I. *Numerorum omnium primorum formae* $8n+3$, $+2$ *erit non-residuum,* -2 *vero residuum.*

II. *Numerorum omnium primorum formae* $8n+5$, *tum* $+2$ *tum* -2 *erunt non-residua.*

113. Per similem inductionem ex tab. II inueniuntur numeri primi quorum residuum est -2 hi: 3, 11, 17, 19, 41, 59, 67, 73, 83, 89, 97 *). Inter quos quum nulli inueniantur formarum $8n+5$, $8n+7$, num etiam haec inductio theorematis generalis vim adipisci possit inuestigemus. Ostenditur simili modo vt in art. praec. quemuis numerum compositum formae $8n+5$ vel $8n+7$, factorem primum inuoluere formae $8n+5$ vel formae $8n+7$, ita vt, si inductio nostra generaliter vera, -2 nullius omnino numeri formae $8n+5$ vel $8n+7$ residuum esse possit. Si autem tales numeri darentur, ponatur omnium minimus $=t$, fiatque $-2=aa-tu$. Vbi si vti supra a impar ipsoque t minor accipitur, u erit formae $8n+5$ vel $8n+7$, prout t formae $8n+7$ vel $8n+5$. At ex eo quod $aa+2=tu$ atque $a<t$; quisquis facile deriuari poterit, etiam u ipso t minorem fore. Denique -2 etiam ipsius u residuum erit; i. e. t non erit minimus numerus qui inductioni nostrae aduersatur, contra hyp. Quare necessario -2 omnium numerorum formarum $8n+5$, $8n+7$ non residuum.

*) Considerando scilicet -2 tamquam productum ex $+2$ et -1 V. art. 111.

Combinando haec cum propp. art. 111, prodeunt theoremata haec:

I. *Omnium numerorum primorum formae* $8n+5$, *tum* -2, *tum* $+2$ *sunt non-residua*, vti iam in art. praec. inuenimus.

II. *Omnium numerorum primorumm formae* $8n+7$, -2 *est non-residuum*, $+2$ *vero residuum.*

Ceterum in vtraque demonstratione pro a etiam valorem parem accipere potuissemus; tunc autem casum vbi a fuisset formae $4n+2$, ab eo distinguere oportuisset, vbi a formae $4n$. Euolutio autem perinde procedit vti supra, nullique difficultati est obnoxia.

114. Vnus adhuc superest casus, scilicet vbi numerus primus est formae $8n+1$. Hic vero methodum praecedentem eludit, artificiaque prorsus peculiaria postulat.

Sit pro modulo primo $8n+1$, radix quaecunque primitiua, a, eritque (art. 62) $a^{4n} \equiv -1$ (mod. $8n+1$), quae congruentia ita etiam exhiberi potest, $(a^{2n}+1)^2 \equiv 2a^{2n}$ (mod. $8n+1$), siue etiam ita, $(a^{2n}-1)^2 \equiv -2a^{2n}$. Vnde sequitur tum $2a^{2n}$, tum $-2a^{2n}$ ipsius $8n+1$ esse residuum: at quia a^{2n} est quadratum per modulum non diuisibile, manifesto etiam tum $+2$ tum -2 residua erunt (art. 98.)

115. Haud inutile erit, adhuc aliam huius theorematis demonstrationem adiicere, quae similem relationem ad praecedentem habet, vt theorematis art. 108 demonstratio secunda

(art. 109) ad primam (art. 108). Periti facilius tunc perspicient, binas demonstrationes tam illas quam has non adeo heterogeneas esse, quam primo forsan aspectu videantur.

I. Pro modulo quocunque primo formae $4m + 1$, inter numeros ipso minores $1, 2, 3 \ldots 4m$, reperientur m qui biquadrato congrui esse possunt, reliqui vero $3m$ non poterunt.

Facile quidem hoc ex principiis sect. praec. deriuatur, sed etiam absque his demonstratio haud difficilis. Demonstrauimus enim pro tali modulo -1 semper esse residuum quadraticum. Sit itaque $ff \equiv -1$ patetque, si z fuerit numerus quicunque per modulum non diuisibilis, quaternorum numerorum $+z$, $-z$, $+fz$, $-fz$ (quos incongruos esse facile perspicitur) biquadrata inter se congrua fore; porro manifestum est biquadratum numeri cuiuscunque, qui nulli ex his quatuor congruus, illorum biquadratis congruum fieri non posse, (alias enim congruentia $x^4 \equiv z^4$ quae est quarti gradus plures quam 4 radices haberet, contra art. 43). Hinc facile colligitur, omnes numeros $1, 2, 3, \ldots 4m$, tantummodo m biquadrata incongrua praebere, quibus inter eosdem numeros m congrui reperientur, reliqui autem nulli biquadrato congrui esse poterunt.

II. Secundum modulum primum formae $8n + 1$, -1 biquadrato congruus fieri poterit (-1 erit *residuum biquadraticum* huius numeri primi).