Omnium enim residuorum biquadraticorum ipso $8n + 1$ minorum (cifra exclusa) multitudo erit $= 2n$ i. e. par. Porro facile probatur, si r fuerit residuum biquadraticum ipsius $8n + 1$, etiam valorem expr. $\frac{1}{r}$ (mod. $8n + 1$) fore tale residuum. Hinc omnia residua biquadratica in classes simili modo distribui poterunt, vti in art. 109 residua quadratica distribimus: nec non reliqua demonstrationis pars prorsus eodem modo procedit vt illic.

III. Iam sit $g^4 \equiv -1$, et h valor expr. $\frac{1}{g}$ (mod. $8n + 1$). Tunc erit $(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$ (propter $gh \equiv 1$). At $g^4 \equiv -1$, adeoque $-h^2 \equiv g^4 h^2 \equiv g^2$, vnde tandem $g^2 + h^2 \equiv 0$, atque $(g \pm h)^2 \equiv \pm 2$ *i. e.* tum $+2$, tum -2 residuum quadraticum ipsius $8n + 1$. *Q. E. D.*

116. Ceterum ex praec. facile regula sequens generalis deducitur: $+2$ *est residuum numeri cuiusuis, qui neque per* 4, *neque per vllum primum formae* $8n + 3$ *vel* $8n + 5$ *diuidi potest, reliquorum autem* (ex. gr. omnium numerorum formarum $8n + 3$, $8n + 5$, siue sint primi, siue compositi) *non-residuum.*

-2 *est residuum numeri cuiusuis, qui neque per* 4, *neque per vllum primum formae* $8n + 5$ *vel* $8n + 7$ *diuidi potest, omnium autem reliquorum non-residuum.*

Theoremata haec elegantia iam sagaci Fermatio innotuerunt, *Op. Mathem.* p. 168.

Demonstrationem vero quam se habere professus est, nusquam communicauit. Postea ab ill. Euler frustra semper est inuestigata: at ill. La Grange primus demonstrationem rigorosam reperit, *Nouv. Mem. de l'Ac. de Berlin* 1775. p. 349, 351. Quod ill. Eulerum adhuc latuisse videtur, quando scripsit diss. in *Opusc. Analyt.* conseruatam, T. I. p. 259.

117. Pergimus ad residua + 3 et — 3. A posteriori initium faciamus.

Reperiuntur ex tab. II. numeri primi quorum residuum est — 3, hi: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, inter quos nullus inuenitur formae $6n + 5$. Quod vero etiam vltra tabulae limites nulli primi huius formae dantur quorum residuum — 3, ita demonstramus: Primo patet quemuis numerum compositum formae $6n + 5$ necessario factorem primum aliquem eiusdem formae inuoluere. Quousque igitur nulli numeri primi formae $6n + 5$ dantur, quorum residuum — 3, eousque tales etiam compositi non dabuntur. Quodsi vero vltra tabulae nostrae limites tales numeri darentur, sit omnium minimus $= t$, ponaturque $-3 = aa - tu$. Tunc erit, si acceperis a parem ipsoque t minorem, $u < t$, atque — 3 residuum ipsius u. Sed quando a formae $6n \pm 2$, tu erit formae $6n + 1$, adeoque u formae $6u + 5$, *Q. E. A.* quia t minimum esse numerum inductioni nostrae aduersantem supposuimus. Quando vero a formae $6n$, erit tu formae $36n + 3$ adeoque $\frac{1}{3}tu$ formae $12n + 1$,

quare $\frac{1}{3}u$ erit formae $6n + 5$; patet autem -3 etiam ipsius $\frac{1}{3}u$ residuum fore, atque esse $\frac{1}{3}u < t$, *Q. E. A.* Manifestum itaque, -3 nullius numeri formae $6n + 5$ residuum esse posse.

Quoniam quisque numerus formae $6n + 5$ necessario vel sub forma $12n + 5$, vel sub hac $12n + 11$ continetur, prior autem forma sub hac $4n + 1$, posterior sub hac $4n + 3$, haec habentur theoremata:

I. *Cuiusuis numeri primi formae* $12n + 5$, *tum* -3 *tum* $+3$ *non-residuum est.*

II. *Cuiusuis numeri primi formae* $12n + 11$, -3 *est non-residuum,* $+3$ *vero residuum.*

118. Numeri quorum residuum est $+3$ ex tabula II. inueniuntur hi: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, inter quos nulli sunt formae $12n + 5$, vel $12n + 7$. Nullos autem omnino numeros formarum $12n + 5$, $12n + 7$ dari quorum $+3$ sit residuum, eodem prorsus modo, vt in artt. 112, 113, 117, comprobari potest, quare hoc negotio supersedemus. Habemus itaque collato art. 111 theoremata:

I. *Numeri cuiusuis primi formae* $12n + 5$, *non-residua sunt tum* $+3$ *tum* -3, (vti iam in art. praec. inuenimus).

II. *Numeri cuiusuis primi formae* $12n + 7$ *non-residuum est* $+3$, -3 *vero residuum.*