Obseruamus adhuc, demonstrationes pro vtroque casu ill. La Grange deberi, *Mem. de l'Ac. de Berlin* 1775, p. 352 sqq.

124. Per similem methodum demonstratur,

— 7 esse non-residuum cuiusuis numeri primi q ipsius 7 sit non-residuum.

Ex inductione vero concludi potest,

— 7 esse residuum cuiusuis numeri qui ipsius 7 sit residuum.

At hoc a nemine hactenus rigorose demonstratum. Pro iis quidem residuis ipsius 7, qui sunt formae $4n - 1$, facilis est demonstratio; etenim per methodum ex praec. abunde notam ostendi potest, $+ 7$ semper esse talium numerorum primorum non-residuum, adeoque $- 7$ residuum. Sed parum hinc lucramur: reliqui enim casus per hanc methodum tractari nequeunt. Vnum quidem adhuc casum simili mod. vt artt. 119, 123 absoluere possumus. Scilicet si p est numerus primus formae $7n + 1$, atque a pro modulo p ad exponentem 7 pertinens, facile perspicitur $\frac{4(a^7 - 1)}{a - 1} = (2a^3 + a^2 - a - 2)^2 + 7(a^2 - a)^2$ per p diuisibilem, adeoque $- 7(a^2 - a)^2$ ipsius p residuum fore. At $(a^2 - a)^2$, tamquam quadratum, ipsius p residuum est, insuperque per p non diuisibile; quum enim a ad exponentem 7 pertinere supponatur, neque $\equiv 0$, neque $\equiv 1$ (mod. p) esse potest, i. e. neque a

neque $a - 1$ per p diuisibilis erit, adeoque etiam quadratum $(a-1)^2 a^2$. Vnde manisto etiam 7 ipsius p residuum erit. *Q. E. D.* — At primi numeri formae $7n+2$ vel $7n+4$ omnes methodos hucusque traditas eludunt. Ceterum etiam haec demonstratio ab ill. La Grange primum est detecta *l. c.* — Infra *sect.* VII. docebimus generaliter, expressionem $\frac{4(x^p - 1)}{x - 1}$ semper ad formam $X^2 \mp p Y^2$ reduci posse, (vbi signum superius est accipiendum quando p est numerus primus formae $4n+1$, inferius quando est formae $4n+3$), denotantibus X, Y functiones rationales ipsius x, a fractionibus liberas. Hanc discerptionem ill. La Grange vltra casum $p=7$ non perfecit v. *l. c.* p. 352.

125. Quoniam igitur methodi praecedentes ad demonstrationes generales stabiliendas non sufficiunt, iam tempus est, aliam ab hoc defectu liberam exponere. Initium facimus a theoremate, cuius demonstratio satis diu operam nostram elusit, quamuis primo aspectu tam obuium videatur, vt quidam ne necessitatem quidem demonstrationis intellexerint. Est vero hoc: *Quemuis numerum, praeter quadrata positiue sumta aliquorum numerorum primorum nonresiduum esse.* Quia vero hoc theoremate tantummodo tamquam auxiliari ad alia demonstranda vsuri sumus, alios casus hic non explicamus quam quibus ad hunc finem indigemus. De reliquis casibus postea sponte idem consta-

bit. Ostendemus itaque, *quemuis numerum primum formae* $4n + 1$, *siue positiue siue negatiue accipiatur* *), *non-residuum esse aliquorum numerorum primorum*, et quidem talium qui ipso sint minores.

Primo, quando numerus primus p, formae $4n + 1$, *negatiue* sumendus proponitur, sit $2a$ numerus par proxime maior quam $\sqrt{p}$; tum facile perspicitur, $4aa$ semper fore $< 2p$ siue $4aa - p < p$. At $4aa - p$ est formae $4n + 3$, $+ p$ autem residuum quadraticum ipsius $4aa - p$, (quoniam $p \equiv 4aa$ (mod. $4aa - p$)); quodsi igitur $4aa - p$ est numerus primus, $-p$ ipsius non-residuum erit; sin minus, necessario factor aliquis ipsius $4aa - p$ formae $4n + 3$ erit; et quum $+ p$ etiam huius residuum esse debeat, $- p$ ipsius non-residuum erit. *Q. E. D.*

Pro numeris primis *positiue* sumendis duos casus distinguimus. *Primo* sit p numerus primus formae $8n + 5$. Sit a numerus quicunque positiuus $< \sqrt{\frac{1}{2}p}$. Tum $8n + 5 - 2aa$ erit numerus positiuus formae $8n + 5$ vel $8n + 3$, (prout a par vel impar) adeoque necessario per numerum aliquem primum formae $8n + 3$ vel $8n + 5$ diuisibilis, productum enim ex quotcunque numeris formae $8n + 1$ et $8n + 7$ neque formam $8n + 3$ neque hanc $8n + 5$ habere potest. Sit hic q, eritque $8n + 5 \equiv 2a^2$ (mod. q). At 2

*) $+ 1$ autem excipi oportere per se manifestum est.