computentur, horum complexum continere numeros 1, p, p', p'' etc. atque omnia producta e binis, ternis etc. horum numerorum. *Hoc itaque modo e valoribus illius expressionis numeros p, p', p'' etc. eruere licebit.*

Ceterum quum methodus art. 327 singulos hosce valores ad valores expressionum huius formae $\frac{m}{n}$ (mod. M) reducat, ita vt denominator n ad M primus sit: ad institutum praesens ne necessarium quidem est, has ipsas computare. Nam diu. comm. max. numeri M cum differentia inter R et R' qui cum $\frac{m}{n}$, $\frac{m'}{n'}$ conueniunt manifesto etiam erit diu. comm. max. ipsorum M et $nn'(R - R')$, siue ipsorum M et $mn' - m'n$, quippe cui $nn'(R - R')$ secundum modulum M est congruus.

334. Applicatio obseruationum praecc. ad problema de quo agimus duplici modo institui potest; prior non solum decidet, vtrum numerus propositus M primus sit an compositus, sed in hoc casu etiam factores ipsos suppeditat; posterior autem eatenus praestat, quod plerumque calculum expeditiorem permittit, sed factores ipsos numerorum compositorum, quos quoque a primis protinus distinguit, interdum non profert, nisi pluries repetatur.

I. Inuestigetur numerus negatiuus $-D$, qui sit residuum quadraticum ipsius M, ad quem finem methodi in art. 332 sub I et II traditae adhiberi poterunt. Per se quidem arbitrarium

est, quidnam residuum eligatur, neque hic vt in methodo praec. opus est, vt D sit numerus paruus; sed calculus eo breuior erit, quo minor est multitudo classium formarum binariarum in singulis generibus pr. pr. det. $-D$ contentarum; quamobrem imprimis talia residua qui inter 65 numeros art. 303 continentur, si qui se offerunt, opportuna erunt. Ita pro $M = 997331$ ex omnibus residuis negatiuis supra erutis hoc -102 maxime idoneum esset. Eruantur omnes valores diuersi expr. $\sqrt{-D}$ (mod. M); quodsi duo tantum proueniunt (oppositi), M certo erit vel numerus primus vel numeri primi potestas; si plures, puta 2^{μ}, M compositus erit ex μ numeris primis, aut primorum potestatibus, diuersis, qui factores per methodum art. praec. erui poterunt. Vtrum vero hi factores numeri primi sint an primorum potestates, tum per se facillimum erit dignoscere; tum etiam via ipsa per quam valores expr. $\sqrt{-D}$ inueniuntur, omnes numeros primos, quorum potestas aliqua ipsum M metitur, sponte indicat; scilicet si M diuisibilis est per quadratum numeri primi π, ille calculus certo etiam vnam pluresue repraesentationes tales numeri M, $M = amm + 2bmn + cnn$, produxerit, in quibus diuisor comm. max. numerorum m, n est π (et quidem ideo, quod in hoc casu $-D$ etiam est residuum ipsius $\frac{M}{\pi\pi}$). Quando vero nulla repraesentatio prodiit, in qua m, et n diuisorem communem habent, hoc certum indicium est, M per nullum quadratum diuisibilem esse adeoque omnes p, p', p'' etc. numeros primos.

Ex. Per methodum supra traditam inueniuntur quatuor valores expr. $\sqrt{} - 102$ (mod. 997331) cum valoribus harum $\pm \frac{1664}{113}$, $\pm \frac{2824}{3}$ conuenientes; diuisores communes maximi 997331 cum his $3.1664 - 113.2824$ et $3.1664 + 113.2824$ siue cum 314120 et 324104 eruuntur hi 7853 et 127, vnde $997331 = 127.7853$, vt supra.

II. Accipiatur aliquis numerus negatiuus $-D$ talis, vt M contentus sit in forma diuisorum ipsius $xx + D$; per se arbitrarium est, quis huiusmodi numerus eligatur, sed commoditatis caussa imprimis videndum est, vt multitudo classium in generibus det. $-D$ sit quam maxime parua. Ceterum inuentio talis numeri nulli difficultati obnoxia est, si tentando adeatur; nam plerumque inter multitudinem considerabilem numerorum tentatorum pro totidem fere M in forma diuisorum continetur, ac in forma non diuisorum. Quare maxime e re erit, tentamen a 65 numeris art. 303 inchoare (et quidem a maximis), et si eueniret, vt nullus idoneus esset (quod tamen generaliter loquendo inter 16384 casus semel tantum accidit), ad alios progredi, vbi classes binae in singulis generibus continentur. — Tunc inuestigentur valores expr. $\sqrt{} - D$ (mod. M), et si qui inueniuntur, factores ipsius M prorsus eodem modo inde deducantur vt supra; si vero nulli valores prodeunt, adeoque $-D$ est non residuum ipsius M, certo M neque numerus primus neque numeri primi potestas esse poterit. Quodsi in hoc casu factores ipsi desiderantur, vel eandem operationem repetere oportet, alios valores pro D accipiendo, vel ad methodum aliam confugere.