simul impares erunt. Sint enim factores primi ipsius P, hi f, f' f'' etc. et inter factores in quibus Q est resolutus, sint m qui ipsius f sint non-residua, m' non-residua ipsius f', m'' non-residua ipsius f'' etc. Tum facile quisquis perspiciet, fore $s = m + m' + m'' +$ etc., p autem exprimere quot numeri inter ipsos m, m', m'' etc. sint impares. Vnde sponte patet, s fore parem, quando p sit par, imparem quando p sit impar.

II. Haec generaliter valent, quomodocunque Q in factores sit resolutus. Descendamus ad casus particulares. Contemplemur primo casus, vbi alter numerorum, P, est positiuus, alter vero, Q, vel formae $+ A$ vel formae $- B$. Resoluantur P, Q in factores suos primos, attribuatur singulis factoribus ipsius P signum positium, singulis autem factoribus ipsius Q signum positiuum vel negatiuum, prout sunt formae a vel b; tunc autem manifesto Q fiet vel formae $+ A$ vel $- B$ vti requiritur. Combinentur factores singuli ipsius P cum singulis factoribus ipsius Q, designetque vt ante s multitudinem combinationum in quibus factor ipsius Q est non residuum factoris ipsius P, similiterque t multitudinem combinationum in quibus factor ipsius P est non-residuum factoris ipsius Q. At ex theoremate fundamentali sequitur illas combinationes indenticas fore cum his adeoque $s = t$. Tandem ex iis quae modo demonstrauimus sequitur esse $p \equiv s$ (mod. 2); $q \equiv t$ (mod. 2), vnde fit $p \equiv q$ (mod. 2).

Habentur itaque propp. 1, 3, 4 et 6 art. 133.

Propositiones reliquae per methodum similem directe erui possunt, sed vna consideratione noua indigent; facilius autem ex praecedentibus sequenti modo deriuantur.

III. Denotent rursus P, Q, numerus quoscunque impares inter se primos, p, q multitudinem factorum primorum ipsorum P, Q, quorum non-residua Q, P respectiue. Tandem sit p' multitudo factorum primorum ipsius P, quorum non-residuum est $-Q$ (quando Q per se est negatiuus, manifesto $-Q$ numerum positiuum indicabit). Iam omnes factores primi ipsius P in quatuor classes distribuantur.

1) in factores formae a, quorum residuum est Q.

2) factores formae b, quorum residuum Q. Horum multitudo sit χ.

3) factores formae a, quorum non-residuum est Q. Horum multitudo sit ψ.

4) factores formae b, quorum non-residuum Q. Quorum multitudo $= \omega$.

Tum facile perspicitur fore $p = \psi + \omega$, $p' = \chi + \psi$.

Iam quando P est formae $\pm A$, erit $\chi + \omega$ adeoque etiam $\chi - \omega$ numerus par: quare fiet $p' = p + \chi - \omega \equiv p$ (mod. 2); quando vero P est formae $\pm B$, per simile ratiocinium inuenitur, numeros p, p' sec. mod. 2 incongruos fore.

IV. Applicemus haec ad casus singulos. Sit primo tum P, tum Q formae $+A$, eritque ex prop. 1. $p \equiv q$ (mod. 2); at erit $p' \equiv p$ (mod. 2); quare etiam $p' \equiv q$ (mod. 2). Quod conuenit cum prop. 2. — Simili modo si P est formae $+A$, Q formae $-A$, erit $p \equiv q$ (mod. 2) ex prop. 2 quam modo demonstrauimus; hinc, ob $p' \equiv p$, erit $p' \equiv q$. Est itaque etiam prop. 5 demonstrata.

Eodem modo prop. 7 ex 3; prop. 8 vel ex 4 vel ex 7; prop. 9 ex 6; ex eademque prop. 10 deriuantur.

135. Per art. praec. propositiones art. 133 non quidem sunt demonstratae, sed tamen earum veritas a veritate theorematis fundamentalis quam aliquantisper supposuimus pendere ostensa est. At ex ipsa deductionis methodo manifestum est, illas valere pro numeris P, Q, si modo theorema fundamentale pro omnibus factoribus primis horum numerorum inter se comparatis locum habeat, etiamsi generaliter verum non sit. Nunc igitur ipsius theorematis fundamentalis demonstrationem aggrediamur. Cui praemittimus sequentem explicationem.

Theorema fundamentale vsque ad numerum aliquem M verum esse dicemus, si valet pro duobus numeris primis quibuscunque, quorum neuter ipsum M superat.