— 918), quarum determinantes sunt 997331, 1994662:

(1, 998, — 1327)	(1, 1412, — 918)
(— 1327, 329, 670)	(— 918, 1342, 211)
(670, 341, — 1315)	(211, 1401, — 151)
(— 1315, 974, 37)	(— 151, 1317, 1723)
(37, 987, — 626)	(1723, 406, — 1062)
(— 626, 891, 325)	(— 1062, 656, 1473)
(325, 734, — 1411)	(1473, 817, — 901)
(— 1411, 677, 382)	(— 901, 985, 1137)
(382, 851, — 715)	etc.

Sunt itaque residua numeri 997331 omnes numeri — 1327, 670 etc.; negligendo autem ea, quae factores nimis magnos implicant, haecce habemus: 2.5.67, 37, 13, — 17.83, — 5.11.13, — 2.3.17, — 2.59, — 17.53; residuum 2.5.67, nec non hoc — 5.11, quod e combinatione tertii cum quinto euoluitur, iam supra erueramus.

III. Si C est classis quaecunque formarum det. neg. $-M$ siue generalius $-kM$, a principali diuersa, ipsiusque periodus haec $2C$, $3C$ etc. (art. 307.): classes $2C$, $4C$ etc. ad genus principale pertinebunt; hae vero $3C$, $5C$ etc. ad idem genus vt C. Si itaque (a, b, c) est forma (simplicissima) ex C atque (a', b', c') forma ex aliqua classe illius periodi puta ex nC, erit vel a', vel aa' residuum ipsius M, prout n par vel impar (in casu priori manifesto etiam c', in posteriori ac', ca' et cc'). Euolutio periodi, i. e. formarum simplicissimarum in ipsius classibus, mira facilitate perficitur, quando a est valde paruus, praesertim quando est $= 3$, quod semper efficere licet, quando $kM \equiv 2$ (mod. 3). Ecce initium periodi classis, in qua est forma (3, 1, 332444)

C (3, 1, 332444)	$6C$ (729, — 209, 1428)
$2C$ (9, — 2, 110815)	$7C$ (476, 209, 2187)
$3C$ (27, 7, 36940)	$8C$ (1027, 342, 1085)
$4C$ (81, 34, 12327)	$9C$ (932, — 437, 1275)
$5C$ (243, 34, 4109)	$10C$ (425, 12, 2347)

Hinc promanant residua (inutilibus reiectis) 3.476, 1027, 1085, 425 siue (tollendo factores quadratos) 3.7.17, 13.79, 5.7.31, 17; e quorum combinatione apta cum octo residuis in II inuentis facile eruuntur duodecim sequentia — 2.3, 13, — 2.7, 17, 37, — 53, — 5.11, 79, — 83, — 2.59, — 2.531, 2.5.67; sex priores sunt iidem quibus in art. 331 vsi sumus. Adiici potuissent residua 19 et — 29, si ea quoque in vsum vocare voluissemus, quae in I reperta sunt; reliqua illic eruta ab iis quae hic euoluimus iam sunt dependentia.

333. Methodus secunda, numerum datum M in factores resoluendi, petitur e consideratione valorum talis expr. $\sqrt{-D}$ (mod. M), obseruationibusque sequentibus innititur.

I. Quando M est numerus primus aut potestas numeri primi (imparis ipsumque D non metientis), erit $-D$ residuum vel non residuum ipsius M, prout M vel in forma diuisorum vel in forma non diuisorum ipsius $xx + D$ continetur, et in casu priori expressio $\sqrt{-D}$ (mod.

M) duos tantummodo valores diuersos habebit, qui oppositi erunt.

II. Quando vero M est compositus, puta $= pp'p''$ etc., designantibus p, p', p'' etc. numeros primos (diuersos impares ipsumque D non metientes) aut talium numerorum potestates: $-D$ tunc tantummodo residuum ipsius M erit, quando est residuum singulorum p, p', p'' etc., i. e. quando hi numeri omnes in formis diuisorum ipsius $xx + D$ continentur. Designando autem valores expr. $\sqrt{-D}$ sec. modulos p, p', p'' etc. resp. per $\pm r$, $\pm r'$, $\pm r''$ etc., omnes valores eiusdem expressionis sec. mod. M orientur, eruendo numeros qui secundum p sint $\equiv r$ aut $\equiv -r$, secundum p' aut $\equiv r'$ aut $\equiv -r'$ etc., quocirca ipsorum multitudo fiet $= 2^\mu$, designante μ multitudinem numerorum p, p', p'' etc. Quodsi itaque hi valores sunt R, $-R$, R', $-R'$, R'' etc., sponte erit $R \equiv R$ secundum omnes p, p', p'' etc., sed secundum nullos $R \equiv -R'$, vnde diuisor communis maximus numeri M cum $R - R$ erit M, et 1 diu. comm. max. ipsius M cum $R + R'$; sed valores duo nec identici nec oppositi vt R et R' necessario secundum vnum pluresue numerorum p, p', p'' etc., neque vero secundum omnes, congrui erunt, et secundum reliquos $R \equiv -R'$; hinc illorum productum erit diuisor communis maximus numerorum M et $R - R'$, productumque horum d. c. m. ipsorum M et $R + R'$. Hinc facile sequitur, si omnes diuisores communes maximi ipsius M cum differentiis inter singulos valores expr. $\sqrt{-D}$ (mod. M) atque aliquem valorem datum