

teram  $\mu'm + v'n = 1$  per  $\mu$ , et subtrahendo fit  $\mu' - \mu = n(\mu'v - \mu v')$  similiterque multiplicando illam per  $v'$  hanc per  $v$  fit subtrahendo  $v' - v = m(\mu v' - \mu'v)$ . Hinc statim prodit  $v' - v = (\mu v' - \mu'v)(amm + 2bmn + cnn) = (\mu v' - \mu'v)M$ , siue  $v' \equiv v \pmod{M}$ . Quomodocunque igitur  $\mu, v$  determinantur, formula  $\mu(mb + nc) - v(ma + nb)$  valores *diuersos* (i. e. incongruos) expressionis  $v(bb - ac) \pmod{M}$  dare nequit. Si itaque  $v$  est valor quicunque illius formulae: repraesentationem numeri  $M$  per formam  $axx + 2bxy + cyy$  eam ubi  $x = m, y = n$ , pertinere dicemus ad valorem  $v$ , expressionis  $\sqrt{(bb - ac)} \pmod{M}$ . Ceterum facile ostendi potest, si valor formulae illius aliquis sit  $v$  atque  $v' \equiv v \pmod{M}$ , loco numerorum  $\mu, v$ , qui dant  $v$ , alios  $\mu', v'$  accipi posse, qui dent  $v'$ . Scilicet faciendo  $\mu' = \mu + \frac{n(v' - v)}{M}$ ,  $v' = v - \frac{m(v' - v)}{M}$ , fiet  $\mu'm + v'n = \mu m + v n = 1$ , valor autem formulae ex  $\mu', v'$  prodiens superabit valorem ex  $\mu, v$  prodeuntem quantitate  $(\mu v' - \mu'v)M$ , quae fit  $= (\mu m + v n)(v' - v) = v' - v$ , siue valor ille erit  $= v'$ .

156 Si duae repraesentationes eiusdem numeri  $M$  per eandem formam  $(a, b, c)$  habentur, in quibus indeterminatae valores inter se primos habent: hae vel ad eundem valorem expr.  $\sqrt{(bb - ac)} \pmod{M}$  pertinere possunt vel ad diuersos. Sit  $M = am + 2bm + cn = am' + 2bm' + cn'$ , atque  $\mu m + v n = 1$ ,  $\mu m' + v' n' = 1$ , patetque si fuerit

$\mu(mb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M}$ , congruentiam semper manere, quicumque alii valores idonei pro  $\mu, \nu; \mu', \nu'$  accipiantur, in quo casu utramque repraesentationem ad eundem valorem expr.  $\sqrt{(bb - ac)} \pmod{M}$  pertinere dicemus; si vero congruentia pro vllis valoribus ipsorum  $\mu, \nu; \mu', \nu'$  locum non habet, pro nullis locum habebit, repraesentationesque ad valores *diuersos* pertinebunt. Si vero  $\mu(mb + nc) - \nu(ma + nb) \equiv -(\mu'(m'b + n'c) - \nu'(m'a + n'b))$ : repraesentationes ad valores *oppositos* expr.  $\sqrt{(bb - ac)}$  pertinere dicentur. Omnibus hisce denominationibus etiam utemur, quando de pluribus repraesentationibus eiusdem numeri per formas *diuersas*, sed quae eundem determinantem habent, agitur.

Ex. Sit forma proposita haec  $(3, 7, -8)$  cuius determinans  $= 73$ . Per hanc formam habentur repraesentationes numeri 57 hae:  $3.13^2 + 14.13.25 - 8.25^2; 3.5^2 + 14.5.9 - 8.9^2$ . Pro prima poni potest  $\mu = 2, \nu = -1$ , vnde prodit valor expr.  $\sqrt{73} \pmod{57}$  ad quam repr. pertinet  $= 2(13.7 - 25.8) + (13.3 + 25.7) = -4$ . Simili modo repraesentatio secunda pertinere inuenitur, faciendo  $\mu = 2, \nu = -1$ , ad valorem  $+4$ . Quare ambae repraesentationes ad valores oppositos pertinent.

Antequam ulterius progredimur, observamus, formas quarum determinans  $= 0$  ab investigationibus sequentibus prorsus exclusas esse, quippe quae theorematum concinnitatem tantummodo turbarent, adeoque tractationem peculiarem postulent.



157. Si forma,  $F$ , cuius indeterminatae sunt  $x, y$  in aliam  $F'$ , cuius indeterminatae sunt  $x', y'$  per substitutiones tales  $x = \alpha x' + \epsilon y'$ ,  $y = \gamma x' + \delta y'$  transmutari potest, ita ut  $\alpha, \epsilon, \gamma, \delta$  sint integri: priorem implicare posteriorem, siue posteriorem sub priori contentam esse dicemus. Sit forma  $F$  haec  $axx + 2bxy + cyy$ , forma  $F'$  vero haec  $a'x'x' + 2b'x'y' + c'y'y'$ , habebunturque sequentes tres aequationes:

$$a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$$

$$b' = a\alpha\epsilon + b(\alpha\delta + \epsilon\gamma) + c\gamma\delta$$

$$c' = a\epsilon\epsilon + 2b\epsilon\delta + c\delta\delta.$$

Multiplicando aequationem secundam per se ipsam, primam per tertiam, et subtrahendo fit deletis partibus se destruentibus  $b'b' - a'c' = (bb - ac)(\alpha\delta - \epsilon\gamma)^2$ . Vnde sequitur determinantem formae  $F'$  per determinantem formae  $F$  diuisibilem et quotientem esse quadratum; manifesto igitur hi determinantes eadem signa habebunt. Quodsi itaque insuper forma  $F'$  per similem substitutionem in formam  $F$  transmutari potest, i. e. si tum  $F'$  sub  $F$ , tum  $F$  sub  $F'$  contenta est, formarum determinantes erunt aequales \*) atque  $(\alpha\delta - \epsilon\gamma)^2 = 1$ . In hoc casu formas *aequivalentes* dicemus. Quare ad formarum aequivalentiam aequalitas determinantium est conditio necessaria, licet illa ex hac sola minime sequatur. —

\*) Manifestum est ex analysi praecedente hanc propositionem etiam ad formas quarum determinans  $= 0$ , patere. Sed aequatio  $(\alpha\delta - \epsilon\gamma)^2 = 1$  ad hunc casum non est extendenda.