

minimus primus huius formae, cuius non-residuum $\pm 2, = a$, ita vt pro omnibus primis ipso a minoribus theorema valeat. Tum accipiat numerus aliquis primus $< \frac{1}{2}a$, cuius non-residuum a (qualem dari ex art. 129 facile deducitur). Sit hic $= p$ eritque per theor. fund. pNa . Hinc fit $\pm 2pRa$. — Sit itaque $e^2 \equiv 2p \pmod{a}$ ita vt e sit impar atque $< a$. Tum duo casus erunt distinguendi.

I. Quando e per p non est diuisibilis. Sit $e^2 = 2p + aq$ eritque q positius, formae $8n + 7$ vel formae $8n + 3$, (prout p est formae $4n + 1$ vel $4n + 3$), $< a$, atque per p non diuisibilis. Iam omnes factores primi ipsius q in quatuor classes distribuuntur, sint scilicet e formae $8n + 1$, f formae $8n + 3$, g formae $8n + 5$, h formae $8n + 7$; productum e factoribus primae classis sit E , producta e factoribus secundae, tertiae, quartae classis respectiue, $F, G, H^*)$. His ita factis, consideremus primo casum vbi p est formae $4n + 1$, siue q formae $8n + 7$. Tum facile perspicitur fore $2RE, 2RH$, vnde pRE, pRH , hincque tandem ERp, HRp . Porro erit 2 non-residuum cuiusuis factoris formae $8n + 3$ aut $8n + 5$, adeoque etiam p ; hinc quiuis talis factor non-residuum ipsius p ; vnde facile concluditur FG fore ipsius p residuum, si $f + g$ fuerit par, non-residuum, si $f + g$ fuerit impar. At $f + g$ impar esse non potest; facile enim perspicietur omnes casus enumerando, $EFGH$ siue q fieri

*) Si ex aliqua classe nulli factores adessent, loco producti ex his describere oporteret.

vel formae $8n + 3$ vel $8n + 5$, si fuerit $f + g$ impar, quidquid sint singuli e, f, g, h . contra hyp. Erit igitur $FGRp, EFGHRp$, siue qRp , hincque tandem, propter $aqRp, aRp$ contra hyp. Secundo quando p est formae $4n + 3$, simili modo ostendi potest, fore pRE adeoque ERp , — pRF adeoque FRp , tandem $g + h$ parem hincque $GHRp$, vnde tandem sequitur qRp, aRp contra hyp.

II. Quando e per p diuisibilis, demonstratio simili modo adornari, et a peritis (quibus solis hic articulus est scriptus) haud difficulter euolui poterit. Nos breuitatis gratia eam o-mittimus.

146. Per theorema fundamentale atque propositiones ad residua — 1 et ± 2 pertinentes semper determinari potest vtrum numerus quicunque datus numeri primi dati residuum sit an non-residuum. At haud inutile erit, reliqua etiam quae supra tradidimus hic iterum in conspectum producere, vt omnia coniuncta habeantur quae sunt necessaria ad solutionem

PROBLEMATIS: *Propositis duobus numeris quibuscunque P, Q , inuenire, vtrum alter Q , alterius P residuum sit an non-residuum.*

Sol. I. Sit $P = a^x b^y c^z$ etc. designantibus a, b, c etc. numeros primos inaequales positue acceptos (nam P manifesto absolute est sumendus). Breuitatis gratia in hoc art. relationem duorum numerorum x, y simpliciter di-

cemus eam quatenus prior x posterioris y residuum est vel non-residuum. Pendet igitur relatio ipsorum Q, P a relationibus ipsorum Q, a^a, Q, b^b etc. (art. 105).

II. Vt relatio ipsorum Q, a^a (de reliquis enim Q, b^b etc. idem valet) innotescat, duo casus distinguendi.

1. Quando Q per a est diuisibilis. Ponatur $Q = Q'a^e$, ita vt Q' per a non sit diuisibilis. Tunc si $e = a$ vel $e > a$, erit QRa^a ; si vero $e < a$ atque impar, erit QNa^a : tandem si $e < a$ atque par, habebit Q ad a^a eandem relationem quam habet Q' ad a^{a-e} . Reductus est itaque hic casus ad

2. Quando Q per a non est diuisibilis. Hic denuo duos casus distinguimus.

(A) Quando $a = 2$. Tunc semper erit QRa^a , quando $a = 1$; quando vero $a = 2$, requiritur, vt sit Q formae $4n + 1$; denique quando $a = 3$ vel > 3 . Q debet esse formae $8n + 1$. Quae conditio si locum habet, erit QRa^a .

(B) Quando a est alius numerus primus. Tunc Q ad a^a eandem relationem habebit quam habet ad a . (V. art. 101).

III. Relatio numeri cuiuscunque Q ad numerum primum a (imparem) ita inuestigatur.