21	5, 18
10	6, 17
20	7, 16
5	8, 15
11	9, 14
15	10, 13
17	11, 12

$29n+$	$\sqrt{\Box}$
28	1, 28
25	2, 27
20	3, 26
13	4, 25
4	5, 24
22	6, 23
9	7, 22
23	8, 21
6	9, 20
16	10, 19
24	11, 18
1	12, 17
5	13, 16
7	14, 15

Hujusmodi tabellae nobis novam methodum ſuppeditant numeros propoſitos quosvis examinandi, vtrum ſint idonei nec ne; quem in finem ſequens problema adjungamus.

PRO-

PROBLEMA.

Numerum quemvis propofitum n *examinare, vtrum fit idoneus nec ne?*

Solutio.

§. 45. Ex praecedentibus patet numerum n tum demum effe idoneum, quando additis quadratis minoribus, ad n primis, fummae refultant, quae funt vel numeri primi, vel eorum dupla, vel etiam quadrata, vel adeo poteftates binarii, idque vsque ad terminum $4n$. Ex quo intelligitur, numerum propofitum n non fore idoneum, quando datur quadratum $aa < 3n$ et primum ad n, vt fumma $n + aa$ evadat numerus compofitus, qui, denotante p numerum primum, neque fit p, neque $2p$, neque pp, neque adeo 2^{α}.

§. 46. Quando autem formula $n + aa$ talem numerum compofitum producit, quia affumimus $n + aa < 4n$, neceffe eft vt is factorem habeat primum et minorem quam $\sqrt{4n}$. Quamobrem res eo redit, ut inquiratur num detur numerus primus $< \sqrt{4n}$ per quem quispiam numerorum in forma $n + aa$ contentorum divifionem admittat, fiquidem quadratum aa fuerit ad n primum atque $aa < 3n$. Ad hoc igitur explorandum percurrantur ordine omnes numeri primi fupra allati, ad examinandum, vtrum numerus nofter propofitus n in quapiam exclufione contineatur, quod fi eveniat non tamen inde ftatim erit concludendum, iftum numerum non effe idoneum, quoniam fieri poteft, vt formula $n + aa$ vel ipfi numero p, vel ejus duplo, vel ejus quadrato fiat aequalis, quippe quibus cafibus, vt vidimus, exclufio locum non habet. Imprimis autem hic meminiffe oportet, quadratum aa ad ipfum numerum propofitum primum esse debere, aliter exclusio quoque locum non habet. Quodsi ergo, percursis hoc modo omnibus numeris primis minoribus quam $\sqrt{4n}$, nulla exclusio reperiatur, tum numerus propositus pro idoneo erit habendus; tota autem haec operatio multo clarius per exempla intelligetur.

Exemplum I.

§. 47. Propositus sit numerus $n = 33$, et cum sit $\sqrt{4n} < 12$, considerentur omnes numeri primi vsque ad 11, utrum iste numerus 33 in quapiam forma excludente contineatur. Statim autem perspicitur hunc numerum neque in prima forma excludente $4n+3$, neque in secunda $3n+2$, neque tertia $5n+1$, 4 contineri; at vero in quarta forma pro numero primo 7 continetur, cum sit $33 = 7m+5$, quae exclusionem innuit; quadratum autem aa, quod ipsi 33 additum divisionem per 7 producit, indicatur vel 3^2, vel 4^2, at vero prius 3^2 hic reiici debet, quia ad 33 non est primum, alterum vero 4^2, additum ad 33, producit 49, qui numerus cum sit quadratus, pariter nullam exclusionem parit. Dantur quidem etiam quadrata majora, divisibilitatem per 7 producentia, scilicet $7\alpha \pm 3^2$, cujusmodi sunt 10^2, 11^2, 17^2, 18^2 etc. quorum primum 10^2, vtpote ad 33 primum, praebet vtique summam 133 per 7 divisibilem, quae autem jam major est quam $4 \cdot 33 = 132$, atque adeo duplici modo in forma $33xx+yy$ continetur, scilicet 1°) $x = 1$ et $y = 10$, 2°) $x = 2$ et $y = 1$.

§. 48. Numerus ergo primus 7 nullam exclusionem gignit, sequentem autem 11 examinare non attinet, quia 11 est divisor ipsius 33, unde recte concludimus numerum 33 esse idoneum.

Exem-

Exemplum II.

§. 49. Propoſitus ſit numerus $n = 58$, vbi $\sqrt{4n} < 16$, ita vt numeros primos minores quam 16 percurri oporteat. Manifeſtum autem eſt hunc numerum neque in prima forma excludente $4n+3$, neque in ſecunda $3n+2$, neque tertia $5n+1, 4$, neque etiam quarta $7n+3, 5, 6$, neque quinta $11n+2, 6, 7, 8, 10$, contineri; neque vero etiam hic numerus per ultimum 13, minorem quam 16, excluditur; unde ſequitur numerum 58 revera eſſe idoneum.

Exemplum III.

§. 50. Sit numerus propoſitus $n = 345 = 3 \cdot 5 \cdot 23$, unde quia $\sqrt{4 \cdot 335} < 38$, omnes numeros primos vsque ad 37 percurri oportet. Hinc autem nulla excluſio occurrit, vsque ad numerum primum 19; propterea quod $345 = 19 \cdot 18 + 3$, unde quadrata addenda ſunt 4^2, 15^2, quorum poſterius rejicitur, quia non eſt primum ad 345; at prius 4^2 additum producit ſummam 361, quae eſt quadratum ipſius 19, ideoque excluſionem non gignit. Reliqua quadrata $(19n \pm 4)^2$, quae ſunt 23^2, 34^2, 42^2, 53^2, 61^2, quae pariter diviſibilitatem per 19 pariunt, at praeter 23^2 terminum $3n$ ſuperant: illud autem 23^2 adhibere non licet, vtpote factorem ipſius 345, quam ob rem iſte numerus 345 pro idoneo eſt habendus, niſi forte ſequentes numeri primi vsque ad 37 excluſionem generent. Jam poſt 19 ſequitur numerus 23, qui hic autem in computum non venit; pro ſequente 29 fit $345 = 29 \cdot 11 + 26$, quod nullam excluſionem innuit; porro vero eſt $345 = 31 \cdot 11 + 4$, pariter nullam excluſionem continens. Denique eſt $345 = 37 \cdot 9 + 12$, qua forma excluſio innuitur, quemadmodum facile pateret, ſi tabulas vlterius continuare liceret. Quadrata enim addenda

F 2 ſunt

sunt 5^2 et 32^2, quorum priore vti non licet, quia non est primum ad 345; alterum vero 32^2 additum producit 1369, hoc est ipsum quadratum 37^2, ita vt hinc nulla exclusio locum habeat, quocirca hic numerus 345 in classem numerorum idoneorum est referendus.

Exemplum IV.

§. 51. Propositus sit numerus $148 = 4 \cdot 37$, quem ergo secundum numeros primos $< \sqrt{592} < 25$ examinemus: at vero nulla exclusio innuitur usque ad 19, siquidem est $148 = 19 \cdot 7 + 15$. Quadrata igitur addenda sunt 2^2, 17^2, quorum prius hic locum non habet, alterum vero additum producit $437 = 19 \cdot 23$, qui ergo est numerus compositus $< 4 \cdot 148$; unde sequitur hunc numerum 148 non esse idoneum.

Exemplum V.

§. 52. Propositus sit numerus $522 = 2 \cdot 9 \cdot 29$, unde numeros primos usque ad 46 percurri conveniet. Minores autem formulae nullam exclusionem gignunt, vsque ad numerum primum 31, per quem divisio succedit, addendo quadrata vel 6^2 vel 25^2, quorum posterius producit $1147 = 31 \cdot 37$; qui numerus compositus, cum sit minor quam 2088, manifesto hunc numerum 522 ex classe idoneorum excludit.

§. 53. Hac methodo haud difficile est istud numerorum examen quousque lubuerit continuare. Postquam autem hunc calculum vsque ad 10000 essem profecutus, nullus novus numerus idoneus se mihi obtulit, praeter eos, quos tabula superior exhibet, ex quo ista tabula omnes plane numeros idoneos in se complecti videtur.

RESO-