

modulum  $a$ ,  $b$  locum habent, etiam secundum modulum  $ab$  valebunt. Hinc per theoriam formarum ternariarum facile concluditur,  $\phi$  repraesentabilem esse per formam  $\begin{pmatrix} -1, 0, 0 \\ 1, 0, 0 \end{pmatrix}$ ; sit itaque  $actt + 2ahtu + iuu = -(\alpha t + \zeta u)^2 + 2(\gamma t + \delta u)(\epsilon t + \zeta u)$ , eritque, multiplicando per  $c$ ,  $a(ct + hu)^2 + buu = -c(\alpha t + \zeta u)^2 + 2c(\gamma t + \delta u)(\epsilon t + \zeta u)$ . Hinc patet, si ipsis  $t, u$  tales valores determinati tribuantur, ut vel  $\gamma t + \delta u$ , vel  $\epsilon t + \zeta u$  fiat  $= 0$ , haberi solutionem aequationis  $\Omega$ , cui igitur satisfiet tum per  $x = \delta c - \gamma h$ ,  $y = \gamma$ ,  $z = \alpha \delta - \zeta \gamma$ , tum per  $x = \zeta c - \epsilon h$ ,  $y = \epsilon$ ,  $z = \alpha \zeta - \zeta \epsilon$ ; simul manifestum est, neque illos valores neque hos simul  $= 0$  fieri posse; si enim  $\delta c - \gamma h = 0$ ,  $\gamma = 0$ , fieret etiam  $\delta = 0$  atque  $\phi = -(\alpha t + \zeta u)^2$  unde  $ab = 0$  contra hyp., et perinde de alteris. — In exemplo nostro inuenimus formam  $\phi$  hanc (161, — 63, 24), valorem expr.  $\sqrt{-\phi} \pmod{105} = (7, -51)$ , atque repraesentationem formae  $\phi$  per  $\begin{pmatrix} -1, 0, 0 \\ 1, 0, 0 \end{pmatrix}$  hanc,  $\phi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$ ; hinc prodeunt solutiones  $x = 7$ ,  $y = 11$ ,  $z = -8$ ;  $x = 20$ ,  $y = 15$ ,  $z = -5$ , siue diuidendo per 5 et negligendo signum ipsius  $z$ ,  $x = 4$ ,  $y = 3$ ,  $z = 1$ .

Ex his duabus methodis aequationem  $\Omega$  soluendi posterior eo praestat, quod plerumque per numeros minores absoluitur; prior vero, quae etiam per varia artificia hic silentio praetereunda contrahi potest, elegantior videtur ea imprimis ratione, quod numeri  $a, b, c$  prorsus eodem

modo tractantur, calculusque per horum permutationem quaecunque nihil mutatur. Hoc secus se habet in methodo secunda, vbi calculus maxime commodus plerumque prouenit, si pro  $a$  accipitur minimus, pro  $c$  maximus trium numerorum datorum, vti in exemplo nostro fecimus.

296. Elegans theorema in artt. praec. explicatum primo inuentum est ab ill. Le Gendre, *Hist. de l'Ac. de Paris* 1785 p. 507, atque demonstratione pulcra (a duabus nostris omnino diuersa) munitum. Simul vero hic egregius geometra hoc loco operam dedit, demonstrationem propositionum quae cum theoremate fundamentalis sect. praec. conueniunt inde deriuare, quam ad hunc scopum non idoneam nobis videri iam supra declarauimus, art. 151. Hic itaque locus erit, hanc demonstrationem (per se valde elegantem) breuiter exponendi iudiciiue nostrae rationes adiungendi. Praemittitur sequens observatio: Si numeri  $a, b, c$  omnes sunt  $\equiv 1 \pmod{4}$ , aequatio  $axx + byy + czz = 0 \dots (\Omega)$  solubilis esse nequit. Facillime enim perspicitur, valorem ipsius  $axx + byy + czz$  necessario in hoc casu fieri vel  $\equiv 1$ , vel  $\equiv 2$ , vel  $\equiv 3 \pmod{4}$ , nisi omnes  $x, y, z$  simul pares accipiantur; si itaque  $\Omega$  solubilis esset, hoc aliter fieri non posset quam per valores pares ipsorum  $x, y, z$ , Q. E. A., quoniam valores quicunque aequationi  $\Omega$  satisfaciunt etiamnum satisfaciunt, si per diuisorem communem maximum diuiduntur, vnde necessario ad minimum vnus impar prodire debet. Iam casus diuersi theorematis demonstrandi ad sequentia momenta referuntur:



I. Designantibus  $p, q$  numeros primos formae  $4n + 3$  (positiuos inaequales), nequit simul esse  $pRq, qRp$ . Si enim possibile esset, manifestum est statuendo  $1 = a, -p = b, -q = c$ , omnes conditiones ad resolubilitatem aequationis  $axx + byy + czz = 0$  adimpletas esse (art. 294); eadem vero per observationem praec. resolutionem non admittit; quare suppositio consistere nequit. Hinc protinus sequitur propositio 7 art. 131.

II. Si  $p$  est numerus primus formae  $4n + 3$ , nequit simul esse  $qRp, pNq$ . Alioquin enim foret  $-pRq$ , atque aequatio  $xx + pyy - qzz = 0$  resolubilis, quae per obs. praec. resolutionem respuit. Hinc deriuantur casus 4 et 5 art. 131.

III. Si  $p, q$  sunt numeri primi formae  $4n + 1$ , nequit simul esse  $pRq, qNp$ . Accipiaturs alius numerus primus  $r$  formae  $4n + 3$ , qui sit residuum ipsius  $q$  et cuius non-residuum sit  $p$ . Tunc erit per casus modo (II) demonstratos  $qRr, rNp$ . Si itaque esset  $pRq, qNq$ , foret  $qrRp, pRq, pqNr$  et proin  $-pqRr$ . Hinc aequatio  $pxx + qyy - rzz = 0$  resolubilis esset contra obs. praec.; quare suppositio consistere nequit. Hinc sequuntur casus 1 et 2 art. 131.

Concinnius hic casusse quenti modo tractatur. Designet  $r$  numerum primum formae  $4n + 3$  cuius non residuum sit  $p$ . Tunc erit etiam  $rNp$ , adeoque (supponendo  $pRq, qNp$ )  $qrRp$ , porro  $-pRq, -pRr$  et proin etiam  $-pRqr$ ; quare