119. Nihil autem per hanc methodum pro numeris formae $12n + 1$ inueniri potest, qui proin artificia singularia requirunt. Ex inductione quidem facile colligitur, omnium numerorum primorum huius formae residua esse $+3$ et -3. Manifesto autem demonstrari tantummodo debet, numerorum talium residuum esse -3, quia tunc necessario etiam $+3$ residuum esse debet (art. 111). Ostendemus autem generalius, -3 esse residuum numeri cuiusuis primi formae $3n + 1$.

Sit p huiusmodi primus atque a numerus pro modulo p ad exponentem 3 pertinens (quales dari ex art. 55 manifestum, quia 3 submultiplum ipsius $p - 1$). Erit itaque $a^3 \equiv 1 \pmod{p}$ i. e. $a^3 - 1$ siue $(a^2 + a + 1)(a - 1)$ per p diuisibilis. Sed patet a esse non posse $\equiv 1 \pmod{p}$, quia 1 ad exponentem 1 pertinet, quare $a - 1$ per p diuisibilis non erit; sed $a^2 + a + 1$ erit, hincque etiam $4aa + 4a + 4$; i. e. erit $(2a + 1)^2 \equiv -3 \pmod{p}$ siue -3 residuum ipsius p. *Q. E. D.*

Ceterum patet, hanc demonstrationem (quae a praecedentibus est independens) etiam numeros primos formae $12n + 7$ complecti quos iam in art. praec. absoluimus.

Obseruare adhuc conuenit, hanc analysin ad instar methodi in artt. 109, 115 vsitatae exhiberi posse, at breuitatis gratia huic rei non immoramur.

120. Colliguntur facile ex praec. theoremata haec (vid. artt. 102, 103, 105).

I. — 3 *est residuum omnium numerorum, qui neque per* 8, *neque per* 9, *neque per vllum numerum primum formae* $6n + 5$ *diuidi possunt, non-residuum autem omnium reliquorum.*

II. + 3 *est residuum omnium numerorum, qui neque per* 4, *neque per* 9, *neque per vllum primum formae* $12n + 5$ *vel* $12n + 7$ *diuidi possunt, omnium reliquorum non-residuum.*

Teneatur imprimis casus particularis hic:

— 3 est *residuum* omnium numerorum primorum formae $3n + 1$, seu quod idem est *omnium, qui ipsius* 3 *sunt residua, non-residuum* vero omnium numerorum primorum formae $6n + 5$, seu, excluso numero 2, omnium formae $3n + 2$, i. e. *omnium qui ipsius* 3 *sunt non-residua.* Facile vero perspicitur omnes reliquos casus ex hoc sponte sequi.

Propositiones ad residua + 3 et — 3 pertinentia iam Fermatio notae fuerunt, *Opera Wallisii* T. II. p. 857. At ill. Euler primus demonstrationes tradidit, *Comm. nou. Petr.* T. VIII. p. 105 sqq. Eo magis est mirandum, demonstrationen propositionum ad residua + 2 et — 2 pertinentium, prorsus similibus artificiis innixas, semper ipsius sagacitatem fugisse. Vid. etiam comment. ill. La Grange, *Nouv. Mem. de l'Ac. de Berlin*, 1775 p. 352.

121. Per inductionem deprehenditur, + 5 nullius numeri imparis formae $5n + 2$, vel $5n + 3$ residuum esse, i. e. nullius numeri impa-

ris qui ipsius non-residuum sit. Hanc vero regulam nullam exceptionem pati, ita demonstratur. Sit numerus minimus, si quis datur, ab hac regula excipiendus $= t$, qui itaque numeri 5 est non-residuum, 5 autem ipsius t residuum. Sit $aa = 5 + tu$, ita vt a sit par ipsoque t minor. Erit igitur u impar ipsoque t minor, + 5 autem ipsius u residuum erit. Quodsi iam a per 5 non est diuisibilis, etiam u non erit; manifesto autem tu ipsius 5 est residuum, quare quum t ipsius 5 sit non-residuum, etiam u non-residuum erit; i. e. datur non-residuum numeri 5 cuius residuum est + 5, ipso t minus, contra hyp. Si vero a per 5 est diuisibilis, ponatur $a = 5b$, atque $u = 5v$, vnde $tv \equiv -1 \equiv 4 \pmod 5$, *i. e.* tv erit residuum numeri 5. In reliquis demonstratio perinde procedit vt in casu priori.

122. Omnium igitur numerorum primorum, qui simul sunt ipsius 5 non-residua simulque formae $4n + 1$, i. e. omnium numerorum primorum formae $20n + 13$ vel $20n + 17$, tum + 5 quam — 5 non residua erunt; omnium autem numerorum primorum formae $20n + 3$ vel $20n + 7$, non residuum erit + 5, — 5 residuum.

Potest vero prorsus simili modo demonstrari, — 5 esse non-residuum omnium numerorum primorum formarum $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$, facileque perspicitur hinc sequi, + 5 esse residuum omnium numerorum primorum formae $20n + 11$, vel $20n + 19$, non-