

c etc. non residua quadratica ipsius  $E$  (omnia, quando  $\mu = 1$ ; necessaria siue ea quae sunt residua potestatum inferiorum, quando  $\mu > 1$ ). Computentur radices congruentiarum  $mz \equiv A - na$ ,  $mz \equiv A - nb$ ,  $mz \equiv A - nc$  etc. (mod.  $Ep^v \equiv p^{\mu+v}$ ), quae sint  $\alpha$ ,  $\epsilon$ ,  $\gamma$  etc., patetque facile, si pro quo valore ipsius  $x$  fiat  $xx \equiv \alpha$  (mod.  $Ep^v$ ), valorem respondentem ipsius  $V$  fieri  $\equiv \alpha$  (mod.  $E$ ) siue non residuum ipsius  $E$ , similiterque de numeris reliquis  $\epsilon$ ,  $\gamma$  etc.; aequa facile vice versa perspicitur, si quis valor ipsius  $x$  producat  $V \equiv \alpha$  (mod.  $E$ ), pro eodem fieri  $xx \equiv \alpha$  (mod.  $Ep^v$ ), adeoque omnes valores ipsius  $x$ , pro quibus  $xx$  nulli numerorum  $\alpha$ ,  $\epsilon$ ,  $\gamma$  etc. sec. mod.  $Ep^v$  congruus sit, tales valores ipsius  $V$  producere, qui nulli numerorum  $a$ ,  $b$ ,  $c$  etc. sec. mod.  $E$  sint congrui. Eligantur iam e numeris  $\alpha$ ,  $\epsilon$ ,  $\gamma$  etc. omnia residua quadratica ipsius  $Ep^v$ , quae sint  $g$ ,  $g'$ ,  $g''$  etc., computentur valores expressionum  $\sqrt{g}$ ,  $\sqrt{g'}$ ,  $\sqrt{g''}$  etc. (mod.  $Ep^v$ ), ponamusque hinc prodire  $\pm h$ ,  $\pm h'$ ,  $\pm h''$  etc. His ita factis manifestum est, omnes numeros formarum  $Ep^v t$   $\pm h$ ,  $Ep^v t \pm h'$ ,  $Ep^v t \pm h''$  etc. ex  $\Omega$  tuto eiici posse, nullaque valori ipsius  $x$  in  $\Omega$  post hanc exclusionem remanenti valorem ipsius  $V$  sub formis  $Eu + a$ ,  $Eu + b$ ,  $Eu + c$  etc. contentum respondere posse. Ceterum manifestum est, tales valores ipsius  $V$  iam per se e nullo valore ipsius  $x$  prodire posse, quando inter numeros  $\alpha$ ,  $\epsilon$ ,  $\gamma$  etc. nulla residua quæ ipsius  $Ep^v$  inueniantur, adeoque in hoc casu numerum  $E$  tamquam excludentem applicari non posse. — Huiusmodi excludentes, quot placet, adhiberi;

atque sic numeri in  $\Omega$  ad libitum diminui possunt.

Videamus iam, annō etiam numeros primos ipsum  $m$  metientes, taliumue numerorum potestates tamquam excludentes adhibere liceat. Sit  $B$  valor expr.  $\frac{A}{n}$  (mod.  $m$ ), patetque,  $V$  semper ipsi  $B$  secundum mod.  $m$  congruum fieri, quicunque valor pro  $x$  accipiatur, adeoque ad possibilitatem aequ. prop. necessario requiri, ut  $B$  sit residuum quadraticum ipsius  $m$ . Designante itaque  $p$  diuisorem quemcunque primum imparem ipsius  $m$ , qui per hyp. ipsos  $n$  et  $A$ , adeoque etiam ipsum  $B$  non metietur, pro valore quocunque ipsius  $x$  erit  $V$  residuum ipsius  $p$ ; adeoque etiam cuiuscunque potestatis ipsius  $p$ ; quamobrem  $p$  ipsiusque potestates nequeunt excludentium loco haberi. — Prorsus simili ratione quando  $m$  per 8 est diuisibilis ad, aequ. prop. possibilitatem necessario requiritur ut sit  $B \equiv 1$  (mod. 8), vnde etiam  $V$  pro valore quocunque ipsius  $x$  fiet  $\equiv 1$  (mod. 8), et proin binarii potestates ad exclusionem non idoneae. — Quando autem  $m$  per 4 neque vero per 8 est diuisibilis, ex simili ratione esse debebit  $B \equiv 1$  (mod. 4), adeoque valor expr.  $\frac{A}{n}$  (mod. 8) vel 1 vel 5; designetur per  $C$ . Nullo negotio perspicietur, pro valore pari ipsius  $x$  hic fieri  $V \equiv C$ ; pro impari,  $V \equiv C + 4$  (mod. 8); vnde patet, valores pares reiiciendos esse, quando  $C = 5$ ; impares, quando  $C = 1$ . — Denique quando  $m$  per 2, neque vero per 4 est diuisibilis, sit vt an-

te  $C$  valor expr.  $\frac{A}{n}$  (mod. 8), qui erit 1, 3, 5, vel 7; atque  $D$  valor huius  $\frac{\frac{1}{2}m}{n}$  (mod. 4), qui erit 1 vel 3. Iam quum valor ipsius  $V$  manifesto semper fiat  $\equiv C - 2Dxx$  (mod. 8), adeoque pro  $x$  pari  $\equiv C$ , pro impari  $\equiv C - 2D$ , facile hinc colligitur, reiiciendos esse omnes valores impares ipsius  $x$ , quando  $C \equiv 1$ ; omnes pares, quando  $C = 3$  et  $D = 1$ , aut  $C = 7$  et  $D = 3$ , atque valores remanentes omnes producere  $V \equiv 1$  (mod. 8) siue residuum cuiusvis potestatis binarii; in casibus reliquis autem, puta quando  $C = 5$ , aut  $C = 3$  et  $D = 3$ , aut  $C = 7$  et  $D = 1$ , fiet  $V \equiv 3, 5$  vel 7 (mod. 8), siue  $x$  accipiatur par siue impar, vnde liquet, in his casibus aequationem prop. solutionem omnino non admittere.

Ceterum quum prorsus simili modo, vt hic valorem ipsius  $x$  per exclusiones inuenire docuimus, etiam, mutatis mutandis, valorem ipsius  $y$  elicere possimus, methodum exclusionis ad problematis propositi solutionem duobus semper modis applicare licebit (nisi  $m = n = 1$ , vbi coincidunt), e quibus si plerumque est praefrendus, pro quo  $\Omega$  terminorum multitudinem minorem continet, quod facile a priori aestimari poterit. — Denique vix necesse erit obseruare, si post aliquot exclusiones *omnes* numeri ex  $\Omega$  abierint, hoc vt certum indicium impossibilitatis aequationis propositae esse considerandum.

325. Ex. Proposita sit aequatio  $3xx + 455yy = 10857362$ , quam dupli modo solue-