les); hinc vero facile perspicitur, pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. omnino eosdem numeros prouenire debere, aliter tantum dispositos. Similiter si post applicationem excludentium p et pp ponitur $E = p^3$, sufficiet pro a, b, c etc. accipere producta singulorum nonresiduorum ipsius p in pp, vnde pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. prouenient vel iidem numeri, vel producta ipsius pp in singula residua ipsius p praeter 0, prout m est residuum vel non residuum ipsius p. Generaliter accipiendo pro E potestatem quamcunque numeri primi puta p^μ, omnibus inferioribus iam applicatis, pro $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. prodibunt producta ipsius $p^{\mu-1}$ vel in omnes numeros ipso p minores, 0 semper excepto, quando μ par, vel in omnia non residua ipsius p minora quam p, quando μ impar atque mRp, vel in omnia residua, quando mNp. — Si $E = 4$, adeoque $a = 2$, $b = 3$, pro $\mathfrak{A}$, $\mathfrak{B}$ habemus vel 2 et 3 vel 2 et 1, prout $m \equiv 1$ aut $\equiv 3 \pmod 4$. Si post vsum excl. 4 statuitur $E = 8$, habemus $\alpha = 5$, vnde $\mathfrak{A}$ fit 5, 7, 1, 3, prout $m \equiv 1, 3, 5, 7 \pmod 8$. Generaliter autem, si E est potestas altior quaecunque binarii puta 2^μ, inferioribus iam applicatis, poni debet $a = 2^{\mu-1}$, $b = 3.2^{\mu-2}$, quando μ est par, vnde fit $\mathfrak{A} = 2^{\mu-1}$, $\mathfrak{C} = 3.2^{\mu-2}$ vel $= 2^{\mu-2}$, prout $m \equiv 1$ vel $\equiv 3$, quando vero μ est impar, ponendum est $a = 5.2^{\mu-3}$, vnde $\mathfrak{A}$ aequalis fit producto numeri $2^{\mu-3}$ in 5, 7, 1, vel 3, prout $m \equiv 1, 3, 5$ vel 7 (mod. 8).

Ceterum periti facile comminiscentur apparatum, per quem valores inutiles ipsius y *mechanice* ex Ω eiici possint, postquam pro tot exclu-

dentibus quot necessarii videntur numeri α, ε, γ etc. sunt computati; sed de hac re sicut de aliis artificiis laborem contrahendi hic agere non licet.

323. Omnes repraesentationes numeri dati A per formam binariam $mxx + nyy$, siue solutiones aequationis indeterminatae $mxx + nyy = A$, in sectione V methodo generali inuenire docuimus, cuius breuitas quoque nihil desiderandum relinquere videtur, si omnes valores expr. $\sqrt{-mn}$ secundum modulum A ipsum, et per suos factores quadratos diuisum, iam habentur; hic autem pro eo casu, vbi mn est positiuus, solutionem explicabimus, directa multo expeditiorem, si ad hanc illos valores antea computare oportet. Supponemus autem, numeros m, n et A esse positiuos atque inter se primos, quum casus reliqui ad hunc facile possint reduci. Manifesto quoque sufficit, valores positiuos ipsorum x, y eruere, quum reliqui inde per solam signorum mutationem deducantur.

Perspicuum est, x ita comparatum esse debere, vt $\frac{A - mxx}{n}$, pro quo scribemus V, positiuus, integer, et quadratus euadat. Conditio prima requirit, vt x non sit maior quam $\sqrt{\frac{A}{m}}$; secunda iam per se locum habet quando $n = 1$, alioquin requirit, vt valor expr. $\frac{A}{m}$ (mod. n) sit residuum quadraticum ipsius n, designandoque omnes valores diuersos expr. $\sqrt{\frac{A}{m}}$ (mod. n) per $\pm r$, $\pm r'$ etc., x sub aliqua formarum nt

$+ r$, $nt - r$, $nt + r'$ etc. contentus esse debebit. Simplicissimum itaque foret, omnes numeros harum formarum infra limitem $\sqrt{\frac{A}{m}}$, quorum complexum per Ω exprimemus, pro x substituere, eosque solos retinere, pro quibus V fit quadratum. Hoc tentamen, quantum lubeat, contrahere, in art. sq. docebimus.

324. Methodus exclusionum, per quam hoc efficiemus, perinde ac in disqu. praec. in eo consistit, vt plures numeros, etiam hic *excludentes* vocandos, ad lubitum accipiamus, pro quibusnam valoribus ipsius x valor ipsius V fiat non residuum qu. horum excludentium inuestigemus, talesque x ex Ω eiiciamus. Per ratiocinia iis quae in art. 321 exposuimus omnino analoga apparet, tales tantum excludentes adhibendos esse, qui sint numeri primi aut numerorum primorum potestates, et pro excludente posterioris generis ea tantum ipsius non residua a valoribus ipsius V arcenda, quae sint residua omnium potestatum inferiorum eiusdem numeri primi, siquidem exclusio cum his iam est instituta.

Sit itaque excludens $E = p^\mu$ (includendo etiam eum casum vbi $\mu = 1$), vbi p est numerus primus ipsum m non metiens, supponamusque *) p^ν esse summam potestatem eiusdem numeri primi per quam n sit diuisibilis. Sint a, b,

*) Breuitatis caussa duos casus, in quibus n per p est diuisibilis ac non diuisibilis, simul complectimur; in posteriori $\nu = 0$ ponere oportet.