1805

Facillima methodus plurimos numeros primos praemagnos inveniendi

Leonhard Euler

FACILLIMA METHODUS
PLURIMOS NUMEROS PRIMOS PRAEMAGNOS INVENIENDI.

AUCTORE
L. EULERO.

Conventui exhibita die 16. Mart. 1778.

1. Sufficiet hanc methodum unico exemplo, numerorum in hac formula $232aa+1$ contentorum, explicasse, ubi omnes valores ipsius a investigabo, quibus haec formula numeros compositos producit; his enim exclusis, omnes reliqui numeri pro a assumti numeros primos suppeditabunt.

2. At si formula $232aa+1$ praebeat numerum compositum, tum semper talis aequatio locum habebit:
$232aa+1 = 232xx+yy$; propterea quod $232 = 8.29$ est numerus idoneus *). Sic igitur erit $232(aa-xx) = yy-1$. Jam ponatur $y = 1+58z$, ac facta divisione per 232 prodibit ista aequatio: $aa-xx = \frac{1}{2}z(29z+1)$, sive, quia unitatem tam positive quam negative accipere licet, erit

$$aa-xx = \tfrac{1}{2}z(29z\pm1).$$

3. Tribuantur nunc ipsi z ordine omnes valores 1, 2, 3. etc. et quia formula $\frac{1}{2}z(29z\pm1)$ certe duos factores, saepiusque plures, involvet, ea semel quoque, vel pluribus modis, per productum rs repraesentari poterit, cui cum aequalis esse debeat

*) Conf. Nov. Act. T. III. pag. 33.

debet, ut $N-xx$ dividi queat per numerum λ. Hoc mo-

divisionem per 8 admittat. Hinc statim ponatur $a = 8b$

formula $aa - xx = (a+x)(a-x)$, statuatur $a + x = r$ et $a - x = s$, unde fit $a = \frac{r+s}{2}$, hocque modo reperientur valores pro a excludendi. Hic igitur evidens est, ambos factores r et s simul vel pares vel impares esse debere.

4. His jam notatis sumamus $z = 1$, eritque duplici modo, pro ambiguitate signi, vel $rs = 14$, vel $sr = 15$, ubi prior valor, utpote impariter par, ad nostrum institutum est ineptus; posterior vero $rs = 15$ praebet duas exclusiones, vel enim erit $r = 15$ & $s = 1$, vel $r = 5$ et $s = 3$, unde valores pro a excludendi erunt 8 et 4.

5. Sit nunc $z = 2$, eritque $rs = 57$, vel $rs = 59$. Prior admittit duas resolutiones: $r = 57$, $r = 19$
$s = 1$, $s = 3$
posterior unicam: $r = 59$ et $s = 1$, unde oriuntur hae tres exclusiones: $a = 29$, $a = 11$, $a = 30$.

6. Sit nunc $z = 3$, eritque vel $rs = 3 \cdot 43$, vel $rs = 3 \cdot 44$, quorum valorum resolutiones ita referentur:

$r = 129$, $r = 43$, $r = 66$, $r = 22$
$s = 1$, $s = 3$, $s = 2$, $s = 6$

unde quatuor exclusiones prodeunt

$a = 65$, $a = 23$, $a = 34$, $a = 14$

7. Sit $z = 4$, erit vel $rs = 230$, vel $rs = 234$, qui numeri, utpote impariter pares, nullas dant exclusiones.

8. Sit nunc $z = 5$, erit $rs = 5 \cdot 72$, vel $rs = 5 \cdot 73$, unde ex priore sequentes prodeunt resolutiones:

$r = 180$, $r = 90$, $r = 60$, $r = 36$, $r = 30$, $r = 20$
$s = 2$, $s = 4$, $s = 6$, $s = 10$, $s = 12$, $s = 18$

Hinc ergo valores ipsius a excludendi erunt 91, 47, 33, 23, 21, 19

Alter

Alter valor dat $r = 73$, $s = 5$, vel $r = 365$, $s = 1$, unde exclusiones hinc natae sunt 39 et 183.

8. Sit $z = 6$, erit vel $rs = 3 \cdot 173$, vel $rs = 3 \cdot 175$, unde sequentes resolutiones:

$r = 173$, 519 | $r = 525$, 175, 105, 75, 35, 25
$s = 3$, 1 | $s = 1$, 3, 5, 7, 15, 21.

Exclusiones ergo nascuntur istae:

88, 260, 263, 89, 55, 41, 25, 23

9. Sit nunc $x = 7$, erit vel $rs = 7 \cdot 101$, vel $rs = 7 \cdot 102$. Hic solus prior casus dat has resolutiones:

$r = 707$, $r = 101$
$s = 1$, $s = 7$, hincque exclusiones erunt 354 et 54.

Ut autem nobis terminum praescribamus, in posterum omnes exclusiones majores quam 300 praetermittamus.

10. Sit nunc $z = 8$, erit vel $rs = 4 \cdot 3 \cdot 7 \cdot 11$, vel $rs = 4 \cdot 233$. Resolutiones hinc nascuntur sequentes:

$r = 462$, 154, 66, 42, | $r = 466$
$s = 2$, 6, 14, 22, | $s = 2$

unde concludimus sequentes exclusiones:

$a = 232$, 80, 40, 32, 234.

11. Sit $z = 9$, erit vel $rs = 9 \cdot 130$, vel $rs = 9 \cdot 131$, hinc a 2do $r = 393$, 131
$s = 3$, 3, excluditur igitur $a = 198$, 70.

12. Sit $z = 10$, erit vel $rs = 5 \cdot 17 \cdot 17$, vel $rs = 3 \cdot 5 \cdot 97$, hinc $r = 495$, 291, 97 | $r = 289$, 85
$s = 3$, 5, 15 | $s = 5$, 17, unde excluditur $a = 147$, 244, 51, 148, 56.

13. Sit

prietas absolute necessaria est ad omnes numeros primos hac ratione explorandos Nisi enim formula $\lambda xx + yy$ hac proprietate gaudea, de numeris, qui unico modo in ea

z omnes 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

13. Sit $z = 11$, erit vel $rs = 3.11.53$, vel $rs = 3^2.5.11$, hinc

$$\begin{array}{l} r = 583, 159, 53; 440, 220, 176, 88, 80, 110, 44, \\ s = 3, 11, 33; 4, 8, 10, 20, 22, 10, 40, \\ a = 293, 85, 43, 222, 114, 93, 54, 51, 63, 42. \end{array} \text{ hinc}$$

14. Sit $z = 12$. erit vel $rs = 6.347$, vel $rs = 6.349$, quorum neuter dat exclusionem.

15. Sit $z = 13$, erit vel $rs = 13.4.57$, vel $rs = 27.13.7$, hinc

$$\begin{array}{l} r = 94, 351, 273, 189, 117, 91, 63, \\ s = 26, 7, 9, 13, 21, 27, 39, \end{array} \text{ excluduntur ergo}$$
$$60, 179, 141, 101, 69, 59, 51.$$

16. Hoc modo calculum ulterius prosequi licet, quousque visum fuerit. Exclusiones ex singulis valoribus ipsius z ortas sequenti tabula repraesentemus:

z	Exclusiones
1	4, 8
2	11, 29, 30
3	14, 23, 34, 65
4	- - - -
5	19, 21, 23, 33, 39, 47, 91, 183
6	23, 25, 41, 55, 88, 89, 260, 263
7	54
8	32, 40, 80, 232, 234
9	70, 198,
10	[illegible], 50, 147, 148, 244,
11	[illegible], 43, 51, 54, 63, [illegible], 93, 114, 222, 293,
12	[illegible], 5[illegible], 60, 69, 101, 141, 179
14	[illegible], 58, 66, 75, 1[illegible], 13[illegible], 16[illegible], 2[illegible]6, 2[illegible]7,

z	Exclusiones
15	64, 68, 88, 116, 236,
16	61, 77, 103, 161, 191,
17	120, 132, 168,
18	265, 266,
19	75, 147, 243, 80, 88,
21	80, 85, 83, 97, 103, 109, 128, 145, 163, 221, 235, 272,
22	84, 96, 123, 276,
23	90, 122, 178,
24	92, 140, 154
25	98, 110, 154, 194
26	108, 145,
27	103, 105, 111, 129, 125, 147, 203, 209, 241.
29	122, 134, 166, 218, 225,
30	122, 131, 133, 146, 187, 214,
31	240,
32	139, 224,
33	256,
34	130, 141, 190,
35	137, 143, 162, 169, 247, 271,
37	141, 145, 171, 287,
38	212,
39	154, 202
40	156, 174, 178, 242,
41	162, 186,
42	160, 220, 268
43	164, 195, 199, 211, 284,
45	208,
46	191, 217, 257,
47	184,
48	185, 253, 241,

z	Exclusiones
49	260
50	191, 193
51	196, 236, 292
53	202, 223, 245, 260,
54	224
56	216, 240
58	224, 236, 296
59	225, 231, 233, 272
61	239, 241, 282
62	237,
63	240,
64	246, 282
65	252
66	274
67	282
69	263, 265, 295, 263, 265
71	278
73	286
75	286, 290
78	298

17. Inter hos numeros excludendos pro littera a nonnulli bis vel ter occurrunt, quod evenit, quando numerus $232aa+1$ tres pluresve habet factores; ita videmus, numerum 265 primo a valore $z=18$, deinde bis a valore $z=69$ excludi. Hoc autem casu revera numerus 232.265^2+1 constat his tribus factoribus: $59.461.599$, atque adeo praeter istam formam tres sequentes recipit:

1° 232.256^2+1043^2

2° 232.34^2+4003^2

3° 232.35^2+4001^2.

18.

18. Referamus autem in tabulam omnes hos numeros excludendos, secundum ordinem dispositos, atque eos, qui plus quam semel occurrunt, asterisco notemus

0	4, 8
1	11, 14, 19
2	21, 23*, 25
3	3[illegible], 32, 33, 34, 39
4	40, 41, 42, 43, 47
5	51*, 54*, 55, 56, 58, 59
6	60, 61, 63, 64, 65, 66, 68, 69
7	7[illegible], 75, 77, 78
8	80*, 83, 84, 85*, 88*, 89
9	90, 91, 92, 93, 96, 97, 98
10	101, 102, 103, 105, 108, 109
11	110, 111, 114, 116
12	120, 122, 123, 125, 128, 129
13	130, 131, 132, 133, 134, 135, 137, 139
14	140, 141, 143, 145, 146, 147, 148
15	154, 156
16	160, 161, 162, 163, 164, 166, 168, 169
17	171, 174, 178, 179
18	183, 184, 185, 186, 187
19	190, 191, 193, 194, 195, 196, 198, 199
20	202, 203, 206, 207, 208, 209
21	211, 212, 214, 216, 217, 218
22	220, 221, 222, 223, 224, 225
23	231, 232, 233, 234, 235, 236, 237, 239
24	240, 241, 242, 243, 244, 245, 246, 247
25	252, 253, 256, 257,
26	260, 263, 2[illegible], 266, 268
27	271, 272, 274, 276, 278

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, 1[illegible], 12, 13, 15, 16, 17, 18,
20, 22, 24, 26, 27, 28, 29, 31, 35, 36, 37, 38,
44, 45, 46, 48, 49, 50, 5[illegible], 53, 57, 62, 67, 71,
72, 73, 74, 76, 79, 81, 82, 86, 87, 94, 95, 99, 100,
104, 106, 107, 112, 113, 11[illegible], 117, 118, 219, 121,
124, 126, 127, 136, 138, 142, 144, 149, 150, 151,
152, 153, 155, 157, 158, 159, 16[illegible], 167, 170, 172,
173, 175, 176, 177, 18[illegible], 181, 182, 186, 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, 272,
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 $\frac{a+x}{y+b} = \lambda . \frac{y-b}{a-x}$, quae fractiones ad minimos terminos reducti sint $\lambda . \frac{p}{q}$. 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