

II. Si valores p, p', p'', p''' ipsorum $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ reddant $B = \mathfrak{B}$, inueniri posse alios valores horum numerorum ex quibus B nanciscatur valorem quemcunque datum ipsi \mathfrak{B} secundum mod. A congruum, puta $\mathfrak{B} + kA$. Primo obseruamus, quatuor numeros $a, c, c', b - b'$ diuisorem communem habere non posse; nam si quem haberent, hic metiretur sex numeros $a, a', b + b', c, c', b - b'$ adeoque tum ipsos $a, 2b, c$, tum ipsos $a', 2b', c'$ et proin etiam ipsos m, m' , qui per hyp. inter se sunt primi. Quamobrem quatuor numeri integri h, h', h'', h''' poterunt assignari tales ut fiat $h^a + h'c + h''c' + h'''(b - b') = 1$. Quo facto si statuitur $kh = d, k(h''(b + b') - h'''a') = \mu d', k(h'(b + b') + h'''a) = \mu d'', -k(h'a' + h''a) = \mu d'''$, patet, ipsos d, d', d'', d''' esse integros; porro facile confirmatur, fieri $ad' + a'd'' + (b + b')d''' = 0, aa'd + ab'd' + a'b'd'' + (bb' + D)d''' = aa'k$. $(\mu h + ch' + c'h'' + (b - b')h''') = \mu ka$. Ex aequatione priori patet, etiam $p + d, p' + d', p'' + d'', p''' + d'''$ esse valores ipsorum $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$; ex posteriori, hos valores producere $B = \mathfrak{B} + kA$. Q. E. D. — Hinc perspicuum est, B semper ita determinari posse ut iaceat inter 0 et $A - 1$ incl., siquidem A est positius; vel inter 0 et $-A - 1$ si A negatius.

243. Ex aequationibus $\mathfrak{P}a + \mathfrak{P}'a' + \mathfrak{P}''(b + b') = \mu, B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$ deducitur $B = b + \frac{a}{\mu}(\mathfrak{P}a' +$

$\mathfrak{P}'(b' - b) - \mathfrak{P}'''c) = b' + \frac{a'}{\mu} (\mathfrak{P}a + \mathfrak{P}''(b - b') - \mathfrak{P}'''c)$; quare $B \equiv b \pmod{\frac{a}{\mu}}$ et $B \equiv b' \pmod{\frac{a'}{\mu}}$. Quoties $\frac{a}{\mu}$, $\frac{a'}{\mu}$ inter se primi sunt, inter o) et $A = 1$ (siue inter o et $-A = 1$ quando A est negatius) vnicus tantum numerus iacebit qui secundum mod. $\frac{a}{\mu}$ sit $\equiv b$, et $\equiv b'$ sec. mod. $\frac{a'}{\mu}$; qui si statuitur $=$ atque $\frac{BB - D}{A} = C$, palam est, (A, B, C) e formis (a, b, c) , (a', b', c') compositam fore. In hoc itaque casu ad inventionem formae compositae ad numeros \mathfrak{P} , \mathfrak{P}' , \mathfrak{P}'' , \mathfrak{P}''' non amplius oportet respicere. Ita e. g. si quaeritur forma e formis $(10, 3, 11)$, $(15, 2, 7)$ composita, erunt $a, a' = b + b'$ resp. $\equiv 10, 15, 5$; $\mu = 5$; hinc $A = 6$; $B \equiv 3 \pmod{2}$ et $\equiv 2 \pmod{3}$, vnde $B = 5$ atque $(6, 5, 21)$ forma quaesita. — Ceterum conditio vt $\frac{a}{\mu}, \frac{a'}{\mu}$ inter se primi sint omnino aequiualeat huic vt numeri duo a, a' diuisorem communem maiorem non habeant quam tres $a, a', b + b'$, siue, quod eodem reddit, vt diuisor communis maximus numerorum a, a' etiam numerum $b + b'$ metiatur. Notentur imprimis sequentes casus particulares:

1) Propositis duabus formis (a, b, c) , (a', b', c') eiusdem determinantis D ita comparatis vt diuisor comm. max. numerorum $a, 2b, c$ primus sit ad diu. comm. max. num. $a', 2b', c'$, atque a

primus ad a' : forma ex his composita (A, B, C) inuenit
natur faciendo $A = aa'$, $B \equiv b$ (mod. a) et $\equiv b'$
(mod. a'), $C = \frac{BB - D}{A}$. Hic casus semper locum
habet, quando altera formarum componendarum
est forma principalis, puta $a = 1$, $b = 0$, $c = -D$. Tunc erit $A = a'$, B statui poterit $= b'$,
vnde fiet $C = c'$; quare ex forma principali et
quacunque alia forma eiusdem determinantis
composita est haec forma ipsa.

2) Si duae formae oppositae proprie primitiuae sunt componendae, puta (a, b, c) et $(a, -b, c)$, erit $\mu = a$. Hinc facile perspicitur,
formam principalem $(1, 0, -D)$ ex illis esse
compositam.

3) Propositis quotcunque formis proprie primitiuis, (a, b, c) , (a', b', c') , (a'', b'', c'') etc.
eiusdem determinantis D , quarum termini antecedentes
 a, a', a'' etc. sunt numeri inter se pri-
mi, forma (A, B, C) ex illis omnibus compo-
sita inuenit, statuendo A aequalem producto
ex omnibus a, a', a'' etc.; B congruum ipsis $b,$
 b', b'' etc. secundum modulos a, a', a'' etc. resp.;
 $C = \frac{BB - D}{A}$. Facile enim perspicietur, ex
duabus formis (a, b, c) , (a', b', c') compositam
fore formam $(aa', B, \frac{BB - D}{aa'})$; ex hac atque
 (a'', b'', c'') formam $(aa'a'', B, \frac{BB - D}{aa'a''})$ etc.
Vice versa

4) Proposita forma proprie primitua $(A, B,$
 $C)$ determinantis D , si terminus A in factores

$A \ a$