Quando $Q > a$, substituatur loco ipsius Q ipsius residuum minimum positiuum secundum modulum a*). Hoc ad a eandem relationem habebit quam habet Q.

Porro resoluatur Q, siue numerus ipsius loco assumtus, in factores suos primos p, p', p'' etc., quibus adiungendus factor — 1, quando Q est negatiuus. Tum constat relationem ipsius Q ad a pendere a relationibus singulorum p, p', p'' etc. ad a. Scilicet si inter illos factores sunt $2m$ non-residua ipsius a erit QRa, si vero $2m + 1$, erit QNa. Facile autem perspicitur, si inter factores p, p', p'' etc., bini aut quaterni aut seni aut generaliter $2k$ aequales occurrant hos tuto eiici posse.

IV. Si inter factores p, p', p'' reperiuntur — 1 et 2, horum relatio ad a ex artt. 108, 112, 113, 114 inueniri potest. Reliquorum autem relatio ad a pendet a relatione ipsius a ad ipsos (*theor. fund.*, atque propp. art. 131). Sit p vnus ex ipsis, inuenieturque, (tractando numerus a, p eodem modo vt antea Q et a illis respectiue maiores) relationem ipsius a ad p aut per artt. 108—114 determinari posse (si scilicet residuum minimum ipsius a (mod. p) nullos factores primos impares habeat), aut insuper a relatione ipsius p ad numeros quosdam primos ipso p minores pendere. Idem valet de reliquis factoribus p', p'' etc. Facile

*) *Residuum* in signific. art. 4. — Plerumque praestat residuum *absolute* minimum accipere.

iam perspicitur per continuationem huius operationes tandem ad numeros peruentum iri quorum relationes per propp. artt. 108—114 determinari possint. Per exemplum haec clariora fient.

Ex. Quaeritur relatio numeri + 453 ad 1236. Est $1236 = 4.3.103$; $+453 R 4$ per II. 2 (*A*); $+453 R 3$ per II. 1. Superest igitur vt relatio ipsius + 453 ad 103 exploretur. Eadem autem erit quam habet + 41 ($\equiv 453$, mod. 103) ad 103; eadem ipsius + 103 ad 41 (*theor. fund.*), siue ipsius — 20 ad 41. At est $-20 R 41$; namque $-20 = -1.2.2.5$; $-1 R 41$, (art. 108); atque $+5 R 41$ ideo quod $41 \equiv 1$ adeoque ipsius 5 residuum est (theor. fund.). Hinc sequitur $+453 R 103$, hincque tandem $+453 R 1236$. Est autem reuera $453 \equiv 297^2$ (mod. 1236).

147. Proposito numero quocunque *A*, *formulae* certae exhiberi possunt, sub quibus omnes numeri ad *A* primi quorum residuum est *A* continentur, siue omnes qui esse possunt *diuisores* numerorum formae $xx - A$ (designante xx quadratum indeterminatum) *). Sed breuitatis gratia ad eos tantum diuisores respiciemus, qui sunt impares atque ad *A* primi, quum ad hos casus reliqui facile reduci possint.

*) Huiusmodi numeros simpliciter *diuisores ipsius* $xx - A$ dicemus vnde sponte patet quid sint *non-diuisores*.

Sit primo A aut numerus primus positiuus formae $4n + 1$, aut negatiuus formae $4n - 1$. Tum secundum theorema fundamentale omnes numeri primi, qui, positiue sumti, sunt residua ipsius A, erunt diuisores ipsius $xx - A$: omnes autem numeri primi (excepto numero 2 qui semper est diuisor) qui ipsius A sunt non residua erunt non diuisores ipsius $xx - A$. Sint omnia residua ipsius A ipso A minora (exclusa cifra), r, r' r'' etc. omnia non-residua vero n, n' n'' etc. Tum quiuis numerus primus, in aliqua formarum $Ak + r$, $Ak + r'$, $Ak + r''$ etc. contentus, erit diuisor ipsius $xx - A$, quiuis autem primus in aliqua formarum $Ak + n$, $Ak + n'$ etc. contentus non-diuisor erit, designante k numerum integrum indeterminatum. Illas formas dicimus *formas diuisorum ipsius* $xx - A$, has vero *formas non-diuisorum*. Vtrorumque multitudo erit $\frac{1}{2}(A - 1)$. Porro si B est numerus compositus impar atque ARB, omnes factores primi ipsius B in aliqua formarum primorum continentur adeoque etiam B. Quare *quiuis* numerus impar in forma non-diuisorum contentus, erit non-diuisor formae $xx - A$. Sed hoc theorema conuertere non licet; nam si B est non-diuisor compositus impar formae $xx - A$, inter factores primos ipsius B aliqui non-diuisores erunt, quorum multitudo si est *par*, B nihilominus in aliqua forma diuisorum reperietur, V. art. 99.

Ex. Hoc modo pro $A = -11$ formae diuisorum ipsius $xx + 11$ inueniuntur hae: