ne erui possunt, et vel cum omnibus non-residuis, vel cum omnibus residuis ipsius $p$ (praeter 0) conuenient, prout valor expr. $-\frac{m}{n}$ (mod. $p$), siue (quod hic eodem redit) numerus $-mn$ est residuum vel non residuum ipsius $p$. Ita in *ex.* II art. praec. pro $E = 17$ fit $k = 7$; $-mn = -1365 \equiv 12$ est non residuum ipsius 17; hinc numeri $\mathfrak{A}$, $\mathfrak{B}$ etc. erunt 1, 2, 4, 8, 9, 13, 15, 16 adeoque numeri $\alpha$, $\mathfrak{C}$ etc. 8, 9, 11, 15, 16, 3, 5, 6; ex his residua sunt 8, 9, 15, 16, vnde $\pm h$, $h'$ etc. fiunt $\pm 5, 3, 7, 4$. — Quibus saepius occasio est huiusmodi problemata soluendi, commoditati suae eximie consulent, si pro pluribus numeris primis $p$, valores ipsorum $h$, $h'$ etc. singulis valoribus ipsorum $k$, (1, 2, 3...$p - 1$) respondentes, in duplici suppositione (puta vbi $-mn$ est residuum et vbi non-residuum ipsius $p$) computent. Ceterum obseruamus adhuc, multitudinem numerorum $h$, $-h$, $h'$ etc. semper esse $\frac{1}{2}(p-1)$, quando vterque numerus $k$ et $-mn$ sit residuum vel vterque non residuum ipsius $p$; $\frac{1}{2}(p-3)$, quando prior *R.*, posterior *N.R.*; $\frac{1}{2}(p+1)$, quando prior *NR.*, posterior *R.*; sed demonstrationem huius theorematis ne nimis prolixi fiamus supprimere debemus.

Quod autem, *secundo*, eos casus attinet, vbi $E$ est numerus primus ipsum $n$ metiens, aut potestas numeri primi (imparis) ipsum $n$ metientis seu non metientis, hi adhuc expeditius tractari possunt. Omnes hos casus simul complectemur, omnibusqus art. 324 signis retentis ponemus $n = n'p'$, ita vt $n'$ per $p$ non sit di-

uisibilis. Numeri $a$, $b$, $c$ etc. erunt producta numeri $p^{\mu-1}$ vel in omnes numeros ipso $p$ minores (praeter o), vel in omnia non residua ipsius $p$ infra $p$, prout $\mu$ est par vel impar; exprimantur indefinite per $up^{\mu-1}$. Sit $k$ valor expr. $\frac{A}{m}$ (mod. $p^{\mu+\nu}$), eritque per $p$ non diuisibilis, quia eadem proprietas in $A$ supponitur; porro patet, omnes $\alpha$, $\beta$, $\gamma$ etc. ipsi $k$ sec. mod. $p$ congruos fieri, adeoque $p^{\mu}$ nihil ex $\Omega$ excludere, si $kNp$; si vero $kRp$ adeoque etiam $kRp^{\mu+\nu}$, sit $r$ valor expr. $\sqrt{k}$ (mod. $p^{\mu+\nu}$), qui per $p$ non erit diuisibilis, atque $e$ valor huius $-\frac{n'}{2mr}$ (mod. $p$), eritque $\alpha \equiv rr + 2erap$ (mod. $p^{\mu+\nu}$), vnde facile colligitur, $\alpha$ esse residuum ipsius $p^{\mu+\nu}$, atque valores expr. $\sqrt{\alpha}$ (mod. $p^{\mu+\nu}$) fieri $\pm (r + eap^{\mu})$; hinc omnes $h$, $h'$, $h''$ etc. exprimentur per $r + ep^{\mu+\nu-1}$. Denique nullo negotio hinc concluditur, numeros $h$, $h'$, $h''$ etc. oriri ex additione numeri $r$ cum productis numeri $p^{\mu+\nu-1}$ *vel* in omnes numeros infra $p$ (praeter o), puta quando $\mu$ par; *vel* in omnia non residua ipsius $p$ infra hunc limitem, quando $\mu$ impar atque $eRp$ siue quod hic eodem redit quando $-2mrn'Rp$; *vel* in omnia residua (praeter o), quando $\mu$ impar atque $-2mrn'Np$.

Ceterum simulac pro singulis excludentibus, quos applicare placet, numeri $h$, $h'$ etc. sunt eruti, exclusionem ipsam etiam per operationes mechanicas perficere licebit, quales quisque harum rerum peritus facile proprio marte excogitare poterit, si operae pretium esse videbitur.

Tandem obseruare debemus, quamuis aequationem $axx + 2bxy + cyy = M$, in qua $bb - ac$ negatiuus $= -D$, facile ad eam formam quam in praecc. considerauimus reduci posse. Designando enim diuisorem communem maximum numerorum $a$, $b$ per $m$, et ponendo $a = ma'$, $b = mb'$, $\frac{D}{m} = a'c - mb'b' = n$, $a'x + b'y = x'$, aequ. illa manifesto aequiualet huic $mx'x' + nyy = a'M$, quae per praecepta supra tradita solui poterit. Ex huius autem solutionibus eae tantum erunt retinendae, in quibus $x' - b'y$ per $a'$ fit diuisibilis, siue vnde $x$ valores integros nanciscitur.

327. Quemadmodum solutio directa aequationis $axx + 2bxy + cyy = M$ in sect. V contenta valores expr. $\sqrt{(bb - ac)}$ (mod. $M$) notos supponit: ita vice versa pro eo casu, vbi $bb - ac$ est negatiuus, solutio indirecta in praecc. exposita methodum expeditissimam subministrat, illos valores eruendi, quae, praesertim pro valore permagno ipsius $M$, methodo art. 322 sqq. longe est praeferenda. Supponemus autem, $M$ esse numerum primum, aut saltem ipsius factores, si compositus esset, adhuc incognitos; si enim constaret, numerum primum $p$ ipsum $M$ metiri, atque esse $M = p^{\mu}M'$, ita vt $M'$ factorem $p$ non amplius implicet, longe commodius foret, valores expr. $\sqrt{(bb - ac)}$ pro modulis $p^{\mu}$ et $M'$ sigillatim explorare (priores ex valoribus secundum modulum $p$, art. 101), valoresque sec. mod. $M$ ex horum combinatione deducere (art. 105).