1805

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

Leonhard Euler

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

His igitur numeris exclusis reliqui omnes loco a scripti in formula $32aa + 1$ producunt numeros primos. Hos igitur valores ipsius a sequens exhibet tabula:

1, 2, 3, 5, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18,
20, 22, 24, 26, 27, 28, 29, 31, 35, 36, 37, 38,
44, 45, 46, 48, 49, 50, 51, 53, 57, 62, 67, 71,
72, 73, 74, 76, 79, 81, 82, 86, 87, 94, 95, 99, 100,
104, 106, 107, 112, 113, 115, 117, 118, 219, 121,
124, 126, 127, 136, 138, 142, 144, 149, 150, 151,
152, 153, 155, 157, 158, 159, 165, 167, 170, 172,
173, 175, 176, 177, 180, 181, 182, 188, 189, 192,
196, 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 milliones exsurgunt.

ME-

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

AUCTORE

L. EULERO.

Conventui exhibita die 16 Martii 1778.

§. 1.

Sit N numerus propositus, et non difficile erit eum reducere ad hujusmodi 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 ejus 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 reducti sint $\lambda \cdot \frac{p}{q}$. Ponatur igitur $a + x = \lambda mp$ et $y - b = np$, erit $y + b = mq$ et $a - x = nq$, et hinc reperietur $a = \frac{\lambda mp + nq}{2}$ et $b = \frac{mq - np}{2}$, ex quibus valoribus, erit $N = \frac{1}{4}(\lambda mm + nn)(\lambda pp + qq)$; unde patet, formulam $\lambda pp + qq$ vel ipsam, vel ejus 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 statuatur vel $N - xx = \lambda yy$, vel $N - \lambda yy = xx$; ac priori quidem casu numerus x ita accipi

 debet

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

Exemplum.

10003 §. 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 $8n + 0$; at tum foret xx formae $8n + 5$, vel $8n + 1$, quorum neutra hic locum habere potest. Sumi ergo debebit x par, eritque xx vel formae $8n + 0$, vel formae $8n + 4$; et quia tum 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 $10000 - 12a - 12aa = xx$, quae per 4 divisa abit in $2500 - 3a - 3aa = \frac{xx}{4}$. Unde patet numerum a denuo per 4 divisibilem esse debere, vel potius statim poni potuisset $y = 1 + 8a$, unde prodiisset aequatio $625 - 3a - 12aa = \frac{xx}{16} = \square$.

§. 5. Nunc jam duos distinguamus casus, prouti 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-

divisionem per 8 admittat. Hinc statim ponatur $a = 8$ fietque $625 - 24b - 12 \cdot 64bb = \square$. Quia igitur a nu mero absoluto 625 subtrahi debet forma $768bb \pm 24b$, pa tet valorem minimum $b = 1$ jam esse nimis magnum hincque nullum oriri posse quadratum. Ex valore quiden $b = 0$ prodiret quadratum, sed ad casum cognitum pertinens

§. 6. Consideremus igitur casum, quo a est numeru impar, cujus 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 que $a = 4d - 1$, qui praebet hanc aequationem: $616 + 84d - 192dd = \square$, quae per 4 divisa in hanc abit $154 + 21d - 48dd = \frac{xx}{64} = \square$. A numero igitur absolutc 154 subtrahi debent numeri minores in forma $48dd \pm 21d$ contenti, qui sunt 27, 69, 150, quorum ultimus subtractus relinquit quadratum 4, ex valore $d = +2$ desumto. Hinc igitur erit $a = 7$, $y = 57$ et $x = 16$.

§. 8. Nacti ergo sumus aliam insuper resolutionem numeri $N = 10003$, cognitae similem, quae est $10003 = 16^2 + 3 \cdot 57^2$. Quare cum jam habeamus $\lambda = 3$, $a = 100$, $b = 1$, $x = 16$ et $y = 57$, hinc ex §. 1. erit $\frac{3p}{q} = \frac{116}{58} = 3 \cdot \frac{56}{84} = 3 \cdot \frac{2}{3}$ ideoque $p = 2$ et $q = 3$, consequenter $3pp + qq = 21$, quod per 3 depressum dat 7, qui numerus revera est divisor numeri propositi 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 proprietas

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

§. 10. Quin etiam haec formula generaliori modo ita exhiberi potest: $\alpha xx + \beta yy$, de qua itidem 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 $N = \alpha aa + \beta bb$, tum vero etiam $N = \alpha AA + \beta BB$, hinc formetur fractio $\frac{p}{q} = \frac{a \pm A}{b \pm B}$, tum semper formula $\alpha pp + \beta qq$ praebebit factorem numeri N, postquam scilicet per minores divisores α, β, 2, si quos admittit, fuerit depressa.

§. 11. Contra vero, si quispiam numerus N unico tantum modo in formula $\alpha xx + \beta yy$ contineatur, inde non semper concludi potest, hunc numerum esse primum, siquidem innumerabiles exhiberi possunt hujusmodi formulae, in quibus etiam numeri compositi semel tantum continentur, cujus rei exemplum jam supra attulimus. Hanc ob circumstantiam maxime necessarium est, formulas hujus posterioris indolis a prioribus distinguere atque a praesenti negotio prorsus 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 $\alpha xx + \beta yy$, de qua quaeritur, utrum in ea numeri compositi unico tantum modo contineri queant nec ne, consideretur haec formula $\alpha\beta + zz$, ubi ipsi z om-

nes successive tribuantur valores ad productum $\alpha\beta$ primi, sive ii ipsius z valores excludantur, qui cum hoc producto communem habent divisorem; tum vero sufficit hos numeros ex formula $\alpha\beta + zz$ resultantes tantum usque ad terminum $4\alpha\beta$ continuare. Quod si enim omnes hi numeri fuerint primi, formula $\alpha xx + \beta yy$ tuto in nostro negotio usurpari poterit; sin autem unicus inter eos fuerit numerus compositus, tum haec formula penitus erit rejicienda. In hoc autem judicio 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: $7xx + 2yy$, unde consideretur haec expressio: $14 + zz$, ubi ipsi z successive tribuantur valores ad 14 primi 1, 3, 5, unde resultant numeri 15, 23, 39, quorum primus cum jam sit compositus, pariter ac tertius, formulam propositam tanquam ineptam excludi oportet perinde atque hanc ad idem judicium deducentem: $14xx + yy$.

§. 14. Proposita formula $30xx + yy$, in forma $30 + zz$ ipsi z tribuantur valores impares ad 30 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 hinc oriundae: $15xx + 2yy$, $6xx + 5yy$, $10xx + 3yy$.

§. 15. Proposita sit formula $120xx + yy$; ubi in forma $120 + zz$ ipsi z tribui debent hi valores impares ad 120 primi: 1, 7, 11, 13, 17; numerus enim 19 praeberet numerum

merum, 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 desumtas, scilicet: $40xx + 3yy$; $24xx + 5yy$; $15xx + 8yy$, tanquam idoneas spectari debere et in examine tuto admitti posse.

§. 16. Sit proposita formula $7xx + 5yy$ et in hac expressione $35 + zz$ valores ipsi z tribuendi erunt: 1, 2, 3, 4, 6, 8, 9, qui praebent hos numeros: 36, 39, 44, 51, 71, 99, 116, ubi cum adeo sex sint compositi, hanc formam 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, 169, 226, 274, 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 numeri loco z successive scribendi, scilicet 1, 2, 4, 5, 7, 8, 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, cujus ope casus idoneos formulae $\alpha xx + \beta yy$ ab ineptis discernere valemus; qua igitur regula stabilita, illos casus optimo cum successu adhibere poterimus ad numeros quosvis in talibus formulis contentos, utrum sint

sint primi nec ne, perscrutandos. Proposito scilicet numero quocunque N facile erit illum pluribus modis ad talem formam $\alpha xx + \beta yy$ reducere, quo facto talis eligatur casus, qui per regulam supra datam non excludatur, ac dispiciatur, utrum ille numerus N unico tantum modo, an vero pluribus, in hac forma contineatur: 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 mani- N=100003
festo in forma $10xx + 3yy$ continetur, existente $x = 100$ et $y = 1$. Videamus ergo, an iste numerus adhuc alio modo in eadem forma contineatur. Hunc in finem ponamus $100003 - 3yy = 10xx$, atque ut divisio per 10 succedat, ponatur $y = 1 + 10z$, hincque orietur $10000 - 6z - 30zz = xx$, sive facta adhuc divisione per 4 erit $2500 - \frac{3}{2}z - \frac{15}{2}zz = \frac{xx}{4}$. Hinc igitur, prouti z fuerit vel par vel impar, formemus duos casus principales. Pro primo scilicet sit $z = 2a$, orietur aequatio $A = 2500 - 3a - 30aa = \frac{xx}{4}$. Pro altero casu sit $z = 2b - 1$, orietur ista: $B = 2494 + 27b - 30bb = \frac{xx}{4}$.

Evolutio formulae

$$A = 2500 - 3a - 30aa = \tfrac{1}{4}xx.$$

§. 21. Hic statim patet, sumto $a = 0$ prodire quadratum, praebens casum cognitum $x = 100$ et $y = 1$. Jam iterum duos casus distinxisse conveniet, quibus a est numerus vel par vel impar: ac priori quidem evidens est pro a sumi debere numerum pariter parem. Sit ergo primo mo $a = 4c$, et facta divisione per 4 oritur haec aequatio: $C = 625 - 3c - 120cc = \frac{1}{16}xx$. Hic igitur, quia c tam positive quam negative sumi poterit, numeri a 625 successive subtrahendi ordine erunt sequentes in forma $120cc + 3c$ 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 inferius valere posse. Fiat igitur $a = 4d - 1$, et aequatio per 4 divisa evadet $D = 2473 + 228d - 480dd$. Hinc igitur a numero absoluto 2473 successive subtrahi debent numeri sequentes in forma $480dd \mp 228d$ contenti, scil. 252, 708, 1464, 2376, unde iterum nullum quadratum resultat.

Evolutio Formulae.

$$B = 2494 + 27b - 30bb = \frac{xx}{4}.$$

§. 23. Hic statim patet, si pro b capiatur numerus par, eum impariter parem esse debere. Sit igitur $b = 4e + 2$, et facta divisione per 4 aequatio hinc resultans erit $B = 627 - 93e - 120ee = \frac{xx}{16}$. A numero ergo absoluto 627 subtrahi debent sequentes in forma $120ee + 93e$ contenti, qui sunt 27, 213, 294; ubi autem nullum quadratum occurrit.

§. 24. Denique pro b numeros impares tentemus. Facile autem patet, poni debere $b = 4f - 1$, ita tamen, ut numerus f sit impar, qui ergo ponatur $= 2g + 1$, eritque $b = 8g + 3$, unde oritur haec aequatio: $2305 - 1224g - 1920gg = \frac{xx}{4}$. Hic ergo unicus numerus 696 ab absoluto 2305 subtrahendus occurrit, unde autem numerus non-quadratus relinquitur.

Quo-

Quoniam igitur ex toto hoc calculo nullus numerus quadratus prodiit, jam certo pronunciare possumus numerum propositum 100003 esse primum.

Brevior Methodus
in hunc numerum inquirendi.

§. 25. Quoniam ante habuimus $100003 = 10 . 100^2 + 3 . 1^2$, etiam statuere poterimus $100003 = 40 . 50^2 + 3 . 1^2$, ita ut sit $\alpha = 40$ et $\beta = 3$, qui casus, uti supra vidimus, admittitur. Hanc ob rem statuamus $100003 - 3yy = 40xx$, fiatque $y = 1 + 20z$, et facta divisione per 40 statim pervenimus ad hanc aequationem: $2500 - 3z - 30zz = xx$; ubi duo casus considerandi occurrunt, prouti z fuerit numerus par vel numerus impar, quorum utrumque seorsim evolvamus.

§. 26. Pro priore casu evidens est pro z sumi debere numerum pariter parem. Sit ergo $z = 4a$, et facta divisione per 4 oritur haec aequatio: $625 - 3a - 120aa = \frac{xx}{4}$. Hic ergo a numero absoluto 625 sequentes ex forma $120aa + 3a$ desumti sunt subtrahendi: 117, 123, 474, 486. Hinc autem nullum occurrit quadratum, praeter casum $a = 0$, qui per se jam est notus.

§. 27. Superest ut pro z numerum imparem scribamus, qui sit $z = 2b - 1$, fietque 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: $2473 + 456c - 1920 . cc = xx = \square$. Sumto igitur $c = \pm 1$ numeri a 2473 subtrahendi erunt 1464 et 2376, quorum neuter quadratum relinquit. Hinc eadem, quam supra, conclusio: numerum 100003 certo esse primum. Ex

C 2 poste-

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

Exemplum 2.

N = 1000003 §. 28. Propositus sit numerus $N = 1000003$, qui manifesto 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 repertus 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 statuamus $1000003 - 3xx = 19yy$ atque ipsi x talis valor tribui debet, ut formula haec divisionem per numerum 19 admittat. Quare cum in casu cognito sit $x = 577 = 30 \cdot 19 + 7$, ponamus hic $x = 7 + 19z$, et facta divisione per 19 orietur haec aequatio: $52624 - 42z - 57zz = yy$. Ubi statim duo casus considerandi occurrunt prouti z fuerit numerus par vel impar. Pro priori casu statuatur $z = 2a$, et aequatio per 4 divisa ita se habebit: $13156 - 21a - 57aa = \frac{yy}{4}$, quam vocemus $= A$. Pro altero casu ponatur $z = 4b - 1$, quoniam facile est videre, valorem $z = 4b + 1$ penitus excludi. Hinc ergo orietur haec altera aequatio principalis:

$$B = 52609 + 288b - 912bb = yy.$$

Has igitur duas aequationes A et B, principales, seorsim ulterius evolvamus.

Evolutio Formulae

$$A = 13156 - 21a - 57aa = \frac{yy}{4}.$$

§. 29. Hic subdivisio in duos alios casus institui debet, quorum quisque iterum seorsim evolvatur. Sit primo a numerus par, et quidem $a = 4c$, qui valor, in aequatione A substitutus, producit sequentem aequationem, postquam scilicet divisio per 4 fuerit facta: $C = 3289 - 21c - 228cc = \frac{yy}{16}$. Hic ergo a numero absoluto 3289 successive subtrahi debent numeri in forma $228cc \mp 21c$ contenti, qui sunt:

si c numerus negativus: 267, 870, 1989

si c numerus positivus: 249, 954, 2115

unde autem nullum quadratum resultat.

§. 30. Sumamus ergo pro a numerum imparem, qui manifesto debet esse formae $4d - 1$. Facta igitur substitutione $a = 4d - 1$, simulque divisione per 4, orietur haec aequatio: $D = 3280 + 93d - 228dd$. Hinc numeri formae $228dd \pm 93d$ a numero absoluto 3280 successive subtrahendi erunt

si d numerus negativus: 135, 726, 1773, 3276

si d numerus positivus: 321, 1098, 2331

quorum quartus prioris seriei dat quadratum 4 ex casu $d = -4$, unde fit $y = 8$, qui casus jam est cognitus, praeter quem hic nullum amplius quadratum occurrit.

Evolutio Formulae

$$B = 52609 + 288b - 912bb = yy.$$

§. 31. Hic ergo a numero absoluto 52609 successive subtrahantur numeri in formula $912bb \mp 288b$ contenti, quos hic in gemina columna, una cum eorum differentiis, 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 crescunt ...

ubi differentiae, quas a quadrato aa continuo subtrahi oporteret ...

§. 32. Jam vero loco succesivae subtractionis numerorum in forma $912bb \pm 2886$ contentorum differentiae eorum augmento constanti 1824 crescentes continuo subtrahi poterunt, quos in subsidium calculi hic subjungamus

624 - - - - - - - -	1200
2448 - - - - - - - -	3024
4272 - - - - - - - -	4848
6096 - - - - - - - -	6672
7920 - - - - - - - -	8496
9744 - - - - - - - -	10320
11568 - - - - - - - -	12144.

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

52609 - - - - - - - - - -	52609
624	1200
51985 - - - - - - - - - -	51409
2448	3024
49537 - - - - - - - - - -	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 praecedentibus, casu scilicet cognito excepto. Hinc igitur jure concludimus, numerum propositum, 1000003 unico modo in forma $3xx + 19yy$ contineri, ideoque certe esse primum.

§. 34. Ex hoc exemplo clare apparet, quantum intersit in formula $\alpha xx + \beta yy$ pro α et β majores numeros investigare, dummodo eorum productum $\alpha\beta$ in classe numerorum idoneorum contineatur, pro quibus inveniendis regula supra fuit exposita. Quamobrem, ut quovis casu statim appareat, utrum tale productum $\alpha\beta$ sit numerus idoneus, nec ne, tabulam istorum numerorum, quousque eam continuare licuit, hic subjungamus.

Tabula numerorum idoneorum $\alpha\beta$, hac proprietate praeditorum, ut omnes numeri unico modo in formula $\alpha xx + \beta yy$ 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.

s	S	Diff.

Exemplum 2.

§. 35. Quoties igitur numerum quempiam propofitum ad talem formam $\alpha xx + \beta yy$ reducere licuerit, ut productum $\alpha\beta$ inter numeros iftius tabulae contineatur, tum haec formula ufurpari poterit ad examen, jam faepius allatum, inftituendum. Conveniet autem accuratius explicare regulam, cujus ope operationes neceffariae expedite inftitui queant, id quod in fequente Problemate oftendamus.

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 refolvere licebit, quarum utraque habeat factorem quadratum, quae fint αaa et βbb, ex quibus igitur talem eligi conveniet, ut numerorum α et β productum in tabula modo expofita contineatur, ubi quidem plurimum intererit majores hujusmodi numeros indagare.

§. 37. Talibus igitur numeris inventis ponamus efse $N = \alpha aa + \beta bb$, et nunc totum negotium huc redit, ut inveftigetur, utrum ifte numerus insuper alio modo in eadem forma $\alpha xx + \beta yy$ contineatur, nec ne. Si enim talis cafus occurrat, numerus propofitus non erit primus, atque tum adeo ejus factores, per praecepta fupra data afsignare licebit. Sin autem nullus talis cafus occurrat certo pronunciare poterimus, iftum numerum N efse primum.

§. 38.

§. 38. Ifta autem inveftigatio fequenti modo generaliter inftituatur: Ponamus efse $N = \alpha xx + \beta yy$, ita ut fit $\alpha aa + \beta bb = \alpha xx + \beta yy$, unde formemus hanc aequationem: $\alpha aa - \beta(yy - bb) = \alpha xx$, ubi praeftabit pro α majorem numerum afsumere, pro β vero minorem. Hic igitur ftatim patet, pro y ejusmodi numerum accipi debere, ut formula $yy - bb$ diviforem α involvat. Evidens enim eft non folum numeros α et β primos inter fe efse debere, fed etiam tam x ad β quam y ad α primum efse ftatuendum.

§. 39. Quoniam igitur $yy - bb$ per α divifibile efse debet, ante omnia erit difpiciendum, utrum α fit numerus primus nec ne. Priori enim cafu vel $y + b$ vel $y - b$ diviforem habere debet α, unde unicus tantum cafus exfurgit; sin autem α involvat factores, tum utique fieri poteft, ut alter contineatur in forma $y + b$, alter vero in forma $y - b$; unde praeter illum cafum adhuc unus vel plures novi cafus examinari debebunt. Unicus fcilicet casus occurret, fi α duos tantum habeat factores; fin autem plures factores involvat tum etiam pluribus modis in duos factores refolvi poterit, quos fingulos feorfim perfcrutari oportet.

§. 40. Ponamus igitur in genere efse $\alpha = \mu\nu$, et quovis cafu facile patebit, quot modis numerus α in binos hujusmodi factores refolvere licet, quotcunque etiam involvat divifores; neque etiam numeri primi hinc excluduntur, quippe quibus cafibus vel pro μ vel pro ν unitas erit fcribenda. Hinc ergo ponamus $y + b = \mu p$ et $y - b = \nu q$, ita ut fit $yy - bb = \mu\nu pq = \alpha pq$, et facta divifione per α aequatio deinceps refolvenda erit $aa - \beta pq = xx$.

§. 41.

6561	. . . .	6561
2040		−1000
4521	. . . .	7561

Hic jam occurrit numerus quadratus * 361 = 19² ipfi yy aequandus. Fit igitur $y = 19$, $s = -5$, hincque $x = 48$,

§. 41. Numeri autem p et q hoc modo commodissime reperiuntur. Eliminata enim littera y habebimus $2b = \nu p - q$. Jam quaeratur fractio $\frac{m}{n}$ proxime aequalis fractioni $\frac{\mu}{\nu}$, ita ut $m\nu - n\mu = 1$; tum capiatur $p = \nu s - 2nb$ et $q = \mu s - 2mb$, ubi jam pro s numeros quoscunque integros accipere licet, five positivos five negativos, et aequatio nostra resolvenda induet hanc formam:

$$aa - \beta(\nu s - 2nb)(\mu s - 2mb) = xx,$$

ubi jam pro s ejusmodi valores investigari debent, ut ista forma $aa - \beta(\nu s - 2nb)(\mu s - 2mb)$ quadratum evadat. Totum negotium igitur eo redit, ut dispiciatur an, tribuendo litterae s fuccefsive omnes valores tam positivos quam negativos, a zyphra ad terminum usque qui numeros praeberet negativos, an dico usquam quadratum refultare possit.

§. 42. Evolvamus igitur singulos numeros, quos a quadrato aa fubtrahi oportet, quos littera S defignemus, ita ut fit $aa - S = xx$. Habebimus ergo

s	S	
0	$4\beta mnbb$ - - -	I
± 1	$\beta(\nu \pm 2nb)(\mu \pm 2mb)$ - - -	II
± 2	$\beta(2\nu \pm 2nb)(2\mu \pm 2mb)$ - - -	III
± 3	$\beta(3\nu \pm 2nb)(3\mu \pm 2mb)$ - - -	IV
± 4	$\beta(4\nu \pm 2nb)(4\mu \pm 2mb)$ - - -	V
± 5	$\beta(5\nu \pm 2nb)(5\mu \pm 2mb)$ - - -	VI

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

$$\text{II} - \text{I} = \beta(\mu\nu \pm 2b(m\nu + n\mu))$$
$$\text{III} - \text{II} = \beta(3\mu\nu \pm 2b(m\nu + n\mu))$$
$$\text{IV} - \text{III} = \beta(5\mu\nu \pm 2b(m\nu + n\mu))$$
$$\text{V} - \text{IV} = \beta(7\mu\nu \pm 2b(m\nu + n\mu))$$

quae-

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

§. 43. His differentiis inventis nihil aliud fupereft, nisi ut eae ordine continuo a quadrato aa, primo termino minuto fubtrahantur. Ab aa fcilicet primo fubtrahatur prima differentia; tum vero a refiduo fecunda, a refiduo hinc nato tertia, porro quarta etc. quoad ad numeros negativos perveniatur; hisque operationibus ita continuatis dispiciatur, utrum usquam numerus quadratus remanferit; quod fi non contigerit, numerus propofitus certe pro primo erit habendus; sin autem usquam quadratum prodierit, ejus radix dabit valorem ipfius x, et notato valore ipfi s conveniente etiam reperiri poterit alter numerus y, fiquidem erit $y = b + \mu\nu s - 2\nu mb$. Quia vero fupra sumfimus $m\nu - n\mu = 1$, erit nunc $y = \mu\nu s - b(m\nu + n\mu)$.

§. 44. Quod fi numerus propofitus N fuerit vehementer magnus, numerum harum operationum non parum diminuere licebit, fi numeri S, quos a quadrato aa continuo fubtrahi oportet, in duas clafses diftinguantur, prouti pro s valores five pares five impares accipiantur. Priore enim cafu, cum fit vel $s = 4n$, vel $s = 4n + 2$, plerumque eveniet, ut alter cafus penitus excludatur, ob eam proprietatem, quod inde pro S numeri prodirent impariter pares. Eodem modo fi pro s fumatur numerus impar, erit vel $s = 4n + 1$, vel $s = 4n - 1$, quarum formarum altera penitus excluditur, quia omnia quadrata imparia funt formae $8n + 1$, ita ut hoc modo numerus operationum ad femifsem redigatur.

§. 45. Quoniam initio pofuimus $\alpha = \mu\nu$, hosque numeros μ et ν ut primos inter fe fpectavimus, id quod potiffi-

D 2 mum

1040 decrescentes: 1640, 600, — 440 — 1480, — 2520, quia inde nullum quadratum refultat, concludimus numerum 64013 effe primum.

999601	756841
840	29400
998761	727441

mum de factoribus imparibus est tenendum, notetur si a sit numerus par et potestatem quamcunque ipsius binarii involvat, tum utrumque factorem $y+b=\mu p$ et $y-b=\nu q$ parem esse debere. Unde si ipsi μ valor par tribuatur, nihil impedit quo minus et ν par statuatur, id quod facile in exemplis oblatis observare licet. Ita cum numerus $520=8.5.13$ in tabula superiore numerorum idoneorum contineatur, secundum praecepta hic tradita in genere numeros $N=40aa+13bb$ evolvamus.

Evolutio generalis

numerorum contentorum in forma

$$N=40aa+13bb.$$

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

$$40aa-13(yy-bb)=40xx$$

ubi statim duos casus distingui conveniet, quibus est vel $\mu=10$ et $\nu=4$, vel $\mu=20$ et $\nu=2$, quia scilicet ambo 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 $\frac{2}{1}$, unde statuamus $p=2s+b$ et $q=5s+2b$, quibus valoribus substitutis aequatio resolvenda erit

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

Posito igitur brevitatis gratia numerum a quadrato aa subtrahendum, scil. $13(2s+b)(5s+2b)=S$, si loco s successive scribamus numeros $0, \pm 1, \pm 2, \pm 3$, etc. valores ipsius S cum suis differentiis, quorum usum jam saepius explicavimus, ita se habebunt:

s	S	Diff.
0	$26bb$	
± 1	$13(2\pm b)(5\pm 2b)$	$130\pm 117bb$
± 2	$13(4\pm b)(10\pm 2b)$	$390\pm 117bb$
± 3	$13(6\pm b)(15\pm 2b)$	$650\pm 117bb$
± 4	$13(8\pm b)(20\pm 2b)$	$910\pm 117bb$
etc.	etc.	etc.

quae differentiae continuo crescunt augmento 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 $aa-13s(10s-b)=xx$. Posito igitur brev. gr. $13s(10s-b)=S$, valores ipsius S, prouti s fuerit vel 0, vel 1, vel 2, vel 3, erunt sequentes:

s	S	Diff.
0	0	
± 1	$13(10\pm b)$	$130\pm 13b$
± 2	$26(20\pm b)$	$390\pm 13b$
± 3	$39(30\pm b)$	$650\pm 13b$
± 4	$52(40\pm b)$	$910\pm 13b$
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 $40aa + 13bb$.

§. 49. Cum habeatur aequatio: $40aa - 13(yy - bb) = 40xx$, tollamus primo tantum factorem parem 8, et quia b denotat numerum imparem, evidens est, dummodo pro y etiam sumatur numerus impar, formulam $yy - bb$ fore divisibilem per 8. Ponatur igitur in genere $y = 2z \pm b$, et facta divisione per 8 habebimus hanc aequationem:
$5aa - \frac{13}{2}(zz \pm bz) = 5xx$; ubi evidens est, membrum medium semper esse integrum. Nunc igitur loco z talem numerum assumi oportet, ut vel z, vel $z \pm b$ factorem habeat 5: perinde autem est uter horum factorum per 5 divisibilis reddatur, propterea quod inter se sunt permutabiles, mutato scilicet signo ipsius b. Ponatur igitur $z = 5s$ et facta divisione per 5 aequatio, cui satisfieri oportet, erit: $aa - \frac{13}{2}(5ss \pm bs) = xx$.

§. 50. Hic igitur a quadrato aa subtrahi debent numeri in forma $\frac{13}{2}(5ss \pm bs)$ contenti, quae si vocetur $= S$, valores ipsius S erunt, uti in sequenti tabula cum suis differentiis exhibentur.

s	S	Diff.
0	0	$\frac{13}{2}(5 \pm b)$
± 1	$\frac{13}{2}(5 \pm b)$	$\frac{13}{2}(15 \pm b)$
± 2	$\frac{13}{2}(20 \pm 2b)$	$\frac{13}{2}(45 \pm b)$
± 3	$\frac{13}{2}(45 \pm 3b)$	$\frac{13}{2}(35 \pm b)$
± 4	$\frac{13}{2}(80 \pm 4b)$	
etc.	etc.	etc.

ubi

ubi differentiae, quas a quadrato aa continuo subtrahi oportet, augmento constanti $\frac{13}{2} \cdot 10 = 65$ crescunt.

§ 51. Quin etiam unica substitutione totus numerus 40 statim tolli potest, ponendo $y = 10s \pm b$; tum enim ob $yy - bb = 100ss \pm 20bs$, dividendo per 40 statim pervenitur ad hanc aequationem: $aa - \frac{13}{2}(5ss \pm bs) = xx$, 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 $a = 2^{\lambda} . fg$, ita ut formula $yy - bb$ per hunc valorem divisibilis reddi debeat, statim poni poterit:

$y = 2^{\lambda - 1} fz \pm b$; tum enim erit:

$yy - bb = 2^{2\lambda - 2} ffzz \pm 2^{\lambda} bfz$, quae forma $2^{2\lambda - 2} ffzz \pm 2^{\lambda} bfz$ per $2^{\lambda} f$ divisa abit in hanc: $2^{\lambda - 2} fzz \pm bz$; quod igitur cum fuerit praestitum, reliqui factores per praecepta generalia, alibi tradita, facile e medio tolli poterunt. En adhuc alia, eaque simplicissima evolutio formulae $N = 40aa + 13bb$.

§. 52. Cum posito $N = 40xx + 13yy$ aequatio prima fundamentalis hoc modo repraesentetur: $13bb - 40(xx - aa) = 13yy$, observasse juvabit, eam unica operatione resolvi posse. ponendo $x = 13s + a$. Facta enim substitutione et divisione per 13 pervenietur ad hanc aequationem simplicissimam: $bb - 40(13ss \pm 2as) = yy$. Hic igitur a quadrato bb successive subtrahi debent valores formulae: $40(13ss \pm 2as)$, qui ita (posita hac formula br. gr. $= S$) ordine cum suis differentiis disponantur:

J

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

ubi differentiae per augmentum conſtans $40 \cdot 26 = 1040$ progrediuntur.

Hanc jam poſteriorem reſolutionem maxime ſuccinctam aliquot exemplis illuſtraſse 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 $40(13 \pm 1)$; $40(39 \pm 1)$; etc. quae creſcunt augmento conſtanti $40 \cdot 26 = 1040$; unde ob ſigna ambigua totus hic calculus per duas columnas abſolvi poterit:

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

Quoniam igitur nullum reſiduorum ex hac ſubtractione natorum quadratum deprehenditur, tuto concludere poſumus 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 $40(13 \pm 20)$, ideoque 1320 et -280; ſequentes autem differentiae creſcunt 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 erit primus.

Exemplum 3.

§. 55. Maneat adhuc $b = 81$ ſumaturque $a = 19$, 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:

A quadrato igitur 10000 ſubtrahantur differentiae numero

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

6561 - - - - - - -	6561
2040	−1020
4521 - - - - - - -	7561
3080	40
1441 - - - - - - -	7521
	1080
	6441
	2120
	4321
	3160
	1161

Quia igitur hic nullum quadratum refultat, numerus 99733 etiam pro primo eft habendus.

Exemplum 4.

§. 56. Adjungamus exemplum numeri propofiti. Maneat iterum $b = 81$ fitque $a = 17$, erit $N = 90853$ et fubtractio differentiarum ita fe habebit:

6561 - - - - - - -	6561
1550 - - - - - - -	840
4651 - - - - - - -	7401
2920	200
1761 - - - - - - -	7201
	1240
	5961
	2280
	3681
	3320
	*361

Hic

Hic jam occurrit numerus quadratus $*361 = 19^2$ ipfi yy aequandus. Fit igitur $y = 19$, $s = -5$, hincque $x = 48$, unde factor numeri propofiti inveniri poteft quaerendo fractionem $\frac{p}{q} = \frac{x \pm a}{y \pm b} = \frac{48 \pm 17}{81 \pm 19} = \frac{1}{2}$; hinc factor eft $40\,pp + 13\,qq = 40 \cdot 1^2 + 13 \cdot 3^2$, qui ad minimos terminos reductus eft $10 \cdot 1^2 + 13 \cdot 1^2 = 23$. Alter factor ex eadem fractione derivari poteft, fi fumatur $\frac{p}{q} = \frac{65}{62}$; hinc enim fiet $40\,pp + 13\,qq = 40 \cdot 65^2 + 13 \cdot 62^2$, qui factor per $4 \cdot 13$ depreffus dat $10 \cdot 65 \cdot 5 + 31^2 = 4211$: at revera eft $96853 = 23 \cdot 4211$.

Exemplum 5.

§. 57. Sumatur $a = 40$ et $b = 1$ et numerus examinandus erit $N = 64013$. Hic autem modus procedendi a praecedentibus diverfus adhiberi debet; quia enim a quadrato bb fubtrahi deberent numeri in forma $40\,(13\,ss + 50\,s)$ contenti, quod autem fieri nequit, hic folum fignum inferius valebit, ita ut fucceffive ad quadratum $bb = 1$ addi debeant numeri in forma $S = 40\,(50\,s - 13\,ss)$ contenti, quos cum fuis differentiis hic adjungamus.

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

ubi differentiae decrefcunt quantitate conftanti 40 . 26; quamobrem, fi ad unitatem primo addamus numerum $40 \cdot 67 = 2680$, tum vero differentias fequentes decremento

 1040

est primus, ejusque factores sequenti modo assignari possunt. Formetur fractio: $\frac{p}{q} = \frac{x \pm 1}{y \pm b}$ et ob signa ambigua hac quatuor habebuntur fractiones: $\frac{41}{1148} = \frac{1}{28}$; $\frac{41}{810}$, $\frac{27}{1148}$, $\frac{27}{810} = \frac{1}{30}$. Hinc forma factoris $840\,pp + qq$ ex priore fractione fit $840 \cdot 1^2 + 28^2$, sive per 28 depressus, $30 + 28 = 15 + 14 = 29$, 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 $\frac{p}{q} = \frac{41}{810}$ fit factor $= 840 \cdot 41^2 + 810^2$, qui per 60 depressus est $= 14 \cdot 41^2 + 27 \cdot 405 = 34469$. Idem prodit ex fractione $\frac{p}{q} = \frac{27}{1148}$: at vero revera est $29 \cdot 34469 = 999601$.

§. 61. Ex hoc exemplo luculenter apparet, quanti momenti sint numeri idonei majores in perscrutandis numeris praegrandibus, utrum sint primi nec ne. Cum igitur numerus 1848 sit maximus idoneus, qui in nostra tabula occurrit, operae pretium erit, in subsidium examinis numerorum vehementer magnorum, sequens problema generalius hic adjungere.

Problema.

Numerum propositum quantumvis magnum $N = 1848\,aa + bb$ *examinare, utrum sit primus nec ne?*

Solutio.

§. 62. Subtrahantur ab isto numero N successive omnes numeri in hac forma: $1848\,xx$ contenti, et si nusquam quadratum remaneat, praeter casum cognitum $x = a$, iste numerus certe erit primus. Sin autem aliud praeterea 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 $1848\,aa - (yy - bb) = 1848\,xx$ et cum sit $1848 = 8 \cdot 3 \cdot 7 \cdot 11$, ponatur primo $y = 22z + b$ et facta divisione per $8 \cdot 11$ fiet $21\,aa - \frac{1}{2}z(11z + b) = 21\,xx$. Quod si ergo brevitatis gratia ponatur $z(11z + b) = 21\,pq$, aequatio nostra erit $aa - \frac{1}{2}pq = xx$, quae 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 *pro primo casu*, ob $z = q$, erit $11q + b = 21p$, hincque $q = 2p - \frac{p - b}{11} = 2p - s$, ita ut $p + b = 11s$, ideoque $p = 11s - b$, et $q = 21s - 2b = z$, ita ut aequatio nostra fiat

$$aa - \frac{1}{2}(11s - b)(21s - 2b) = xx.$$

Pro secundo casu. ob $z = 21q$, erit $231q + b = p$, sicque sumto $q = s$ erit $p = 231s + b$ et $z = 21s$, unde aequatio pro hoc casu erit $aa - \frac{1}{2}s(231s + b) = xx$.
Pro tertio casu, ob $z = 3q$, erit $33q + b = 7p$ ideoque $p = 5q - \frac{2q + b}{7} = 5q - r$, ita ut $2q - b = 7r$ et $2q = 7r + b$, sive $q = 3r + \frac{r + b}{2} = 3r + s$, unde fit $r = 2s - b$, hincque $q = 7s - 3b$ et $p = 33s - 14b$, et $z = 21s - 9b$, unde nostra aequatio erit $aa - \frac{1}{2}(7s - 3b)(33s - 14b) = xx$.

Pro

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

Exemplum.

§. 65. Sumatur $a = 100$ et $b = 197$, ut numerus examinandus sit $N = 1848aa + bb = 18518809$, ubi facile patet numerum y majorem fore quam 197 ideoque z 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.

§. 67. *Pro casu primo* nostra aequatio erit $10000 - \frac{1}{2}(11s-b)(21s-2b) = xx$; et quia hinc est $z = 21s - 394$, patet numerum s majorem esse debere quam 18. Statuamus igitur $s = 18 + t$, ut fiat $z = 21t - 16$, atque aequatio nostra hanc induet formam: $10000 - \frac{1}{2}(11t+1)(21t-16) = xx$. 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		0	− 8	
		38			193
+ 1	30		− 1	185	
		269			424
+ 2	299		− 2	609	
		500			655
+ 3	799		− 3	1264	
etc.	etc.	etc.	etc.	etc.	etc.

ubi differentiae crescunt augmento constanti 231. At quia primus numerus subtrahendus est − 8, continua differentiarum subtractio fieri debet a numero 10008, ut sequitur.

10008	- - - - - - - - -	10008
38		193
9970	- - - - - - - - -	9815
269		424
9701	- - - - - - - - -	9391
500		655
9201	- - - - - - - - -	8736
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		0	0	
		214			17
+ 1	214		− 1	17	
		445			248
+ 2	659		− 2	265	
		676			479
+ 3	1335		− 3	744	
etc	etc.	etc.	etc.	etc.	etc.

quoties & alius numerus quicunque N unico modo in forma

10.12. 7.10. 2.50. 10.10. 8.20. 11. 23. Reliqui

A quadrato igitur 10000 fubtrahantur 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	1403
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, pofito $s = 84 + t$, abibit in hanc: $10000 - \frac{1}{2}(7t - 3)(33t + 14) = xx$. Prouti igitur t valorem habet vel pofitivum vel negativum, numeri fubtrahendi

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

Jam a numero abfoluto 10021 fubtrahantur 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
7036	7131
1270	1271
5866	5860
1501	1502
4365	4358
1732	1733
2633	2625
1963	1964
670	661

ubi nullum plane quadratum occurrit.

§. 70.

OBSERVATIO SINGULARIS

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

t	s	Diff.	t	S	Diff.
0	− 20		0	− 20	
		137			94
+ 1	+ 117		− 1	74	
		368			325
+ 2	485		− 2	399	
		599			556
+ 3	1084		− 3	955	
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
830		787
8086	- - - - - - - -	8258
1061		1018
7025	- - - - - - - -	7240
1292		1249
5733	- - - - - - - -	5991
1523		1480
4210	- - - - - - - -	4511

1754

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 forma $1848aa + bb$ etiam aptissima 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 fit satisfactum.

§. 72. Quoniam in hoc exemplo numeri successive a quadrato aa subtrahendi iidem manent, quamdiu sumitur $b = 197$; operae pretium erit pro littera a alios quoque valores, potissimum minores, statuere, 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 statutum fuisse ut sequitur:

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

Pro

§. 5. Proposita autem tali forma generali:

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

1040 decrescentes: 1640, 600, — 440 — 1480, — 2520, quia inde nullum quadratum refultat, concludimus numerum 64013 effe primum.

§. 58. His circa evolutionem numerorum in forma $40aa + 13bb$ contentorum expeditis, praeftabit ufum majorum numerorum idoneorum exemplo illuftraffe. Confideretur numerus $N = 999601 = 840 \cdot 34^2 + 169^2$, et examinetur, utrum hic numerus propofitus plus uno modo in forma idonea $840xx - yy$ contineatur, id quod fine pluris ambagibus fequenti modo fatis commode fieri licet.

§. 59. Cum debeat effe $999601 - 840xx = yy$, ipfi x fuccefsive tribuantur numeri naturales et numeri S a propofito fubtrahendi cum fuis differentiis erunt

x	S	Diff.
0	0	
		1 . 840
1	1 . 840	
		3 . 840
2	4 . 840	
		5 . 840
3	9 . 840	
		7 . 840
4	16 . 840	
etc.	etc.	etc.

Loco S jam continuo fubtrahantur differentiae augmento 1680 crescentes, quae fubtractiones continuae fequenti modo inftituantur.

999601

999601	756841
840	29400
998761	727441
2520	31080
996241	696361
4200	32760
992041	663601
5880	34440
986161	629161
7560	36120
978601	593041
9240	37800
969361	555241
10920	39480
958441	515761
12600	41160
945841	474601
14280	42840
931561	431761
15960	44520
915601	387241
17640	46200
897961	341041
19320	47880
878641	293161
21000	49560
857641	243601
22680	51240
834961	192361
24360	52920
810601	139441
26040	54600
784561	84841
27720	56280
756841	28561

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

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

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

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

§. 73. Sit $a = 1$, existente $b = 197$, et numerus propositus erit $N = 40657$. Hic igitur statim ex primo casu occurrit quadratum $aa + 8 = xx$, unde fit $xx = 9$ 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 $\frac{p}{q} = \frac{a \pm x}{b \pm y} = \frac{1 \pm 3}{197 \pm 155}$, cujus 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 $aa + 21 = 25 = xx$, unde fit $x = 5$, existente $t = 0$, adeoque $z = -9$, consequenter $y = -9 \cdot 22 + 197 = 1$. Ad divisorem igitur numeri propositi explorandum fiat $\frac{p}{q} = \frac{a + x}{b \pm y} = \frac{1}{28}$, 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

ipsius 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
1702009	30
2995609	40
4658809	50
9094009	70
11866009	80
18518809	100

§. 76. Omnes ergo isti numeri primi deducti sunt ex formula $1848aa + 197^2$; unde patet, hinc patefactum esse fontem inexhaustum quamplurimos numeros primos ad plures

$$d^3 . mt - d^2 ms + d . mr + mq - \int mp = 0;$$

cujus denique differentiale producit ipsam aequationem

$$R = r - 3ds + 6ddt$$

plures nilliones exsurgentes modico labore inveniendi; quandoquidem non solum in eadem formula: $1848aa + 197^2$, loco 197 quoque aliis numeris uti licet, sed etiam loco numeri idonei 1848 etiam majores eum praecedentes adhiberi possent. Ac si forte adhuc major numerus idoneus investigari posset, pari labore insuper ad multo majores numeros primos pertingere possemus. At vero examini instituto 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 praebebit. Dico autem hoc casu usque ad 9N nullos numeros compositos oriri posse; si enim talis daretur, is tam in forma $N + aa$ quam in forma $4N + bb$ contineretur. Hinc ergo foret $3N = aa - bb$; quia vero $N = 4n + 2$, ista quadratorum differentia $aa - bb$ foret $= 12n + 6$, ideoque numerus impariter par, id quod fieri nequit. Hinc igitur certum est, in intervallo ab N usque ad 9N, 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, ii nullo modo in forma $Nxx + yy$ continerentur, idque ob rationem praecedentem. Si enim talis numerus compositus foret tam $4N + bb$ quam $9N + cc$, foret $bb - cc = 5N$, 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 reperiuntur sequentes numeri impariter pares: 2, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462, quorum ergo quadrupla etiam, vi superioris theorematis, sunt numeri idonei, scilicet: 8, 24, 40, 72, 88, 120, 168, 232, 280, 312, 408, 520, 760, 840, 1320, 1848, 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 $C = 2iaa + bb$ et $C = 2icc + dd$, hincque fiet $2i(aa - cc) = dd - bb$; ubi observetur numeros b et d impares esse debere, quandoquidem primi esse debent ad $2i$, quamobrem quadratorum differentia $dd - bb$ per 8 erit divisibilis.

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

quo-

quocirca si alius numerus quicunque N unico modo in forma $8ixx + yy$ contineatur, is certe debebit esse primus; unde manifesto concluditur, etiam numerum $8i$ in tabula numerorum idoneorum contineri debere.

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

1°. Videmus in hac tabula alios numeros primos non occurrere, praeter 2, 3, 5, 7, 13 et 37, atque rationes non desunt numerum 37 tanquam ultimum plane primum in classe numerorum idoneorum spectandi, siquidem quo longius procedatur, numeri idonei eo plures factores involvant,

2°. Praeterea cum etiam dupla numerorum primorum in hoc negotio pro primis haberi debeant, etiam tales numeri pauci occurrunt, qui sunt 2.2; 2.3; 2.5; 2.11; 2.29; ita ut 58 pro ultimo talium numerorum habendus videatur, idque ob rationem modo ante allatam, quod scilicet numeri idonei continuo plures factores recipiant.

3°. 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°. Consideremus etiam omnes eos numeros idoneos, qui tantum ex duobus factoribus constant, ubi quidem ipsum 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, 7.10, 8.9, 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°. 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 prorsus 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 ne unus quidem deprehenditur.

6°. Quod autem hic maxime est mirandum, post istum numerum, in tabula nostra postremum, nulli alii a me sunt inventi, quamquam istum calculum usque ad 4 millia sum prosecutus, ita ut totum hoc spatium prorsus sit vacuum.

7°. 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, postremum numerum nostrae tabulae 1848 etiam revera esse ultimum, id quod utique tanquam insigne paradoxon spectari potest, propterea quod hi numeri secundum certam legem formantur, quae adeo in infinitum progredi debere videtur.