SECTIO QVINTA

DE

FORMIS AEQVATIONIBVSQVE INDETERMINATIS

SECVNDI GRADVS.

153. In hac sectione imprimis de functionibus duarum indeterminatarum x, y, huius formae, $axx + 2bxy + cyy$, vbi a, b, c sunt integri dati tractabimus, quas *formas secundi gradus*, siue simpliciter *formas* dicemus. Huic disquisitioni superstruetur solutio problematis famosi, inuenire omnes solutiones aequationis cuiuscunque indeterminatae secundi gradus duas incognitas implicantis, siue hae incognitae valores integros siue rationales tantum nancisci debeant. Problema hoc quidem iam ab ill. La Grange in omni generalitate est solutum, multaque insuper ad naturam *formarum* pertinentia tum ab hoc ipso magno geometra, tum ab ill. Eulero partim primum inuenta, partim, a Fermatio olim inuenta, demonstrationibus munita. Sed nobis acriter formarum perquisitioni insistentibus tam multa noua se obtulerunt, vt totum argumen-

tum ab integro resumere operae pretium duxerimus, eo magis, quod Virorum illorum inuenta, multis locis sparsa, paucis innotuisse comperti sumus; porro quod methodus per quam haec tractabimus nobis ad maximam partem est propria; tandem quod nostra sine noua illorum expositione ne intelligi quidem possent. Nullum vero dubium nobis esse videtur, quin multa eaque egregia in hoc genere adhuc lateant in quibus alii vires suas exercere possint. Ceterum quae ad veritatum insignium historiam pertinent, loco suo semper trademus.

Formam $axx + 2bxy + cyy$, quando de indeterminatis x, y non agitur, ita designabimus, (a, b, c). Haec itaque expressio denotabit indefinite summam trium partium, producti numeri dati a in quadratum indeterminatae cuiuscunque; producti duplicati numeri b in hanc indeterminatam in aliam indeterminatam; producti numeri c in quadratum huius secundae indeterminatae. Ex. gr. $(1, 0, 2)$ exprimet summam quadrati et quadrati duplicati. Ceterum, quamuis formae (a, b, c) et (c, b, a) idem designent, si ad *partes ipsas* tantum respicimus, tamen different si insuper ad partium *ordinem* attendimus; quare sedulo eas in posterum distinguemus; quid vero inde lucremur in sequentibus sufficienter patebit.

154. Numerum aliquem datum per formam datam *repraesentari* dicemus, si formae indeterminatis tales valores integri tribuuntur,

vt ipsius valor numero dato fiat aequalis. Hic habebimus sequens

THEOREMA. *Si numerus M ita per formam* (a, b, c) *repraesentari potest, vt indeterminatarum valores, per quos hoc efficitur, inter se sint primi: erit* $bb - ac$ *residuum quadraticum numeri M.*

Dem. Sint valores indeterminatarum m, n, scilicet $amm + 2bmn + cnn = M$, accipianturque numeri μ, ν ita vt sit $\mu m + \nu n = 1$ (art. 40). Tum per euolutionem facile probatur esse, $(amm + 2bmn + cnn)(a\nu\nu - 2b\mu\nu + c\mu\mu) = (\mu(mb + nc) - \nu(ma + nb))^2 - (bb - ac)(m\mu + n\nu)^2$, siue $M(a\nu\nu - 2b\mu\nu + c\mu\mu) = (\mu(mb+nc) - \nu(ma + nb))^2 - (bb - ac)$. Quare erit $bb - ac \equiv (\mu(mb+nc) - \nu(ma + nb))^2 \pmod{M}$, *i. e.* $bb - ac$ residuum quadraticum ipsius M.

Numerum $bb - ac$, a cuius indole proprietates formae (a, b, c) imprimis pendere, in sequentibus docebimus, *determinantem* huius formae vocabimus.

155. Erit itaque $\mu(mb + nc) - \nu(ma+nb)$ valor expressioris $\sqrt{(bb - ac)} \pmod{M}$. Constat autem, numeros μ, ν infinitis modis ita determinari posse vt sit $\mu m + \nu n = 1$, vnde alii aliique valores illius expressionis prodibunt, qui quem nexum inter se habeant videamus. Sit non modo $\mu m + \nu n = 1$, sed etiam $\mu' m + \nu' n = 1$, ponaturque $\mu(mb + nc) - \nu(ma+nb) = v$, $\mu'(mb + nc) - \nu'(ma + nb) = v'$. Multiplicando aequationem $\mu m + \nu n = 1$ per μ', al-