quinque etc.) implicare. Multitudo factorum formae $4n + 1$ indeterminata manet.

Prop. 9 ita demonstratur. Sit A productum e factoribus primis a', a'', a''' etc., b, b', b'' etc.; eritque factorum b, b', b'' multitudo par (possunt etiam nulli adesse, quod eodem redit). Iam si a est residuum ipsius A, erit residuum etiam omnium factorum a', a'', a''' etc. b, b', b'' etc. quare per propp. 1, 3 art. praec. singuli hi factores erunt residua ipsius a, adeoque etiam productum A. — A vero idem esse debet. — Quodsi vero — a est residuum ipsius A, eoque ipso omnium factorum a', a'' etc. b, b' etc.; singuli a', a'' etc erunt ipsius a residua, singuli b, b' etc. autem non residua. Sed quum posteriorum multitudo sit par, productum ex omnibus, *i. e.* A, ipsius a residuum erit, hincque etiam — A.

133. Inuestigationem adhuc generalius instituamus. Contemplemur duos numeros quoscunque impares inter se primos, signis quibuscunque affectos, P et Q. Concipiatur P sine respectu signi sui in factores suos primos resolutus, designeturque per p, quot inter hos reperiantur quorum non-residuum sit Q. Si vero aliquis numerus primus, cuius non-residuum est Q, pluries inter factores ipsius P occurrit, pluries etiam numerandus erit. Similiter sit q multitudo factorum primorum ipsius Q, quorum non-residuum est P. Tum numeri p, q certam relationem mutuam habebunt ab

indole numerorum P, Q pendentem. Scilicet si alter numerorum p, q est par vel impar, numerorum P, Q forma docebit, vtrum alter par sit vel impar. Haec relatio in sequenti tabula exhibetur.

Erunt p, q simul pares vel simul impares, quando numeri P, Q habent formas:

1. $+A, +A'$
2. $+A, -A'$
3. $+A, +B$
4. $+A, -B$
5. $-A, -A'$
6. $+B, -B'$

Contra numerorum p, q alter erit par, alter impar, quando numeri P, Q habent formas:

7. $-A, +B$
8. $-A, -B$
9. $+B, +B'$
10. $-B, -B'$.

Ex. Sint numeri propositi — 55 et + 1197, qui ad casum quartum erunt referendi. Est autem 1197 non-residuum vnius factoris primi ipsius 55, scilicet numeri 5, — 55 autem non-residuum trium factorum primorum ipsius 1197, scilicet numerorum 3, 3, 19.

Si P et Q numeros primos designant, propositiones hae abeunt in eas quas art. 131 tra-

didimus. Hic scilicet p et q maiores quam 1 fieri nequeunt, quare quando p ponitur esse par necessario erit $= 0$ i. e, Q erit residuum ipsius P, quando vero p est impar, Q ipsius P non-residuum erit. Et vice versa. Ita scriptis a, b loco ipsorum A, B, ex 8 sequitur, si $-a$ fuerit residuum vel non-residuum ipsius b, fore $-b$ non-residuum vel residuum ipsius a, quod cum 3 et 4 art. 131 conuenit.

Generaliter vero patet, Q residuum ipsius P esse non posse nisi fuerit $p = 0$; si igitur p impar, Q certo ipsius P non-residuum erit.

Hinc etiam propp. art. praec. sine difficultate deriuari possunt.

Ceterum mox patebit, hanc repraesentationem generalem plus esse quam speculationem sterilem, quum theorematis fundamentalis demonstratio completa absque ea vix perfici possit.

134. Aggrediamur nunc deductionem harum propositionum.

I. Concipiatur, vt ante, P in factores suos primos resolutus, signis neglectis, insuperque etiam Q in factores quomodocunque resoluatur, ita tamen vt signi ipsius Q ratio habeatur. Combinentur illi singuli cum singulis his. Tum si s designat multitudinem omnium combinationum, in quibus factor ipsius Q est non-residuum factoris ipsius P, p et s vel simul pares vel