erit producto e multitudinibus valorum ipsorum A, B, C etc. quas determinare in art. praec. docuimus. — Porro manifestum est, si vnus valor expressionis $\sqrt{n}$ (mod. m) siue ipsius N fuerit notus, hunc simul fore valorem omnium A, B, C etc.; et quum hinc per art. praec. omnes reliqui valores harum quantitatum deduci possint, facile sequitur, ex vno valore ipsius N omnes reliquos obtineri posse.

Ex. Sit modulus 315 cuius residuum an non-residuum sit 46, quaeritur. Diuisores primi numeri 315 sunt 3, 5, 7, atque numerus 46 residuum cuiusuis eorum quare etiam ipsius 315 erit residuum. Porro, quia $46 \equiv 1$, et $\equiv 64$ (mod. 9); $\equiv 1$ et $\equiv 16$ (mod. 5); $\equiv 4$ et $\equiv 25$ (mod. 7), inueniuntur radices quadratorum, quibus 46 secundum modulum 315 congruus, 19, 26, 44, 89, 226, 271, 289, 296.

106. Ex praecedentibus colligitur, si tantummodo semper dignosci possit vtrum *numerus primus* datus numeri *primi dati* residuum sit an non-residuum, omnes reliquos casus ad hunc reduci posse. Pro illo itaque casu criteria certa omni studio nobis erunt indaganda. Antequam em hanc perquisitionem aggrediamur, criterium quoddam exhibemus ex Sect. petitum quod quamuis in praxi nullum fere vsum habeat tamen propter simplicitatem atque generalitatem memoratu dignum est.

Numerus quicunque A per numerum primum $2m+1$ non diuisibilis, huius primi residuum est vel non-residuum, prout $A^m \equiv +1$ vel $\equiv -1$ (mod. $2m+1$).

Sit enim pro modulo $2m+1$ in systemate quocunque numeri A index, a, eritque a par, quando A est residuum ipsius $2m+1$, impar vero quando A non-residuum. At numeri A^m index erit ma, i. e. $\equiv 0$ vel $\equiv m$ (mod. $2m$), prout a par vel impar. Hinc denique A^n in priori casu erit $\equiv +1$, in posteriori vero $\equiv -1$ (mod. $2m+1$). V. artt. 57, 62.

Ex. 3 ipsius 13 est residuum quia $3^6 \equiv 1$ (mod. 13), 2 vero ipsius 13 non-residuum, quoniam $2^6 \equiv -1$ (mod. 13).

At quoties numeri examinandi mediocriter sunt magni, hoc criterium ob calculi immensitatem prorsus inuitile erit.

107. Facillimum quidem est, proposito modulo, omnes assignare numeros, qui ipsius residua sunt vel non residua. Scilicet si ille numerus ponitur $= m$, determinari debent quadrata, quorum radices semissem ipsius m non superant, siue etiam numeri his quadratis secundum m congrui (ad praxin methodi adhuc expeditiores dantur), tuncque omnes numeri horum alicui secundum m congrui, erunt residua ipsius m, omnes autem numeri nulli istorum congrui erunt non-residua. — At quaestio inuersa, *proposito numero aliquo, assignare omnes numeros quorum ille sit residuum vel non-residuum*, multo altioris est indaginis. Hoc itaque problema, a cuius solutione illud quod in art. praec. nobis proposuimus pendet, in sequentibus perscrutabimur, a casibus simplicissimis inchoantes.

108. THEOREMA. *Omnium numerorum formae $4n+1$, -1 est residuum quadraticum, omnium vero numerorum primorum formae $4n+3$, non-residuum.*

Ex. -1 est residuum numerorum 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc., e quadratis numerorum 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22 etc. respetiue oriundum; contra non-residuum est numerorum 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 etc.

Mentionem huius theor. iam in art. 64 fecimus. Demonstratio vero facile ex art. 106 petitur. Etenim pro numero primo formae $4n+1$ est $(-1)^{2n} \equiv 1$, pro numero autem formae $4n+3$ habetur $(-1)^{2n+1} \equiv -1$. Conuenit haec demonstratio cum ea quam *l. c.* tradidimus. Sed propter theorematis elegantiam atque vtilitatem non superfluum erit, alio adhuc modo idem ostendisse.

109. Designemus complexum omnium residuorum numeri primi p, quae ipso p sunt minora, excluso residuo o, per literam C, et quoniam horum residuorum multitudo semper $= \frac{p-1}{2}$, manifestum est, eam fore parem, quoties p sit formae $4n+1$, imparem vero, quoties p sit formae $4n+3$. Dicantur, ad instar art. 77, vbi de numeris in genere agebatur, *residua socia* talia, quorum productum $\equiv 1$ (mod. p); manifesto enim si r est residuum, etiam $\frac{1}{r}$ (mod. p) residuum erit. Et quoniam idem residuum plura socia inter residua C habere nequit, patet omnia residua C in classes distribui posse,