

294. THEOREMA. Designantibus a, b, c , numeros inter se primos quorum nullus neque $= 0$ neque per quadratum diuisibilis, aequatio $axx + byy + czz = 0 \dots (\Omega)$ resolutionem in integris non admittet (praeter hanc $x = y = z = 0$ ad quam non respicimus) nisi $-bc, -ac, -ab$ resp. sint residua quadratica ipsorum a, b, c , atque hi numeri signis in aequalibus affecti; his vero quatuor conditionibus locum habentibus, (Ω) in integris resolubilis erit.

Dem. Si (Ω) per integros omnino est resolubilis, etiam per tales valores ipsorum x, y, z resolui poterit qui diuisorem communem non habent; nam valores quicunque, aequ. Ω satisfacientes, etiamnum satisfacent, si per diuisorem communem maximum diuiduntur. Iam supponendo $app + bqg + crs = 0$, atque p, q, r a diuisore communi liberos, etiam inter se primi erunt; si enim q, r diuisorem communem μ haberent, hic ad p primus esset, $\mu\mu$ autem metiretur ipsum app adeoque etiam ipsum a , contra hyp.; et perinde $p, r; p, q$ inter se primi erunt. Repraesentatur itaque $-app$ per formam binariam $byy + czz$, tribuendo ipsis y, z valores inter se primos q, r ; vnde illius determinans $-bc$ residuum quadraticum ipsius app adeoque etiam ipsius a erit (art. 154); eodem modo erit $-acRb, -abRc$. Quod vero (Ω) resolutionem admittere non possit, si a, b, c idem signum habeant, tam obuium est ut explicacione non egeat.

Demonstrationem propositionis inuersae, quae theorematis partem secundam constituit, ita adornabimus, ut primo formam ternariam ipsi

$(\begin{smallmatrix} a & b & c \\ o & o & o \end{smallmatrix})$... f aequiualentem inuenire doceamus, cuius coëfficientes 2, 3, 4 per abc diuisibles sint, vnde secundo solutionem aëquationis (Ω) deducemus.

I. Inuestigentur tres integri A, B, C a diuisore communi liberi, atque ita comparati, vt A primus sit ad b et c ; B ad a et c ; C ad a et b ; $aAA + bBB + cCC$ autem per abc diuisibilis, quod efficietur sequenti modo. Sint $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ resp. valores expressionum $\sqrt{-bc}$ (mod. a), $\sqrt{-ac}$ (mod. b), $\sqrt{-ab}$ (mod. c), qui necessario ad a, b, c resp. primi erunt. Accipientur tres integri a, b, c omnino ad libitum, modo ita vt ad a, b, c resp. primi sint (e. g. omnes = 1), determinenturque A, B, C ita vt sit $A \equiv bc$ (mod. b) et $\equiv c\mathfrak{C}$ (mod. c); $B \equiv ca$ (mod. c) et $\equiv a\mathfrak{A}$ (mod. a), $C \equiv ab$ (mod. a) et $\equiv b\mathfrak{B}$ (mod. b). Tunc fiet $aAA + bBB + cCC \equiv aa(b\mathfrak{A}\mathfrak{A} + cbb) \equiv aa(b\mathfrak{A}\mathfrak{A} - \mathfrak{A}\mathfrak{A}b) \equiv o$ (mod. a) siue per a diuisibilis, et perinde per b, c , adeoque etiam per abc diuisibilis erit. Praeterea patet, A necessario fieri primum ad b et c ; B ad a et c ; C ad a et b . Si vero hi valores ipsorum A, B, C diuisorem communem (maximum) μ implicant, hic manifesto ad a, b, c adeoque ad abc primus erit; quare illos valores per μ diuidendo nouos obtinebimus, qui diuisorem communem non habebunt, valorem ipsius $aAA + bBB + cCC$ etiamnum per abc diuisibilem producent, adeoque omnibus conditionibus satisfacent.

II. Numeris A, B, C , hoc modo determinatis, etiam Aa, Bb, Cc diuisorem communem

non habebunt. Si enim haberent diu. comm. μ , hic necessario primus esset ad a (quippe qui tum ad Bb tum ad Cc primus est) et similiter ad b et c ; quare μ etiam ipsos A , B , C metiri deberet, contra hyp. Inueniri poterunt itaque integri α , β , γ tales ut sit $\alpha Aa + \beta Bb + \gamma Cc = 1$; quaerantur insuper sex integri α' , β' , γ' , α'' , β'' , γ'' tales ut sit $\beta''\gamma'' - \gamma'\beta'' = Aa$, $\gamma'\alpha'' - \alpha''\gamma'' = Bb$, $\alpha'\beta'' - \beta'\alpha'' = Cc$. Iam transeat f per substitutionem

$$\begin{array}{l} \alpha, \alpha', \alpha'' \\ \beta, \beta', \beta'' \\ \gamma, \gamma', \gamma'' \end{array}$$

in $\binom{m, m', m''}{n, n', n''} = g$ (quae ipsi f aequivalens erit), dicoque m' , m'' , n per abc diuisibiles fore. Ponatur enim $\beta''\gamma'' - \gamma'\beta'' = A'$, $\gamma'\alpha'' - \alpha''\gamma'' = B'$, $\alpha''\beta'' - \beta'\alpha'' = C'$, $\beta'\gamma' - \gamma'\beta' = A''$, $\gamma'\alpha' - \alpha'\gamma' = B''$, $\alpha'\beta' - \beta'\alpha' = C''$, eritque $\alpha' = B''Cc - C''Bb$, $\beta' = C'Aa - A''Cc$, $\gamma' = A''Bb - B''Aa$, $\alpha'' = C'Bb - B'Cc$, $\beta'' = A'Cc - C'Aa$, $\gamma'' = B'Aa - A'Bb$. Quibus valoribus in aequationibus $m' = a\alpha'\alpha' + b\beta'\beta' + c\gamma'\gamma'$, $m'' = a\alpha''\alpha'' + b\beta''\beta'' + c\gamma''\gamma''$, $n = a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma''$ substitutis, fit, secundum modulum a , $m' \equiv bcA'A''(BBb + CCc) \equiv 0$, $m'' \equiv bcA'A'(BBb + CCc) \equiv 0$, $n \equiv bcA'A''(BBb + CCc) \equiv 0$, i. e. m' , m'' , n per a diuisibiles erunt; similique modo iidem numeri per b , c adeoque etiam per abc diuisibiles inteniuntur. Q. E. P.

III. Ponamus, concinnitatis caussa, determinantem formarum f , g , i. e. numerum $-abc$