



1805

Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne?

Leonhard Euler

Follow this and additional works at: <https://scholarlycommons.pacific.edu/euler-works>

 Part of the [Mathematics Commons](#)

Record Created:

2018-09-25

Recommended Citation

Euler, Leonhard, "Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne?" (1805). *Euler Archive - All Works*. 719.

<https://scholarlycommons.pacific.edu/euler-works/719>

This Article is brought to you for free and open access by the Euler Archive at Scholarly Commons. It has been accepted for inclusion in Euler Archive - All Works by an authorized administrator of Scholarly Commons. For more information, please contact mgibney@pacific.edu.

28|282, 284, 286, 287
29|290, 292, 293, 295, 296, 298

His igitur numeris exclusis reliqui omnes loco a scripti in formula $3^2aa - 1$ producant numeros primos. Hos igitur valores ipsius a sequens exhibet tabula:

- 1, 2, 3, 5, 6, 7, 9, 11, 12, 13, 15, 16, 17, 18,
- 20, 22, 24, 26, 27, 28, 29, 31, 35, 36, 37, 38,
- 41, 45, 46, 48, 49, 50, 51, 53, 57, 62, 67, 71,
- 73, 74, 76, 79, 81, 82, 86, 87, 94, 95, 99, 100,
- 104, 106, 107, 112, 113, 115, 117, 118, 219, 221,
- 124, 126, 127, 136, 138, 142, 144, 149, 150, 151,
- 152, 153, 155, 157, 158, 159, 165, 167, 170, 172,
- 173, 175, 176, 177, 181, 182, 185, 189, 192,
- 190, 197, 200, 201, 204, 205, 210, 213, 215, 219,
- 226, 227, 228, 229, 230, 238, 248, 249, 250, 251,
- 254, 255, 258, 259, 261, 262, 264, 267, 269, 270,
- 273, 275, 277, 279, 280, 281, 283, 285, 288, 289,
- 291, 294, 297, 299.

horum numerorum ultimi fere ad 20 miliones exsurgunt.

ME.

METHODUS GENERALIOR
NUMEROS QUOSVIS SATIS GRANDES PERSCRUTANDI
UTRUM SINT PRIMI NEC NE?

AUCTORE
L. EULERO.

Conventui exhibita die 16 Martii 1778.

§. I.

Sit N numerus propositus, et non difficile erit eum reduce ad huiusmodi formam: $N = aa + \lambda bb$; tum vero inquiratur, utrum adhuc alio modo ad similem formam reduci queat. Si enim quoque fuerit $N = xx + \lambda yy$, ita ut sit $aa + \lambda bb = xx + \lambda yy$, tum, certe numerus N non erit primus, sed eius factores hoc modo assignari poterunt. Quoniam hinc est $aa - xx = \lambda (yy - bb)$, erit $\frac{a+x}{y-b} = \lambda \cdot \frac{y+b}{a-x}$, quae fractiones ad minimos terminos reduci sint $\lambda \cdot \frac{p}{q}$. Ponatur igitur $a+x = imp$ et $y-b = np$, erit $y+b = mq$ et $a-x = nq$, et hinc reperietur $a = \frac{\lambda m p + n q}{2}$ et $b = \frac{m q - n p}{2}$, ex quibus valoribus, erit $N = \frac{1}{4} (\lambda m m + n n)$ ($\lambda p p + q q$); unde patet, formulam $\lambda p p + q q$ vel ipsam, vel eius semissem, vel quadrantem esse factorem numeri propositi N.

§. 2. Quando autem ad talem formam $N = aa + \lambda bb$ pervenimus, tum statuamus $N = xx + \lambda yy$, ubi statim facile patebit, utrum hi numeri x et y sint pares, an vero impares, quo reperto statuaturs vel $N = xx + \lambda yy$, vel $N = \lambda yy = xx$; ac priori quidem casu numerus x ita accipi debet

B 2

debet, ut $N = xx$ dividi queat per numerum λ . Hoc modo ad novas formulas pervenietur, quae quadrata fieri debent. in quibus inveniuntur numerus incognitus, qui, prout fuerit acceptus vel par vel impar, ad casus leducet seorsim evolventes. Omnes autem istae operationes facilius exemplis doceantur.

E x e m p l u m.

1000; §. 3. Sit numerus examinandus $N = 10003 = 100^2 + 3 \cdot 1^2$, ubi ergo $\lambda = 3$. Statuatur $N = xx + 3yy$, et quia horum numerorum x et y alter necessario est par, alter impar, videamus ante omnia uter eorum sit par, uter impar. Quoniam autem N est numerus formae $8n + 3$, si y esset par, foret $3yy$ numerus vel formae $8n + 4$, vel formae $8n + c$; at tunc foret xx formae $8n + 5$, vel $8n + 1$, quorum neutra hic locum habere potest. Sumi ergo debeat x par, eritque xx vel formae $8n + c$, vel formae $8n + 4$; et quia tunc y est impar, erit $3yy$ formae $8n + 3$, ideoque xx formae $8n + 0$ et x numerus pariter par.

§. 4. Quod si ergo statuamus $N = 3yy = xx$, istum numerum divisibilem esse oportet per 16; unde si ponamus $y = 1 + 2a$, haec aequatio dabit $1000 = 12a - 12aa = xx$, quae per 4 divisa abit in $250 = 3a - 3aa = \frac{xx}{4}$. Unde patet numerum a denuo per 4 divisibilem esse debere. vel potius statim poni potuisset $y = 1 + 8a$, unde prodisset aequatio $625 = 3a - 12aa = \frac{xx}{16} = \square$.

§. 5. Nunc jam duos distinguamus casus. prout numerus a capiatur vel par vel impar. Sit igitur primo a numerus par, et quia numerus absolutus 625 jam habet formam $8n + 1$ et 12aa formam $8n$; necesse est ut etiam $3a$ divisio-

divisorem per 8 admitat. Hinc statim ponatur $a = 8i$ fectue $625 = 24b - 12 \cdot 64bb = \square$. Quia igitur a numero absoluto 625 subtrahi debet forma $768bb + 24b$, patet valorem minimum $b = 1$ jam esse nimis magnam hincque nullum oriri posse quadratum. Ex valore quidem $b = 0$ prodiret quadratum, sed ad casum cognitum pertinens

§. 6. Consideremus igitur casum, quo a est numerus impar, cuius forma cum sit duplex, vel $4n + 1$, vel $4n - 1$ statuatur primo $a = 4c + 1$, eritque $610 = 108c - 192cc = \square$ qui numerus, cum sit impariter par, quadratum esse nequit

§. 7. Tantum igitur examinandus superest casus quae $a = 4d - 1$, qui praebet hanc aequationem: $616 + 84d - 192dd = \square$, quae per 4 divisa in hanc abit $154 + 21d - 48dd = \frac{xx}{4} = \square$. A numero igitur absolute 154 subtrahi debent numeri minores in forma $48dd + 21d$ contenti, qui sunt 27, 69, 150, quorum ultimus subtrahendus relinquit quadratum 4, ex valore $d = 2$ delimito. Hinc igitur erit $a = 7$, $y = 57$ et $x = 16$.

§. 8. Nacti ergo sumus aliam insuper resolutionem numeri $N = 10003$, cognitae similem, quae est $10003 = 100^2 + 3 \cdot 57^2$. Quare cum jam habeamus $\lambda = 3$, $a = 100$, $b = 1$, $x = 16$ et $y = 57$, hinc ex §. 1. erit $\frac{3p}{q} = \frac{16}{58} = 3 \cdot \frac{56}{58} = 3 \cdot \frac{2}{3}$ ideoque $p = 2$ et $q = 3$, consequenter $3pp + qq = 21$, quod per 3 depressum dat 7, qui numerus reversa est divisor numeri propoliti 10003, quoto existente $= 1429$, numero primo.

§. 9. Hoc exemplum innititur formula $3xx + yy$, de qua satis rigide jam est demonstratum omnes numeros, qui unico modo in ea continentur, certe esse primos; quae proprietates

prietas absolute necessaria est ad omnes numeros primos hac ratione explorandos Nisi enim formula $axx + \beta yy$ hac proprietate gaudeat, de numeris, qui unico modo in ea continentur, tuto pronunciari non potest, eos esse primo; veluti casu $a = 11$, quo in formula $11:xx + yy$ numerus 15 unico tantum modo continetur, etiam si certe non sit primus.

§. 10. Quin etiam haec formula generaliori modo ita exhiberi potest: $axx + \beta yy$, de qua iidem est demonstratum, omnes numeros, qui duplici modo in ea continentur, non esse primos, sed compositos, quorum adeo factores facile assignari poterunt. Si enim duplici modo fuerit $N = aax + \beta\beta b$, tum vero etiam $N = aAA + \beta BB$, hinc formetur fractio $\frac{p}{q} = \frac{a \pm \beta}{b \pm \beta}$, tum semper formula $pp + qq$ praebebit factorem numeri N , postquam scilicet per minores divisores $\alpha, \beta, \gamma, \delta$, quos admittit, fuerit deversa.

§. 11. Contra vero, si quisquam numerus N unico tantum modo in formula $axx + \beta yy$ continetur, inde non semper concludi potest, hunc numerum esse primum, quidem innumerabiles exhiberi possunt huiusmodi formulae, in quibus etiam numeri compositi semel tantum continentur, cujus rei exemplum jam supra attulimus. Hanc ob circumstantiam maxime necessarium est, formulas huius posterioris indolis a prioribus distinguere atque a praesenti negotio prioris excludere. Demonstravi autem alio loco regulam, cujus ope formae posterioris indolis dignosci atque adeo e medio tolli poterunt. Regula autem ista ita se habet:

§. 12. Proposita formula $axx + \beta yy$, de qua quaeritur, utrum in ea numeri compositi unico tantum modo contineri queant nec ne, consideretur haec formula $\alpha\beta + \gamma\gamma$, ubi ipsi α, β, γ omnes

α, β omnes successively tribuantur valores ad productum $\alpha\beta$ primi, sive si ipsius α valores excludantur, qui cum hoc producto communiem habent divisorem; tum vero sufficit hos numeros ex formula $\alpha\beta + \gamma\gamma$ resultantibus tantum usque ad terminum $\alpha\beta$ continuare. Quod si enim omnes hi numeri fuerint primi, formula $\alpha\beta + \beta\beta\gamma$ tuto in nostro negotio usurari poterit; si autem unusquis inter eos fuerit numerus compositus, tum haec formula penitus erit rejicienda. In hoc autem iudicio probe est tenendum, numeros quadratos instar primorum esse spectandos, pariter ac dupla primorum, et potestates binarii, quae circumstantia summi in dijudicatione nostra est momenti.

§. 13. Illustremus hanc regulam aliquibus exemplis; ac primo quidem proposita sit haec forma: $xx + 2yy$, unde consideretur haec expressio: $14 + 2z$, ubi ipsi z successively tribuantur valores ad 14 primi 1, 3, 5, unde resultant numeri 15, 17, 19, quorum primus cum jam sit compositus, pariter ac tertius, formulam propositam tanquam in eam exclusi oportet perinde atque haec ad idem iudicium deducentem: $14xx + yy$.

§. 14. Proposita formula $3cxx + yy$, in forma $3c + 2z$ ipsi z tribuantur valores impares ad 3c primi, qui sunt 1 et 7, unde oriuntur numeri 31 et 79, qui cum ambo sint primi, haec formula in praesenti negotio tuto adhiberi poterit, nec non sequentes lineae oriundae: $15xx + 2yy$, $6xx + 5yy$, $1cxx + 3yy$.

§. 15. Proposita sit formula $12cxx + yy$; ubi in forma $12c + 2z$ ipsi z tribui debent hi valores impares ad 12c primi: 1, 7, 11, 13, 17; numerus enim 19 praebet numerum

meritum, quadruplum producti $\alpha\beta = 120$ superantem. Inde autem colliguntur numeri sequentes: 121, 169, 241, 289, 409, qui cum sint vel primi vel quadrati, hinc concludimus formulam propositam, perinde ac sequentes inde desumptas, scilicet: 4. $xx + 3yy$; 24 $xx + 5yy$; 15 $xx + 9yy$, tanquam idoneas spectari debere et in examine tuto admitti posse.

§. 16. Sit proposita formula $-xx + 5yy$ et in hac expressione 35 + zz valores ipsi z tribuendi erunt: 1, 7, 11, 17, 19, 23, 25, 29, qui praebent hos numeros: 36, 39, 44, 51, 55, 64, 76, 91, 106, ubi cum adeo lex sint compositi, hanc formulam omnino excludi oportet.

§. 17. Habeatur formula $15xx + 7yy$ et in expressione $105 + zz$ ipsi z tribuendi erunt hi valores ad 105 primi: 1, 2, 4, 8, 11, 13, 16, 17, qui praebent hos numeros, omnes pro primis habendos: 106, 109, 121, 109, 226, 273, 361, 394 unde sequentes formulae in classem idoneorum sunt ponendae: $105xx + yy$; $35xx + 3yy$; $21xx + 5yy$; $15xx + 7yy$.

§. 18. Addamus his exemplis examen formulae $57xx + yy$: et nument loco z successive scribendi, scilicet 1, 2, 4, 5, 7, 10, 11, 13 hos praebent valores formae $57 + zz$ notatu dignos: 58, 61, 73, 82, 106, 121, 157, 178, 226, qui omnes sunt vel primi, vel quadrati vel dupli primorum, ita ut formula proposita certe sit inter idoneos referenda.

§. 19. Haec sufficient ad insignem simulque facillimum usum nostrae regulae illustrandum, cuius ope casus idoneos formulae $\alpha xx + \beta yy$ ab ineptis discernere valeamus; qua igitur regula stabilita, illos casus optimo cum successu adhibere poterimus ad numeros quosvis in talibus formulis contentos, utrum sint

sint primi nec ne, perferuntandos. Proposito scilicet numero quocunque N facile erit illum pluribus modis ad talem formulam $\alpha xx + \beta yy$ reducere, quo facto talis eligatur casus, qui per regulam supra datam non-excludatur, ac discipietur, utrum ille numerus N unico tantum modo, an vero pluribus, in hac forma continatur; Priore enim casu certe erit primus, posteriori vero compositus, cujus factores ope methodi supra traditae facile assignare licebit.

EXEMPLUM I

§. 20. Proponatur numerus $N = 100003$, qui manifeste non est primo in forma $10xx + 3yy$ continetur, existente $x = 100$ et $y = 1$. Videamus ergo, an iste numerus adhuc alio modo in eadem forma continetur. Hunc in finem ponamus $100003 - 3yy = 10xx$, atque ut divisio per 10 succedat, ponatur $y = 1 + 10z$, hincque oriatur $10000 - 6z - 30zz = 10x$, sive facta adhuc divisione per 4 erit $2500 - \frac{3}{2}z - \frac{15}{2}zz = 4x$. Hinc igitur, prouti z fuerit vel par vel impar, formemus duos casus principales. Pro primo scilicet sit $z = 2a$, oriatur aequatio $A = 2500 - 3a - 30aa = \frac{x}{4}$. Pro altero casu sit $z = 2b - 1$, oriatur ista: $B = 2494 + 27b - 30bb = \frac{x}{4}$.

Evolutio formulae

$$A = 2500 - 3a - 30aa = \frac{x}{4}$$

§. 21. Hic statim patet, sumto $a = 0$ prodire quadratum, praebens casum cognitum $x = 100$ et $y = 1$. Jam iterum duos casus distinguere conveniet, quibus a est numerus vel par vel impar: ac priori quidem evidens est pro a sumi debere numerum pariter patrem. Sit ergo pri-

no $a = 4c$, et facta divisione per 4 oritur haec aequatio:
 $C = 625 - 3c - 120c = \frac{1}{10}xx$. Hic igitur, quia c lam
 positive quam negative sumi poterit, numeri a 625 successi
 five subtrahendi ordine erunt sequentes in forma $12:cr + 3c$
 contenti: 117, 123, 474, 486, unde autem nullum plane
 quadratum resultat.

§. 22. Tribuamus nunc ipsi a valorem imparem, qui
 sit $a = 4d + 1$, et facile est videre, solum signum inferioris
 valere posse. Fiat igitur $a = 4d - 1$, et aequatio per 4
 divisa evadet $D = 2473 + 225d - 45cd$. Hinc igitur a
 numero absoluto 2473 successiive subtrahi debent numeri
 sequentes in forma $45:cd$ contenti, scilicet 225, 705,
 1464 , 2376, unde iterum nullum quadratum resultat.

Evolutio Formulae.

$$B = 2494 + 27b - 3:bb = \frac{xx}{4}$$

§. 23. Hic statim patet, si pro b capitur numerus
 par, eum impariter parem esse debere. Sit igitur $b = 4e + 2$,
 et facta divisione per 4 aequatio hinc resultans erit
 $B = 627 - 93e - 120e = \frac{xx}{4}$. A numero ergo absoluto 627
 subtrahi debent sequentes in forma $12:ee$ contenti,
 qui sunt 27, 213, 294; ubi autem nullum quadratum oc-
 currit.

§. 24. Denique pro b numeros impares tentemus. Fac-
 ile autem patet, poni debere $b = 4f - 1$, ita tamen, ut
 numerus sit impar, qui ergo ponatur $= 2g + 1$, eritque $b = 4g + 3$,
 unde oritur haec aequatio: $2305 - 1224g - 492g = \frac{xx}{4}$. Hic
 ergo unicus numerus 696 ab absoluto 2305 subtrahendus
 occurrit, unde autem numerus non-quadratus relinquatur.

Quo-

Quoniam igitur ex toto hoc calculo nullus numerus qua-
 dratus prodit, jam certo pronunciare possumus numerum
 propositum 100003 esse primum.

Brevior Methodus

in hunc numerum inquirendi.

§. 25. Quoniam ante habuimus $10003 = 10,100^2 + 3.1^2$,
 etiam statim poterimus $10003 = 40.50^2 + 3.1^2$, ita ut sit
 $a = 40$ et $\beta = 3$, qui casus, nisi supra vidimus, admittitur. Hanc
 ob rem statim 100003 $= 3\gamma\gamma = 40xx$, statque $\gamma = 1 + 20x$,
 et facta divisione per 40 statim pervenimus ad hanc aequa-
 tionem: $2500 - 5x - 302x = xx$; ubi duo casus considerandi
 occurrunt, prouti x fuerit numerus par vel numerus impar,
 quorum utrumque seorsim evolvamus.

§. 26. Pro priore casu evidens est pro x sumi debere
 numerum pariter parem. Sit ergo $x = 4a$, et facta divisione
 per 4 oritur haec aequatio: $625 - 3a - 120aa = \frac{xx}{4}$. Hic
 ergo a numero absoluto 625 sequentes ex forma $12:aa + 3a$
 defuncti sunt subtrahendi: 117, 123, 474, 486. Hinc
 autem nullum occurrit quadratum, praeter casum $a = c$, qui
 per se jam est notus.

§. 27. Superest ut pro x numerum imparem scribamus,
 qui sit $x = 2b - 1$, factque aequatio $2473 + 114b - 120bb = xx$,
 qui numerus cum sit impar, ideoque debeat esse formae
 $8n + 1$, evidens est sumi debere $b = 4c$, unde prodit haec
 aequatio: $2473 + 456c - 1920c = xx = \square$. Sumto igitur
 $c = 1$ numeri a 2473 subtrahendi erunt 1464 et 2376,
 quorum neuter quadratum relinquunt. Hinc eadem, quam
 supra, conclusio: numerum 100003 certo esse primum. Ex

C 2

posse-

posteriori autem hujus numeri examine intelligere licet, in genere eo majus lucrum expectari posse, quo majores numeros pro α et β accipere liceat.

Exemplum 2.

§. 28. Propositus sit numerus $N = 1000003$, qui manifeste continetur in formula: $3 \cdot 1^2 + 1 \cdot 1000$. Quoniam autem, uti modo monuimus, expedit pro α et β numeros majores adhibere, idem quoque numerus facile repetitus est contineri in forma $3 \cdot 577^2 - 19 \cdot 8^2$, ita ut sit $\alpha = 3$ et $\beta = 19$, ideoque $\alpha\beta = 57$, qui numerus, uti commode evenit, inter idoneos jam supra est relatus. Hanc ob rem statim $1000003 = 3xx = 19yy$ atque ipsi x talis valor tribui debet, ut formula haec divisionem per numerum 19 admittat. Quare cum in casu cognito sit $x = 577 = 3 \cdot 19 + 7$, ponamus hic $x = 7 + 19z$, et facta divisione per 19 oriatur haec aequatio: $52624 = 42z - 57zz = 19y$. Ubi statim duoculus considerandi occurrunt proati z fuerit numerus par vel impar. Pro priori casu statuitur $z = 2a$, et aequatio per 4 divisa ita se habebit: $13155 = 21a - 5^2aa = a$, quam vocemus = A. Pro altero casu ponatur $z = 4b - 1$, quoniam facile est videre, valorem $z = 4b + 1$ penitus excludi. Hinc ergo oriatur haec altera aequatio principalis: $B = 52609 + 288b - 912bb = 19y$. Has igitur duas aequationes A et B, principales, seorsim ulterius evolvamus.

Evolutio Formulae

$A = 13155 = 21a - 5^2aa = a$

§. 29. Hic subdiviso in duos alios casus insitui debet, quorum quisque iterum seorsim evolvatur. Sit primo a numerus

merus par, et quidem $a = 4c$, qui valor, in aequatione A substitutus, producit sequentem aequationem, postquam scilicet divisio per 4 fuerit facta: $C = 3259 - 21c - 228ce = 19y$. Hic ergo a numero absoluto 3289 successively subtrahi debent numeri in forma $228ce + 21c$ contenti, qui sunt: $19c$ numerus negativus: 267, 870, 1959 $19c$ numerus positivus: 249, 954, 2115 unde autem nullum quadratum resultat.

§. 30. Sumamus ergo pro a numerum impari, qui manifeste debet esse formae $4d - 1$. Facta igitur substitutione $a = 4d - 1$, simulque divisione per 4, oriatur haec aequatio: $D = 3252 + 91d - 228dd$. Hinc numeri formae $228dd \pm 93d$ a numero absoluto 3289 successively subtrahendi erunt $19d$ numerus negativus: 135, 726, 1773, 3276 $19d$ numerus positivus: 321, 1098, 2331 quorum quartus prioris seriei dat quadratum 4 ex casu $d = 4$, unde sit $y = 8$, qui casus jam est cognitus, praeter quem hic nullum amplius quadratum occurrit.

Evolutio Formulae

$B = 52609 + 288b - 912bb = 19y$

§. 31. Hic ergo a numero absoluto 52609, successively subtrahantur numeri in formis $912bb \pm 288b$ contenti, quos hic in gemina columna, una cum eorum differentis, tam pro valoribus ipsius b positivis quam negativis repraesentemus:

b	$912bb - 288b$	Diff.	b	$912bb + 288b$	Diff.
0	0	624	0	0	1200
1	624	2448	1	1200	3024
2	3072	4272	2	4224	4848
3	7344		3	9072	

ubi differentiae iterum manifesto augmento constanti 260

ubi differentiae, quas a quadrato aa continua subtrahi oportet

§. 32. Jam vero loco successivae subtractionis numero-
rum in forma $912bb \pm 288b$ contentorum differentiae eorum
augumento confanti 1824 crescentes continuo subtrahi pote-
runt, quos in subfidium calculi hic subjungamus

624	-	-	-	-	1200
2448	-	-	-	-	3624
4272	-	-	-	-	4848
6096	-	-	-	-	6672
7920	-	-	-	-	8496
9744	-	-	-	-	10320
11568	-	-	-	-	12144.

§. 33. Nunc igitur hi numeri a numero absoluto 52609
continuo subtrahantur, ac difficiatur, an usquam numerus
quadratus relinquantur, quem calculum commode in duabus
columnis hoc modo repraesentare licet:

52609	-	-	-	-	52609
624	-	-	-	-	1200
51985	-	-	-	-	51409
2448	-	-	-	-	3024
19537	-	-	-	-	48385
4272	-	-	-	-	4848
45265	-	-	-	-	43537
6096	-	-	-	-	6672
39169	-	-	-	-	36865
7920	-	-	-	-	8496
31249	-	-	-	-	28369
9744	-	-	-	-	10320
21505	-	-	-	-	18049
11568	-	-	-	-	12144
9937	-	-	-	-	5905

ubi

ubi nullum plane quadratum occurrit, pariter ac in praec-
edentibus, casu scilicet cognito excepto. Hinc igitur jure
concludimus, numerum propositum, 100003 unico modo
in forma $\xi xy + 19yy$ contineri, ideoque certe esse primum.

§. 34. Ex hoc exemplo clare apparet, quantum in-
terit in formula $2xx + 2yy$ pro α et β majores numeros
investigare, dummodo eorum productum $\alpha\beta$ in classe nume-
rorum idoneorum contineretur, pro quibus inveniendis regu-
la supra fuit exposita. Quamobrem, ut quovis casu statim
appareat, utram tale productum $\alpha\beta$ sit numerus idoneus,
nec ne, tabulam istorum numerorum, quousque eam conti-
nere licuit, hic subjungamus.

Tabula numerorum idoneorum $\alpha\beta$, hac proprietate prae-
ditorum, ut omnes numeri unico modo in formula
 $2xx + 2yy$ contenti certe sint primi:

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

§. 35.

§. 35. Quoties igitur numerum quempiam propofitum ad talem formam $\alpha xx + \beta yy$ reducere licuerit, ut productum $\alpha\beta$ inter numeros istius tabulae continetur, tum haec formula uiripari poterit ad examen, jam faepius alatum, infitendum. Conveniet autem accuratius explicare regulam, cuius ope operationes neceffariae expedite infitui queant, id quod in fequente Problemate offendamus.

Problema.

Propofito numero quantumvis magno N, explorare, utrum is fit primus nec ne?

Solutio.

§. 36. Quo major fuerit ifte numerus N, eo pluribus modis eum in ejuſmodi duas partes reſolvere licebit, quarum utraque habeat factorem quadratum, quae ſint αaa et βbb , ex quibus igitur talem eligi conveniet, ut numerorum α et β productum in tabula modo expoſita continetur, ubi quidem plurimum intererit majores hujusmodi numeros indagare.

§. 37. Talibus igitur numeris inventis ponamus eſſe $N = \alpha aa + \beta bb$, et nunc totam negotium huc redit, ut inveſtigetur, utrum ifte numerus infuper alio modo in eadem forma $\alpha xx + \beta yy$ contineatur, nec ne. Si enim talis caſus occurrat, numerus propoſitus non erit primus, atque tum adeo ejus factores, per praeccepta ſupra data, aſſignare licebit. Sin autem nullus talis caſus occurrat certo pronunciarie poterimus, iftum numerum N eſſe primum.

§. 38.

$$\begin{array}{r} 6561 \\ 2040 \\ \hline 4521 \end{array} \quad \begin{array}{r} 6561 \\ -1000 \\ \hline 7561 \end{array}$$

34

§. 38. Iſta autem inveſtigatio ſequenti modo generatiter infituitur: Ponamus eſſe $N = \alpha xx + \beta yy$, ita ut fit $\alpha aa + \beta bb = \alpha xx + \beta yy$, unde formemus hanc aequationem: $\alpha aa - \beta yy = \alpha xx - \beta yy$, ubi praetabit pro α majorem numerum aſſumere, pro β vero minorem. Hic igitur ſtatim patet, pro y ejuſmodi numerum accipi debere, ut formula $\beta yy - hb$ diviſorem α involvat. Evidens enim eſt non ſolum numeros α et β primos inter ſe eſſe debere, ſed etiam tam x ad β quam y ad α primum eſſe ſtatuumdum.

§. 39. Quoniam igitur $\beta y - hb$ per α diviſibile eſſe debet, ante omnia erit diſpiciendum, utrum α fit numerus primus nec ne. Priori enim caſu vel $y + b$ vel $y - b$ diviſorem habere debet α , unde unicus tantum caſus exurgit; ſin autem α involvat factores, tum utique fieri poſſeſt, ut alter contineatur in forma $y + b$, alter vero in forma $y - b$; unde praeter illum caſum adhuc unus vel plures novi caſus evamirari debebunt. Unicus ſcilicet caſus occurreret, ſi α duos tantum habeat factores; ſin autem plures factores involvat tum etiam pluribus modis in duos factores reſolvi poterit, quos ſingulos ſeorſim perſcrutari oportet.

§. 40. Ponamus igitur in genere eſſe $\alpha = \mu \nu$, et quovis caſu facile patebit, quot modis numerus α in binos hujusmodi factores reſolvere licet, quotcumque etiam involvat diviſores; neque etiam numeri primi hinc excludantur, quippe quibus caſibus vel pro μ vel pro ν unitas erit ſcribenda. Hinc ergo ponamus $y + b = \mu p$ et $y - b = q$, ita ut fit $\beta y - hb = \mu pq$, et facta diviſione per α aequatio deinceps reſolvenda erit $aa - \beta pq = xx$.

Novae Acta Acad. Imp. Scient. Tom. XIV.

D

§. 41.

35

Iſte jam occurrat numerus quadratus * 361 = 19² ipſi βy aequandus. Fit igitur $y = 19$, $s = 5$, hincque $x = 4^2$,

§. 41. Numeri autem p et q hoc modo commodissime reperiuntur. Eliminata enim litera y habebimus $ab = v \cdot p - q$. Jam quaeratur fractio $\frac{m}{n}$ proxime aequalis fractioni $\frac{p}{q}$, ita ut $m \cdot n - n \cdot p = 1$; tum capiatur $p = s - nb$ et $q = \mu s - amb$, ubi jam pro s numerus quoscunque integros accipere licet, sive positivos sive negativos, et aequatio nostra resolvenda inducet hanc formam:

$$aa - \beta(s - amb)(\mu s - amb) = xv,$$

ubi jam pro s ejusmodi valores investigari debent, ut ista forma ad $\beta(\mu s - amb) : \mu s - amb$ quadratum evadat. Totum negotium igitur eo redit, ut dispiciatur, an, tribuendo litterae s successively omnes valores tam positivos quam negativos, a zephyra ad terminum usque qui numeros praebet negativos an dico usquam quadratum resultare possit.

§. 42. Evolvam s igitur singulos numeros, quos a quadrato ad subtrahi oportet quos littera S designemus, ita ut sit $aa - S = xv$. Habebimus ergo

0	$41 \ m^2 n^2 b^2$	1
± 1	$2(\nu \pm amb)$	2
± 2	$2(2\nu \pm amb)$	3
± 3	$2(3\nu \pm amb)$	4
± 4	$2(4\nu \pm amb)$	5
± 5	$2(5\nu \pm amb)$	6

Quoniam isti valores sat simplici lege progrediuntur, perpendamus eorum differentias, ac repelemus:

- II - I = $2\nu \pm 2b$ ($m\nu + n\nu$)
- III - II = $2\nu \pm 2b$ ($m\nu + n\nu$)
- IV - III = $2\nu \pm 2b$ ($m\nu + n\nu$)
- V - IV = $2\nu \pm 2b$ ($m\nu + n\nu$)

quae-

rogo decrecentes: 1640, 600, — 440 — 1480, — 2570, quia inde nullam quadratum resultat, concludimus numerum 6401 esse primum.

quae manifesto in progressionem arithmetica progrediuntur, cujus differentia est $2\beta\mu\nu$.

§. 43. His differentis inventis nihil aliud superest, nisi ut eae ordine continuo a quadrato aa , primo termino minuto subtrahantur. Ab aa scilicet primo subtrahatur prima differentia; tum vero a residuo secunda, a residuo hinc nato tertia, porro quarta etc. quoad ad numeros negativos perveniatur; hisque operationibus ita continuatis dispiciatur, utrum usquam numerus quadratus remanserit; quod si non contigerit, numerus propositus certe pro primo erit habendus; sin autem usquam quadratum prodierit, ejus radix dabit valorem ipsius x , et notato valore ipsi s conveniente etiam reperiri poterit alter numerus y , siquidem erit $y = b + \mu\nu s - 2\nu mb$. Quia vero supra sumimus $m\nu - n\mu = 1$, erit nunc $y = \mu\nu s - b(m\nu + n\nu)$.

§. 44. Quod si numerus propositus N fuerit vehementer magnus, numerum harum operationum non parum diminuire licebit, si numeri S , quos a quadrato aa continuo subtrahi oportet, in duas classes distinguantur, prouti pro s valores sive pares sive impares accipiantur. Priore enim casu, cum sit vel $s = 2n$, vel $s = 4n + 1$, plerumque eveniet, ut alter casus penitus excludatur, ob eam proprietatem, quod inde pro S numeri prodierint impariter pares. Eodem modo si pro s sumatur numerus impar, erit vel $s = 4n + 1$, vel $s = 4n - 1$, quarum formarum altera penitus excluditur, quia omnia quadrata imparia sunt formae $8n + 1$, ita ut hoc modo numerus operationum ad semissem redigatur.

§. 45. Quoniam initio posuimus $a = \mu\nu$, hosque numeros μ et ν ut primos inter se spectavimus, id quod possimum

D^2

999601 756841
840 59400
998761 727441

num de factoribus imparibus est tenendum, notetur si a sit numerus par et potestatem quamcumque ipsius binarii involvat, tunc utramque factorem $y + b = \mu p$ et $y - b = \nu q$ parem esse debere. Unde si ipsi μ valor par tribuatur, nihil impediti quo minus et ν par statuatur, id quod facile in exemplis oblati observare licet. Ita cum numerus $5 \cdot 20 = 8 \cdot 5 \cdot 13$ in tabula superiore numerorum idoneorum continetur, fecundum praecepta hic tradita in genere numerus $N = 4caa + 13bb$ evolvamur.

Evolutio generalis

numerorum contentorum in forma

$$N = 4: aa + 13bb.$$

§. 46. Hic igitur erit $a = 40$ et $\beta = 13$, atque hinc numeros x et y ex sequenti forma elicere licebit:

$$4caa - 13(y^2 - bb) = 4cax$$

ubi statim duos casus distingui conveniet, quibus est vel $\mu = 10$ et $\nu = 4$, vel $\mu = 20$ et $\nu = 2$, quia scilicet ambobus factores debent esse pares.

Casus I.

quo $\mu = 10$ et $\nu = 4$.

§. 47. Hic igitur erit $y + b = 10p$ et $y - b = 4q$, hincque $b = 5p - 2q$. Fractioni ergo $\frac{5}{2}$ proxima erit $\frac{1}{2}$, unde statuamus $p = 2s + b$ et $q = 5s + 2b$, quibus valoribus substituitis aequatio resolvenda erit

$$aa - 13(2s + b)(5s + 2b) = 4cx.$$

Posto igitur brevitate gratia numerum a quadrato aa subtrahendum, scil. $13(2s + b)(5s + 2b) = S$, si loco s fac-

cessit-

cessive scribamur numeros $0, +1, +2, +3$, etc. valores ipsius S cum suis differentiis, quorum usum jam saepius explicavimus, ita se habebunt:

5	S	Dif.
0	26bb	130 ± 117bb
+1	13(2 ± b)(5 ± 2b)	390 ± 117bb
+2	13(4 ± b)(13 ± 2b)	650 ± 117bb
+3	13(6 ± b)(15 ± 2b)	1910 ± 117bb
+4	13(8 ± b)(20 ± 2b)	etc.
etc.	etc.	etc.

quae differentiae continuo crescent augumento constanti 260, unde facile, quousque libuerit, continuabuntur; ubi autem probe notetur, subtractionem differentiarum fieri debere a numero $aa - 26bb$.

Casus II.

quo $\mu = 20$ et $\nu = 2$.

§. 48. Hic igitur erit $y + b = 20p$ et $y - b = 2q$ unde, cum hinc fiat $b = 10p - q$, sumto $p = s$ fiet $q = 10s - b$, et aequatio resolvenda erit: $aa - 13pq = xx$ sive $aa - 13s(10s - b) = xx$. Posto igitur brev. gr. $13(10s - b) = S$, valores ipsius S , prouti s fuerit vel 0 , vel 1 , vel 2 , vel 3 , erunt sequentes:

s	S	Dif.
0	0	130 ± 13b
+1	13(10 ± b)	390 ± 13b
+2	26(20 ± b)	650 ± 13b
+3	39(30 ± b)	910 ± 13b
+4	52(40 ± b)	etc.
etc.	etc.	etc.

ubi

ubi differentiae iterum manifesto augmento constanti 260 crescunt, quas igitur loco S continuo ab ipso quadrato aa subtrahi oportet.

Alia Evolutio

numerorum formae $4c\ aa + 13\ bb$.

§. 49. Cum habeatur aequatio: $4c\ aa - 13\ (yy - bb) = 4c\ xx$, tollamus primo tantum factorem parem s, et quia b denotat numerum imparem, evidens est, dummodo pro y etiam sumatur numerus impar, formulam $yy - bb$ fore divisibilem per s. Ponatur igitur in genere $y = az \dots b$, et facta divisione per s habebimus hanc aequationem: $5aa - \frac{13}{s}(az + bz) = 5xx$; ubi evidens est, membrum medium semper esse integrum. Nunc igitur loco z talem numerum assumi oportet, ut vel z, vel z . b factorem habeat s: perinde autem est inter horum factorum per s divisibilibus reddatur, propterea quod inter se sunt permutabiles, mutato scilicet signo ipsius b. Ponatur igitur $z = 5s$ et facta divisione per s aequatio, cui satisfieri oportet, erit: $aa - \frac{13}{s}(5ss \pm bs) = xx$.

§. 50. Hic igitur a quadrato aa subtrahi debent numeri in forma $\frac{13}{s}(5ss \pm bs)$ contenti, quae si vocetur = S, valores ipsius S erunt, uti in sequenti tabula cum suis differentiis exhibentur.

s	S	Dif.
1	$13(5 \pm b)$	$\frac{13}{s}(5 \pm b)$
2	$\frac{13}{2}(20 \pm 2b)$	$\frac{13}{2}(15 \pm b)$
3	$\frac{13}{3}(45 \pm 3b)$	$\frac{13}{3}(45 \pm b)$
4	$\frac{13}{4}(80 \pm 4b)$	$\frac{13}{4}(35 \pm b)$
etc.	etc.	etc.

ubi

ubi differentiae, quas a quadrato aa continuo subtrahi oportet, augmento constanti $\frac{13}{s} \cdot 10 = 6$; crescunt.

§ 51. Quin etiam unica substitutione totus numerus, 40 factum tolli potest, poriendo $y = rs + b$; tum enim ob $yy - bb = 15c\ ss + 2c\ bs$, dividendo per 40 factum pervenitur ad hanc aequationem: $aa - \frac{13}{40}(5ss + bs) = xx$, uti modo invenimus. Hoc igitur artificio semper uti licebit, quoties littera a valorem habeat parem, atque adeo cum potestate binarii simul unum factorem primum tollere licebit. Veluti si $z = 2^{\lambda} \cdot f \cdot k$, ita ut formula $yy - bb$ per hunc valorem divisibilis reddi debeat, factum poni poterit:

$$y = 2^{\lambda} - 1 f s + b; \text{ tum enim erit:}$$

$$yy - bb = 2^{2\lambda} - 2 f f z z + 2^{\lambda} b f z, \text{ quae forma}$$

$$2^{2\lambda} - 2 f f z z + 2^{\lambda} b f z \text{ per } 2^{\lambda} f \text{ dividit ab it in hanc:}$$

$$2^{\lambda} - 2 f z + b z; \text{ quod igitur cum fuerit praestitum, reliqui factores per praecepta generalia, alibi tradita, facili e medio tolli poterunt. Et adhuc alia, eaque simplicissima evolutio formulae } N = 40aa + 13bb.$$

§. 52. Cum posito $N = 4c\ xx + 13\ yy$ aequatio prima fundamentalis hoc modo repraesentetur: $13bb - 4c(xr - aa) = 13yy$, observalle juvabit, eam unica operatione resolvvi posse. Ponendo $x = 13s + a$. Facta enim substitutione et divisione per 13 pervenietur ad hanc aequationem simplicissimam: $bb - 4c(13ss + 2 \cdot as) = yy$. Hic igitur a quadrato bb successive subtrahi debent valores formulae: $4 \cdot (13ss \pm 2as)$, qui ita (posita hac formula br. gr. = S) ordine cum suis differentis disponantur:

S	S	Diff.
0	0	4 (13 ± a)
+ 1	40 (13 ± 2a)	40 (39 ± a)
+ 2	40 (52 ± 4a)	40 (65 ± 2a)
+ 3	40 (117 ± 6a)	40 (91 ± 2a)
+ 4	40 (208 ± 8a)	etc.
etc.	etc.	etc.

ubi differentiae per augmentum confans 40 . 26 = 1040 progrediuntur.

Hanc jam potterem resolutionem maxime succinctam aliquot exemplis illustrare operae pretium erit.

Exemplum I.

§. 53. Sumatur $b = 81$ et $a = 1$, ita ut numerus examinandus sit 85333. Hic ergo differentiae a quadrato $bb = 6561$ continuo subtrahendae erunt $4c (13 \pm 2)$; $4c (39 \pm 2)$; etc. quae crescent augmento constanti $4c . 26 = 1040$; unde ob signa ambigua totus hic calculus per duas columnas abfolvi poterit:

6561	-	-	-	-	6561
600					440
5961	-	-	-	-	6121
1640					1480
4321	-	-	-	-	4641
2680					2520
1641	-	-	-	-	2121

Quoniam igitur nullum residuum ex hac subtractione naturam quadratum deprehenditur, tuto concludere possumus hunc numerum 85333 esse primum.

Exem-

Exemplum 2.

§. 54. Maneat $b = 81$ sitque $a = 10$, et numerus examinandus erit $N = 89293$. Hic igitur a quadrato $bb = 6561$ subtrahenda erit differentia $4c (13 \pm 20)$, ideoque 1320 et 280; sequentes autem differentiae crescent augmento = 1040. Hinc calculus ita se habet:

6561	-	-	-	-	6561
1320					280
5241	-	-	-	-	6841
2360					760
2881	-	-	-	-	6081
					1800
					4281
					2840
					1441

Quoniam igitur hic etiam nullum quadratum occurrit, numerus propositus 89293 certe est primus.

Exemplum 3.

§. 55. Maneat adhuc $b = 81$ famaturque $a = 19$, ut sit $N = 99733$; et ad examen hujus numeri necesse est ut a quadrato 6561 subtrahantur differentiae augmento 1040 crescentes, quarum primae sunt 2040 et 1000, hoc modo:

Novae Acta Acad. Imp. Scient. Tom. XIV.

E 6561

34

6561	-	6561			
2c40		-1020			
4521		7561			
3c80		40			
14+1		7521			
		1080			
		64+1			
		2120			
		4321			
		3160			
		1161			

Quia igitur hic nullum quadratum relinquit, numerus 99733 etiam pro primo est habendus.

Exemplum 4.

§. 56. Adjungamus exemplum numeri propositi. Maneat iterum $b = 81$ sitque $a = 17$, erit $N = 90853$ et subtractio differentiarum ita se habebit:

6561	-	6561			
1550		840			
4051		7421			
2920		200			
1761		7201			
		1240			
		5961			
		2280			
		3681			
		3320			
		* 361			

Hic

35

Hic jam occurrit numerus quadratus * 361 = 19' ipsi yy aequandus. Fit igitur $y = 19$, $s = -5$, hincque $x = 48$, unde factor numeri propositi inveniri potest quaerendo fractionem $\frac{p}{q} = \frac{x \pm a}{y \pm b} = \frac{48 \pm 17}{19 \pm 5} = \frac{1}{2}$; hinc factor est $4c \cdot pp + 17 \cdot qq = 40 \cdot 1^2 + 13 \cdot 3^2 = 23$, qui ad minimo; terminos reductus est $19 \cdot 1^2 + 13 \cdot 1^2 = 23$. Alter factor ex eadem fractione derivari potest, si sumatur $\frac{p}{q} = \frac{65}{12}$; hinc enim fiet $4c \cdot pp + 13 \cdot qq = 40 \cdot 65^2 + 13 \cdot 62^2$, qui factor per $4 \cdot 13$ depressus dat $10 \cdot 65 \cdot 5 + 31^2 = 4211$; at revera est $96853 = 23 \cdot 4211$.

Exemplum 5.

§. 57. Sumatur $a = 40$ et $b = 1$ et numerus examinandus erit $N = 64c13$. Hic autem modus procedendi a precedentibus diversus adhiberi debet; quia enim a quadrato bb subtrahi deberent numeri in forma $4c(13ss + 50s)$ contenti, quod autem fieri nequit, hic solum signum inferius valebit, ita ut successe ad quadratum $bb = 1$ addi debeant numeri in forma $S = 4c(50s - 13ss)$ contenti, quos cum suis differentis hic adjungamus.

s	S	Diff.
0	0	40 . 67 +
+ 1	40 . 67	40 . 41 +
+ 2	40 . 108	40 . 15 +
+ 3	40 . 123	40 . 11 -
+ 4	40 . 112	etc.
etc.	etc.	etc.

ubi differentiae decrescunt quantitate constanti $40 \cdot 26$; quamobrem, si ad unitatem primo addamus numerum $40 \cdot 67 = 2680$, tum vero differentias sequentes decremento E_2

1040

est primus, ejusque factores sequenti modo assignari possunt. Remittitur fractio: $p = \frac{1+2r}{5-2r}$ et ob signa ambigua hæc quatuor habebuntur fractiones: $\frac{11}{25}, \frac{1}{10}, \frac{11}{30}, \frac{1}{3}$. Hinc forma factoris $5+2pp + 2q$ ex priore fractione fit $84 \cdot 1^2 + 25^2$, sive per 25 depressus, $36 + 25 = 15 + 14 = 29$, qui idem factor etiam prodit ex quarta fractione $\frac{p}{q} = \frac{1}{30}$; hinc enim fit factor $= 840 \cdot 1^2 + 30^2 = 14 + 15 = 29$. Alter factor vel ex secunda vel tertia fractione colligitur; sumto enim $p = \frac{11}{25}$ fit factor $= 540 \cdot 41^2 + 81r^2$, qui per 6 depressus est $= 14 \cdot 41^2 + 27 \cdot 405 = 34469$. Idem prodit ex fractione $\frac{p}{q} = \frac{11}{30}$; at vero revera est $29 \cdot 34469 = 99961$.

§. 61. Ex hoc exemplo luculenter apparet, quanti momenti sint numeri idonei majores in perferendis numeris. Pira grandibus, utrum sint primi nec ne. Cum igitur numerus 1845 sit maximus idoneus, qui in nostra tabula occurrit, operæ pretium erit, in subsidium examinis numerorum vehementer magnorum, sequens problema generalius hinc adungere.

Problemata.

Numerum propositum quantumvis magnum N = 1845aa + bb examinare, utrum sit primus nec ne?

Solutio.

§. 62. Subtrahantur ab isto numero N successive omnes numeri in hac forma: $1845xx$ contenti, et si musquam quadratum remaneat, præter casum cognitum $x = a$, iste numerus certe erit primus. Sin autem aliud præterea quadratum relinquatur, iste numerus erit compositus, ejusque adeo

adeo factores assignare licebit. Verum quia iste calculus ob ingentes numeros continuo subtrahendos non parum est molestus, totum negotium sequenti modo facilius reddi poterit.

§. 63. Statuatur $1848aa - (yy - bb) = 1848xx$ et cum sit $1848 = 8 \cdot 3 \cdot 7 \cdot 11$, ponatur primo $y = 22z + b$ et facta divisione per 8, 11 fiet $21aa - \frac{1}{2}z(11z + b) = 21xz$. Quod si ergo brevitate gratia ponatur $z(11z + b) = 21pq$, æquatio nostra erit $aa - \frac{1}{2}pq = xx$, quæ quadruplici modo locum habere potest:

- I. Si $11z + b = 21p$ et $z = q$.
- II. Si $11z + b = p$ et $z = 21q$.
- III. Si $11z + b = 7p$ et $z = 3q$.
- IV. Si $11z + b = 3p$ et $z = 7q$.

§. 64. Evolvamus seorsim singulos hos modos et primo casu, ob $z = q$, erit $11q + b = 21p$, hincque $q = 2p - \frac{b}{11} = 2p - s$, ita ut $p + b = 11s$, ideoque $p = 11s - b$, et $q = 21s - b = z$, ita ut æquatio nostra fiat $aa - \frac{1}{2}(11s - b)(21s - b) = xx$.

Pro secundo casu. ob $z = 21q$, erit $231q + b = p$, sicque sumto $q = s$ erit $p = 231s + b$ et $z = 21s$, unde æquatio pro hoc casu erit $aa - \frac{1}{2}s(231s + b) = xx$.

Pro tertio casu, ob $z = 3q$, erit $33q + b = 7p$ ideoque $p = 5q - \frac{b}{7} = 5q - r$, ita ut $2q - b = 7r$ et $2q = 7r + b$, sive $q = 3r + \frac{7+b}{2} = 3r + s$, unde fit $r = 2s - b$, hincque $q = 7s - 3b$ et $p = 33s - 14b$, et $z = 21s - 9b$, unde nostra æquatio erit $aa - \frac{1}{2}(7s - 3b)(33s - 14b) = xx$.

Pro

Pro quarto casu, ob $x = 79$, erit $77q + b = 3p$, hincque $p = 2cq - \frac{2}{3}b = 2c9 - s$, exiliente $s = \frac{9c-b}{3}$, unde fit $q = 3s + b$ ideoque $p = 77s + 26b$ et $x = 21s + 7b$, unde aequatio resolvenda erit: $aa - \frac{1}{2}(5s + b)(77s + 26b) = xx$. Ulteriorem calculum sequenti exemplo illustremus.

Exemplum.

§. 65. Sumatur $a = 100$ et $b = 197$, ut numerus examinandus fit $N = 1848aa + bb = 18518809$, ubi facile patet numerum y majorem fore quam 197 ideoque x fore numerum positivum. Hoc observato ad examen hujus ingentis numeri instituendum singulos casus supra a se invicem separatos hic etiam in commodum calculi seorsim evolvamus.

§. 65. Pro casu primo nostra aequatio erit $10000 - \frac{1}{2}(11s - b)(21s - b) = xx$; et quia hinc est $x = 21s - 194$, patet numerum s majorem esse debere quam 18. Statuamus igitur $s = 18 + t$, ut fiat $x = 21t - 10$, atque aequatio nostra hanc indet formam: $10000 - \frac{1}{2}(11t + 1)(1t + 16) = xx$. Numeri S igitur a numero absoluto 10000 subtrahendi, cum suis differentiis tam pro valoribus ipsius t positivis quam negativis, in sequenti tabula referantur:

t	S	Diff.	t	S	Diff.
0	8	38	0	8	193
+ 1	30	269	- 1	185	424
+ 2	299	500	- 2	609	655
+ 3	799	etc.	- 3	1264	etc.
etc.	etc.	etc.	etc.	etc.	etc.

ubi differentiae creverunt augmento constanti 231. At quia primus numerus subtrahendus est $- 8$, continua differentiarum subtrahatio fieri debet a numero 10000, ut sequitur.

10008

10008	10008
38	193
9970	9815
269	424
9701	9391
500	655
9201	8786
731	886
8470	7850
962	1117
7508	6733
1193	1348
6315	5385
1424	1579
4891	3706
1655	1810
3236	1996
1886	
1350	

ex quo igitur calculo nullum quadratum resultat.

§. 68. Pro casu secundo aequatio resolvenda erit $10000 - \frac{1}{2}s(231s + 197) = xx$. Hic ergo a numero 10000 subtrahendi sunt numeri in forma $S = \frac{1}{2}s(231s \pm 197)$ contenti, qui cum suis differentiis hic exhibentur:

s	S	Diff.	s	S	Diff.
0	0	214	0	0	17
+ 1	214	445	- 1	17	248
+ 2	659	676	- 2	265	479
+ 3	1335	etc.	- 3	744	etc.
etc.	etc.	etc.	etc.	etc.	etc.

Novae Acta Acad. Imp. Scient. Tom. XIII.

A

A quadrato igitur 10000 subtrahantur differentiae numero 231 crescentes

10000					10000
214	-	-	-	-	17
9786	-	-	-	-	9983
445	-	-	-	-	248
9341	-	-	-	-	9735
676	-	-	-	-	479
8665	-	-	-	-	9256
907	-	-	-	-	710
7758	-	-	-	-	8546
1138	-	-	-	-	941
6620	-	-	-	-	7605
1369	-	-	-	-	1172
5251	-	-	-	-	6433
1600	-	-	-	-	1493
3651	-	-	-	-	5030
1831	-	-	-	-	1634
1820	-	-	-	-	3396
					1865
					1531

Ubi iterum nullus numerus quadratus occurrit praeter 10000, qui autem dat casum cognitum.

§. 69. Pro casu tertio aequatio examinanda erit
 $10000 - \frac{1}{2}(7s - 591)(33s - 2758) = xx$, quae igitur, posito
 $s = 84 + t$, abibit in hanc:
 $10000 - \frac{1}{2}(7t - 3)(33t + 14) = xx$. Provi igitur t valo-
 rem habet vel positivum vel negativum, numeri subtrahen-
 di

di S continebuntur in hac forma: $\frac{1}{2}(7t \mp 3)(33t \pm 14)$,
 et erunt uti hic exhibentur:

t	S	Diff.	t	S	Diff.
0	- 21	115	0	- 21	116
+ 1	+ 94	346	- 1	+ 95	347
+ 2	440	577	- 2	442	578
+ 3	1017	etc.	- 3	1020	etc.
etc.	etc.	etc.	etc.	etc.	etc.

Jam a numero absoluto 10021 subtrahantur differentiae hic assignatae, et, quousque rei natura postulat, continuatae

10021					10021
115	-	-	-	-	116
9906	-	-	-	-	9905
346	-	-	-	-	347
9560	-	-	-	-	9558
577	-	-	-	-	578
8983	-	-	-	-	8980
808	-	-	-	-	809
8075	-	-	-	-	8171
1039	-	-	-	-	1040
7086	-	-	-	-	7131
1270	-	-	-	-	1271
5866	-	-	-	-	5800
1501	-	-	-	-	1502
4365	-	-	-	-	4358
1732	-	-	-	-	1733
2633	-	-	-	-	2625
1963	-	-	-	-	1964
670	-	-	-	-	661

ubi nullum plane quadratum occurrit. F 2 §. 70.

§. 70. Pro casu quarto aequatio resolvenda est
 $10000 - \frac{1}{2}(3s + 197)(77s + 5122) = xx$. Sit brevitate gratia
 $s = t - 66$, erit $10000 - \frac{1}{2}(3t - 1)(77t + 40) = xx$, sicque
 numeri subtrahendi continentur in forma $S = \frac{1}{2}(3t + 1)(77t + 40)$,
 qui cum suis differentis sunt uti sequitur:

t	S	Dif.	t	S	Dif.
0	-20	137	0	-20	94
+1	+117	368	+1	74	325
+2	485	599	+2	399	556
+3	1084	etc.	+3	955	etc.
etc.	etc.	etc.	etc.	etc.	etc.

Hinc ergo ob primum numerum negativum $= -20$ a numero
 absoluto 10020 subtrahendae erunt differentiae quousque
 opus est continuatae hoc modo:

10020	10020
137	94
9883	9926
368	325
9515	9601
599	556
8916	9045
839	787
8086	8258
1061	1018
7025	7240
1292	1249
5733	5991
1523	1480
4210	4511

1754

§. 5. Proposita autem tali forma generali:

1754	1711
2456	2800
1985	1942
471	858

nullum quadratum in hisce residuis occurrit.

§. 71. Quoniam igitur in omnibus his quatuor casibus nullum quadratum est relictum, certo affirmare possumus, numerum 18518809 esse primum. Ex hoc exemplo simul intelligere licet, satis raro evenire posse, ut in talibus operationibus quadrata relinquantur; hanc ob rem formula $1845aa + bb$ etiam apertissima videtur, ad plures inde numeros primos deducendos; tantum enim opus est valores a et b variare, quod, cum infinitis modis fieri queat, inde haud difficulter plures alii numeri primi tam ingentes reperiri poterunt, ut problemati illo *Fermatiano*, quo numeros primos, dato quovis majores, requiruntur, quodammodo satisfactum.

§. 72. Quoniam in hoc exemplo numeri successively a quadrato aa subtrahendi idem manent, quamvis sumitur $b = 197$, operae pretium erit pro littera a alios quoque valores, possimum minores, fatuere, ubi totus calculus evadet facillimus. Ut autem, quando quadratum occurrit, pro xx etiam valorem respondentem ipsius y assignare liceat, meminisse oportet, in initio hujus solutionis positum fuisse $y = 22z + 197$; tum vero in quaternis casibus allatis fatutum fuisse ut sequitur:

Pro primo casu $z = 215 - 394$, tum vero $s = t + 18$; quoniam, quia ipsi t tam valores positivos quam negativos tribuimus, erit $z = + 21t - 16$; ubi signum superius pro columna prima, inferius vero pro altera valet. Pro

multiplicatoris quaesiti m investigari oportet, quippe quo inventio forma integrata erit

1000 decrecentes: 1640, 600, — 440 — 1480, — 2590, quia inde nullum quadratum refultat, conclusimus numerum 6403 esse primum.

§. 58. His circa evolutionem numerorum in forma $40aa + 13bb$ contentorum expeditis, praestabit usum majorum numerorum idoneorum exemplo illustrasse. Consideretur numerus $N = 999001 = 840 \cdot 34 + 169^2$, et examine- tur, utrum hic numerus propofitus plus uno modo in forma idonea $840xx + yy$ continetur, id quod sine plaris ambagibus sequenti modo satis commode fieri licet.

§. 59. Cum debeat esse $999601 = 840xx + yy$, ipsi x successively tribuantur numeri naturales et numeri S a proposito subtrahendi cum suis differentiis erunt

x	S	Diff.
0	0	1 · 840
1	840	3 · 840
2	1680	5 · 840
3	2520	7 · 840
4	3360	etc.

Loco S jam continuo subtrahantur differentiae augmento 1680 crescentes, quae subtractiones continuas sequenti modo infultantur.

999601

999601	736841
840	59400
998761	72741
250	5080
996241	696361
4200	32760
992041	663601
5880	3440
986161	629161
7560	36120
978601	593041
9240	3780
969361	553241
10920	39480
958441	513761
12600	41160
945841	474601
14280	42840
931361	431761
13960	44520
915661	387241
17640	46200
897961	341041
19520	47880
878641	293161
21020	49560
857641	245601
22680	51240
834661	192361
24360	52920
810601	159441
26040	54600
784561	84841
27720	56280
756841	28361

§. 66. Hic jam duo occurrunt quadrata pro yy . Prius dat $y = 979$ et $x = 7$; posterius praebet casum cognitum $y = 169$ et $x = 34$. Numerus igitur propofitus duplici modo in forma idonea $840xx + yy$ continetur, ideoque non est

Pro secundo casu erat $z = 21s$, unde ob binas columnas cum ambiguitate signorum erit $z = \pm 21s$.

Pro tertio casu erat $z = 21s - 9$, 197, tum vero $s = t + 84$, unde cum ambiguitate signorum erit $z = \pm 21t - 9$.

Pro quarto casu erat $z = 21s + 7$, 197; tum vero posuimus $s = t - 66$, unde cum signorum ambiguitate erit $z = \pm 21t - 7$. His notatis sequentes numeros examini subiciamus.

§. 73. Sit $a = 1$, existente $b = 197$, et numerus propositus erit $N = 40657$. Hic igitur statim ex primo casu occurrit quadratum $aa + 8 = ax$, unde fit $ax = 9$ ideoque $x = 3$, cui respondet valor $t = 0$, ex quo fit $z = -16$, consequenter $y = 155$. Numerus igitur propositus etiam continetur in forma $1848 \cdot 3^2 + 155^2$, unde formatur fractio $\frac{p}{q} = \frac{a \pm x}{b \pm y} = \frac{1 \pm 3}{197 \pm 155}$, cuius valor simplicissimus est $\frac{p}{q} = \frac{1}{21}$. Hinc factor numeri propositi erit $1848pp + qq = 1848 \cdot 1^2 + 21^2$, qui per 21 depressus fit $88 + 21 = 109$. Numerus igitur propositus 40657 non est primus, sed divisorem habet 109, quoto existente 373.

§. 74. Sit $a = 2$ eritque numerus propositus $N = 46201$, Hic neque ex primo neque ex secundo casu quadratum resultat, verum ex casu tertio statim fit $aa + 21 = 25 = x^2$, unde fit $x = 5$, existente $t = 0$, adeoque $z = -9$, consequenter $y = -9 \cdot 2 + 197 = 197$. Ad divisorem igitur numeri propositi explorandum fiat $\frac{p}{q} = \frac{a \pm x}{b \pm y} = \frac{2}{197}$, unde pro factore haec prodit forma: $1848 \cdot 1^2 + 28^2 = 33 + 14 = 47$. At revera est $N = 46201 = 47 \cdot 983$.

§. 75. Quoniam autem hic numeros compositos non curamus, superfluum foret examen pro omnibus valoribus ipsius

ipsum a hic ordine apponere. Sufficiet enim omnes numeri primi in forma $1848aa + 197$ contenti in sequenti tabula exhibuisse

Tabula numerorum primorum in forma $1848aa + 197$ contentorum.

Numerus primus	ex valore a
55441	-3
85009	5
105337	6
129361	7
157081	8
351121	13
401017	14
454609	15
511897	16
572881	17
705937	19
933241	22
1016401	23
1103257	24
1288057	26
1487641	28
1722009	30
2095609	40
4658809	50
9094029	70
11866009	80
18518809	100

§. 76. Omnes ergo isti numeri primi deducti sunt ex formula $1848aa + 197$; unde patet, hinc patet factum esse fontem inexhaustum quamplurimos numeros primos ad plures

$d^3 \cdot mt - d^3 \cdot ms + d \cdot mr + mq - fmp = 0$;
 cuius denique differentiale productit infam accurationem...

$R = r - 3ds + 6d^2t$

plures nulliones exurgentes modico labore inveniendi; quoadquidem non solum in eadem formula: $184^4 aa + 197^2$, loco 197 quoque aliis numeris uti licet, sed etiam loco numeri idonei 1848 etiam majores eam praecedentes adhiberi possunt. Ac si forte adhuc major numerus idoneus investigari possit, pari labore insuper ad multo majores numeros primos perstringere possemus. At vero examini insulso inveni hujusmodi numeros usque ad terminum 7000 certe non dari; quod autem ultra hunc terminum adhuc dentur numeri idonei, vix probabile videtur.

THEOREMA

Si quispiam numerus idoneus fuerit impariter par, scilicet $N = 4n + 2$, tum etiam ejus quadruplum in classe numerorum idoneorum reperietur.

Demonstratio.

§. 77. Cum N sit numerus idoneus, intra intervallum N et $4N$ formula $Nxx + yy$ non nisi numeros primos prebebit. Dico autem hoc casu usque ad $4N$ nullos numeros compositos dari posse; si enim talis daretur, is tam in forma $N + aa$ quam in forma $4N + bb$ contingeretur. Hinc ergo foret $4N = aa - bb$; quia vero $N = 4n + 2$, ista quadratorum differentia $aa - bb$ foret $= 4n + 6$, ideoque numerus impariter par. id quod fieri nequit. Hinc igitur certum est, in intervallo ab N usque ad $4N$, nullos existere posse numeros compositos ex formula $Nxx + yy$ oriundos. Ac si hinc orantur majores numeri compositi in intervallo ab N usque ad $16N$ contenti, si nullo modo in forma $Nxx + yy$ contingerentur, idque ob rationem praecedentem. Si enim talis numerus compositus foret tam $N + bb$ quam $9N + cc$, foret $bb - cc = 8N$, hoc est numerus impariter par; ex quo concluditur, etiam intra intervallum $4N$ et $16N$ nullos nume-

numeros compositos formae $4Nxx + yy$ cadere posse; unde sequitur numerum $4N$ etiam esse idoneum.

§. 78. Hoc etiam colligere licet. ex ipsa tabula numerorum idoneorum supra § 34. exhibita, in qua reperuntur sequentes numeri impariter pares: 2, 6, 10, 18, 22, 30, 42, 58, 70, 78, 10, 130, 190, 210, 330, 462, quorum ergo quadrupla etiam, vi superioris theorematis, sunt numeri idonei, scilicet: 8, 24, 40, 72, 85, 120, 168, 322, 280, 312, 478, 520, 700, 840, 1320, 1548, qui omnes in eadem tabula occurrunt.

Alia Demonstratio.

§. 79. Sit $2i$ numerus idoneus impariter par, ideoque i numerus impar, et quia natura numerorum idoneorum in hoc consistit, ut omnes numeri unico modo in formula $2ixx + yy$ contenti certe sint primi: necesse est, ut omnis numerus compositus, qui sit C , in eadem formula contentus, simul insuper alio modo in ea contineatur. Ponamus igitur esse $C = iaa + bb$ et $C = 2icc + dd$, hincque fiet $2i$ aut $-cc = dd - bb$, ubi observetur numeros b et d impares esse debere, quandoquidem primi esse debent ad $2i$, quam obrem quadratorum differentia $dd - bb$ per 8 erit divisibilis.

§. 80. Consideremus jam casum, quo a est numerus par $= 2f$, ita ut sit $C = i \cdot 4ff + hb$, atque postrema aequatio erit $2i(f^2 - cc) = dd - bb$. Hic manifestum est, ut prius hujus aequationis membrum per 8 divisibile fiat, numerum c necessario parum esse debere. Sit igitur $c = 2g$, atque hinc sequitur, si numerus compositus C fuerit $= 4ff + hb$, tum adhuc alio modo fore $C = 2gg + dd$; *Nova Acta Acad. Imp. Scient. Tom. XIV.*

G

quo-

quocirca si alius numerus quicumque N unico modo in forma $8ix + y$ continetur, is certe debet esse primus; unde manifesto concluditur, etiam numerum 51 in tabula numerorum idoneorum contineri debere.

§. 81. Super tabula autem numerorum idoneorum sequentes observationes fecisse operae erit pretium:

- 1^o. Videmus in hac tabula alios numeros primos non occurrere, praeter 2, 3, 5, 7, 13 et 17, atque rationes non delint numerum 37 tanquam ultimum plane primum in classe numerorum idoneorum spectandi, siquidem quo longius procedatur, numeri idonei eo plures factores involvant,
- 2^o. Praeterea cum etiam dupla numerorum primorum in hoc negotio pro primis haberi debeant, etiam tales numeri pauci occurrunt, qui sunt 2. 3; 2. 5; 2. 11; 2. 29; ita ut si pro ultimo talium numerorum habendus videatur, idque ob rationem modo ante allatam, quod scilicet numeri idonei continuo plures factores recipiant.
- 3^o. Quoniam in isto calculo etiam quadrata numerorum primorum pro primis sunt habita, talia quadrata hic quoque pauca occurrunt, quae sunt 4, 9, 16, 25, neque enim ob eandem rationem plures admitti posse videntur.
- 4^o. Consideremus etiam omnes eos numeros idoneos, qui tantum ex duobus factoribus constant, ubi quidem ipsam binarium rejicimus, ejus vero potestates, perinde ac quadrata numerorum primorum, tanquam simplices factores spectamus. Tales numeros tabula nostra offert sequentes: 4. 3, 3. 5, 3. 6, 3. 7, 4. 6, 4. 7, 5. 6, 5. 8, 6. 7, 6. 8, 3. 19, 7. 11, 5. 9, 6. 13, 5. 17, 3. 31, 6. 17, 16. 7, 10. 13,

10. 13, 7. 19, 3. 59, 10. 19, 8. 29, 11. 23. Reliqui vero omnes vel tres vel adeo plures factores involvunt. His rationibus conjectura nostra non parum confirmatur, quod, quo longius progrediamur, numeri idonei continuo plures factores involvere debeant.

5^o. Cum numeri idonei ab initio usque ad 11 omnes numeros complectantur, deinde vero continuo evadant rariores, maxime mirandum, mox tanta intervalla occurrere a talibus numeris pro suis vacua. Veluti in toto intervallo a 520 usque ad 760 nullus plane reperitur; deinde vero ab 840 usque ad 1320, h. e. in intervallo fere quingentorum numerorum, nullus est inventus; ac fere per simile intervallum a 1365 usque ad 1848 nullus quidem apprehenditur.

6^o. Quod autem hic maxime est mirandum, post istum numerum, in tabula nostra profertur, nulli alii a me sunt inventi, quamquam istum calculum usque ad 4 millia sum profectus, ita ut totum hoc spatium profusum vacuum.

7^o. Hinc autem porro concludi oportet, ulterius usque ad 16000 progrediendo nullum saltem numerum idoneum pariter parem occurrere posse; si enim talis daretur, ejus pars quarta in hanc classem, atque adeo ante 4000, cadere deberet. Quare cum maxime probabile sit, etiam per hoc intervallum neque numeros impares neque impariter pares reperiri: hinc manifesto sequitur, profertur numerum nostrae tabulae 1848 etiam revera esse ultimum, id quod utique tanquam insignis paradoxon spectari potest, propterea quod hi numeri secunda certam legem formantur, quae adeo in infinitum progredi debere videtur.