

Quaerendi sint itaque omnes valores expr.  $\sqrt{-D} \pmod{M}$ , vbi  $D$  et  $M$  positiui supponuntur, atque  $M$  sub forma diuisorum ipsius  $xx + D$  contentus (art. 147 sqq.), alioquin enim a priori constaret, nullos numeros expressioni propositae satisfacere posse. Sint valores quaesiti, e quibus bini semper oppositi erunt,  $\pm r, \pm r', \pm r''$  etc., atque  $D + rr = Mh, D + r'r' = Mh', D + r''r'' = Mh''$  etc.; porro designentur classes ad quas formae  $(M, r, h), (M, -r, h), (M, r', h), (M, -r', h), (M, r'', h), (M, -r'', h)$  etc. pertinent, resp. per  $\mathfrak{C}, -\mathfrak{C}, \mathfrak{C}', -\mathfrak{C}', \mathfrak{C}'', -\mathfrak{C}''$  etc., ipsarumque complexus per  $\mathfrak{G}$ . Hae classes quidem, generaliter loquendo, tamquam incognitae sunt spectandae; attamen perspicuum est, *primo*, omnes esse positiuas atque proprie primitiuas, *secundo* omnes ad idem genus pertinere, cuius *character* ex indole numeri  $M$ , i. e. ex ipsius relationibus ad singulos diuisores primos ipsius  $D$  (insuperque ad 4 aut 8 quando hae sunt necessariae) facile cognosci possit (art. 230). Quum suppositum sit,  $M$  contineri sub forma diuisorum ipsius  $xx + D$ , a priori certi esse possumus, huic characteri necessario genus pos. pr. pr. formarum determ. —  $D$  respondere, etiamsi forsan expressioni  $\sqrt{-D} \pmod{M}$  satisfieri nequeat; quum itaque hoc genus sit notum, omnes classes in ipso contentae erui poterunt, quae sint  $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$  etc., atque ipsarum complexus  $\mathfrak{G}$ . Patet igitur, singulas classes  $\mathfrak{C}, -\mathfrak{C}$  etc. cum aliqua classe in  $\mathfrak{G}$  identicas esse debere; fieri potest quoque, vt plures classes in  $\mathfrak{G}$  inter se, adeoque cum eadem in  $\mathfrak{G}$  identicae sint, et quando  $\mathfrak{G}$  vnicam

classem continet, certo omnes in  $\mathfrak{G}$  cum hac conuenient. Quare si e classibus  $C, C', C''$  etc. formae (simplissimae)  $f, f', f''$  etc. eliguntur, (vna e singulis): e singulis classibus in  $\mathfrak{G}$  vna forma inter has reperietur. Iam si  $axx + 2bxy + cyy$  est forma in classe  $\mathfrak{G}$  contenta, dabuntur duae repraesentationes numeri  $M$  per ipsam ad valorem  $r$  pertinentes, et si vna est  $x = m, y = n$ , altera erit  $x = -m, y = -n$ ; vnicus casus excipi debet, vbi  $D = 1$ , in quo quatuor repraesentationes dabuntur (v. art. 180).

Ex his colligitur, si omnes repraesentationes numeri  $M$  per singulas formas  $f, f', f''$  etc. inuestigentur (per methodum indirectam in praec. traditam), atque hinc valores expr.  $\sqrt{-D}$  (mod.  $M$ ) ad quos singulae pertinent deducantur (art. 154 sqq), omnes valores huius expressionis inde obtineri, et quidem singulos bis, aut, si  $D = 1$ , quater. Q. E. F. Si quae formae inter  $f, f'$  etc. reperiuntur, per quas  $M$  repraesentari nequit, hoc est indicium, ipsas, ad nullam classem in  $\mathfrak{G}$  pertinere, adeoque negligendas esse: si vero  $M$  per nullam illarum formarum repraesentari potest, necessario  $-\sqrt{-D}$  debet esse non residuum quadraticum ipsius  $M$ . — Circa has operationes teneantur adhuc observationes sequentes.

I. Repraesentationes numeri  $M$  per formas  $f, f'$  etc., quas hic adhibemus, subintelliguntur esse tales, in quibus indeterminatarum valores inter se primi sunt; si quae aliae se offerunt, in quibus hi valores diuisorem communem  $\mu$  ha-



bent (quod tunc tantummodo accidere potest, vbi  $\mu$  metitur ipsum  $M$ , certoque accidet, quando —  $DR^M$ ) hae: ad institutum praesens omnino negligi debent, etsi alio respectu viles esse possint.

II. Ceteris paribus labor manifesto eo facilius erit, quo minor est multitudo classium  $f, f', f''$  etc., adeoque breuissimus, quando  $D$  est vnus e 65 numeris in art. 303. traditis, pro quibus in singulis generibus vnica tantum classis datur.

III. Quum binae semper huiusmodi repraesentationes  $x = m, y = n; x = -m, y = -n$  ad eundem valorem pertineant, perspicuum est, sufficere, si eae tantummodo repraesentationes considerentur, in quibus  $y$  positivus. Tales itaque repraesentationes diuersae semper valoribus diuersis expr.  $\sqrt{-D} \pmod{M}$  respondent, vnde multitudo omnium valorum diuersum multitudini omnium talium repraesentationum prodeuntium aequalis erit (semper excipiendo casum  $D = 1$ , vbi illa huius semissis erit).

IV. Quoniam, simulac alter duorum valorum oppositorum  $+r, -r$ , cognitus est, alter sponte innotescit, operationes adhuc aliquantum abbreviari possunt. Si valor  $r$  obtinetur e repraesentatione numeri  $M$  per formam in classe  $C$  contentam, i. e. si  $\mathfrak{C} = C$ ; valor oppositus  $-r$  manifesto emerget e repraesentatione per formam, in classe ipsi  $C$  opposita contentam,