

quae differens erit a classe  $C$ , nisi haec est anceps. Hinc sequitur, quando non omnes classes in  $G$  ancipites sint, e reliquis semisseim tantum considerare oportere, puta e binis oppositis quibusque vnam, alteram negligendo, e qua valores iis, quos prior suppeditauit, oppositos resultare iam absque calculo praeuidere licet. Quando autem  $C$  est anceps, ambo valores  $r$  et  $-r$  simul inde emergent; puta, si ex  $C$  classis anceps  $axx + 2bxy + cyy$  electa est, atque valor  $r$  prodidit e repr.  $x = m, y = n$ , valor  $-r$  prodidit ex hac  $x = -m - \frac{2bn}{a}, y = n$ .

V. Pro eo casu vbi  $D = 1$ , vna tantum classis omnino datur, e qua formam  $xx + yy$  electam esse supponere licebit. Quodsi valor  $r$  ex repraesentatione  $x = m, y = n$  prouenit, idem ex his prodibit  $x = -m, y = -n; x = n, y = -m; x = -n, y = m$ , oppositusque  $-r$  ex his  $x = m, y = -n; x = m, y = n; x = -n, y = -m$ ; quare ex his octo repr., quae vnicam discriptionem constituunt, vna sufficit, si modo valori inde resultanti oppositum associemus.

VI. Valor expr.  $\sqrt{-D}$  (mod.  $M$ ), ad quem repr. haec  $M = amm + 2bmn + cnn$  pertinet, per art. 155 est  $\mu(mb + nc) - \nu(ma + nb)$  siue numerus quicunque huic secundum  $M$  congruus, ipsis  $\mu, \nu$  ita acceptis ut fiat  $\mu m + \nu n = 1$ . Designando itaque talem valorem per  $v$ , erit  $mv \equiv \mu m(mb + nc) - \nu(M - mn) \equiv$

$nnc \equiv (m + n)(mb + nc) \equiv mb + nc$  (mod.  $M$ ). Hinc patet,  $v$  esse valorem expr.  $\frac{mb+nc}{m}$  (mod.  $M$ ); similique modo inuenitur,  $v$  esse valorem expr.  $-\frac{ma+nb}{n}$  (mod.  $M$ ). Hae formulae saepenumero ei ex qua deductae fuerunt praferendae sunt.

328. *Exempla.* I. Quaeruntur omnes valores expr.  $\sqrt{-1365}$  (mod.  $5428681 = M$ ); numerus  $M$  hic est  $\equiv 1, 1, 1, 6, 11$  (mod.  $4, 3, 5, 7, 13$ ) adeoque sub forma diuisorum ipsorum  $xx + 1, xx + 3, xx - 5$ , et sub forma non diuisorum ipsorum  $xx + 7, xx - 13$ , et proin sub forma diuisorum ipsius  $xx + 1365$  contentus; characterque generis in quo classes  $\mathfrak{G}$  reperientur erit  $1, 4; R_3; R_5; N_7; N_{13}$ . In hoc genere vna classis continetur, e qua eligimus formam  $6xx + 6xy + 229yy$ ; vt omnes repraesentationes numeri  $M$  per hanc inueniantur, ponemus  $2x + y = x'$ , vnde fieri debet  $3x'x' + 455yy = 2M$ . Haec aequatio quatuor solutiones admittit in quibus  $y$  est positius, puta  $y = 127, x' = \pm 1083, y = 119, x' = \pm 1213$ . Hinc prodeunt quatuor solutiones aequ.  $6xx + 6xy + 229yy = M$ , in quibus  $y$  positius,

$x$	478	-605	547	-666
$y$	127	127	119	119

Solutio prima dat pro  $v$  valorem expr.  $\frac{30517}{478}$  si-

ue —  $\frac{3249}{127}$  (mod.  $M$ ), vnde inuenitur 2350978;  
 secunda producit valorem oppositum — 2350978;  
 tertia hunc 2600262, quarta oppositum —  
 2600262.

II. Si quaerendi sunt valores expr.  $\sqrt{-286}$  (mod.  $4272943 = M$ ), character generis in quo classes  $G$  contentae sunt, inuenitur 1 et 7, 8;  $R_{11}$ ;  $R_{13}$ ; quare erit genus principale, in quo tres classes continentur, per formas (1, 0, 286), (14, 6, 23), (14, — 6, 23) exhibatae; ex his tertiam, vtpote secundae oppositam negligere licet. Per formam  $xx + 286yy$  duae representationes numeri  $M$  inueniuntur, in quibus  $y$  positius, puta  $y = 103$ ,  $x = \pm 1113$ , vnde prodeunt valores expr. propositae hi 1493445, — 1493445. Per formam (14, 6, 23) autem  $M$  non represeñabilis inuenitur, vnde concluditur, praeter duos valores inuentos alios non dari.

III. Proposita expr.  $\sqrt{-70}$  (mod. 997331), classes  $G$  contentae esse debebunt in genere cuius character 3 et 5, 8;  $R_5$ ;  $N_7$ ; in hoc vnica classis reperitur cuius forma represeñans haec (5, 0, 14). At calculo instituto inuenitur, numerum 997331 per formam (5, 0, 14) non esse represeñabilem, quamobrem — 70 necessario erit non residuum qu. illius numeri.

329. Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resoluendi, ad grauissima ac vtilissima toti-