

meri primi imparis potestas aut $= 4$; quando vero m sit $= 8$ aut altior potestas numeri 2, quatuor omnino dari. Hinc facile deducitur per VI, si determinans D formae (a, b, c) sit $= \pm 2^\mu A^\alpha B^\beta \dots$, designantibus A, B etc. numeros primos impares diuersos quorum multitudo $= n$, atque M numerus characteristicus illius formae: dari omnino vel 2^n vel 2^{n+1} vel 2^{n+2} valores diuersos expr. $\sqrt{M(a, b, c)} \pmod{D}$, prout μ vel < 2 vel $= 2$ vel > 2 . Ita e. g. habentur sedecim valores expr. $\sqrt{7(12, 6, -17)} \pmod{240}$, puta $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Demonstrationem ampliorem quum ad sequentia non sit adeo necessaria breuitatis gratia non apponimus.

VIII. Denique obseruamus, si duarum formarum aequiualentium (a, b, c) , (a', b', c') determinans sit D , numerus characteristicus M , priorque transeat in posteriorem per substitutionem $a, \epsilon, \gamma, \delta$: ex quouis valore expr. $\sqrt{M(a, b, c)}$ vt (g, h) sequi valorem expr. $\sqrt{M(a', b', c')}$, puta $(ag + \gamma h, \epsilon g + \delta h)$. Demonstrationem quisque nullo negotio eruere poterit.

234. Postquam haec de formis in classes genera et ordines distribuendis praemisimus, proprietatesque generales quae ex his distinctionibus statim defluunt explicauimus, ad aliud argumentum grauissimum transimus a nemine hucusque attactum, de formarum *compositione*. In cuius disquisitionis limine, ne posthac demonstrationum

seriem continuam interrompere oporteat, statim intercalamus

LEMMA. *Habentur quatuor series numerorum integrorum $a, a', a'' \dots a^n$; $b, b', b'' \dots b^n$; $c, c', c'' \dots c^n$; $d, d', d'' \dots d^n$ ex aequae multis (puta $n + 1$) terminis constantes, atque ita comparatae, ut $cd' - dc'$, $cd'' - dc''$ etc., $c'd'' - d'c''$ etc. etc. respectiue sint $= k(ab' - ba')$, $k(ab'' - ba'')$ etc., $k(a'b'' - b'a'')$ etc. etc., siue generaliter $c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$, denotante k numerum integrum datum; λ, μ integros quoscunque inaequales inter 0 et n incl. quorum maior μ *); praeterea omnes $a^\lambda b^\mu - b^\lambda a^\mu$ diuisorem communem non habent. Tunc inueniri possunt quatuor numeri integri $\alpha, \beta, \gamma, \delta$ tales, ut sit $\alpha a + \beta b = c$, $\alpha a' + \beta b' = c'$, $\alpha a'' + \beta b'' = c''$ etc.; $\gamma a + \delta b = d$, $\gamma a' + \delta b' = d'$ etc. siue generaliter $\alpha a^\nu + \beta b^\nu = c^\nu$, $\gamma a^\nu + \delta b^\nu = d^\nu$; quo facto erit $\alpha\delta - \beta\gamma = k$.*

Quum per hyp. numeri $ab' - ba'$, $ab'' - ba''$ etc. $a'b'' - b'a''$ etc. (quorum multitudo erit $= \frac{1}{2}(n+1)n$) diuisorem communem non habeant, inueniri poterunt totidem alii numeri integri, per quos illis resp. multiplicatis productorum summa fiat $= 1$ (art. 40). Designentur hi multiplicatores per $(0, 1)$, $(0, 2)$ etc. $(1, 2)$ etc., siue generaliter multiplicator ipsius $a^\lambda b^\mu - b^\lambda a^\mu$ per (λ, μ) , ita ut sit $\sum (\lambda, \mu) (a^\lambda b^\mu -$

*) Considerando a tamquam a^0 , b tamquam b^0 etc. — Ceterum manifeste eadem aequatio valebit quoque quando $\lambda = \mu$ aut $\lambda > \mu$.

$b^\lambda a^\mu) = 1$. (Per litteram Σ denotamus aggregatum omnium valorum expressionis, cui praefixa est, qui oriuntur tribuendo ipsis λ, μ omnes valores inaequales inter 0 et n , ita ut sit $\mu > \lambda$). Quo facto si statuitur $\Sigma (\lambda, \mu) (c^\lambda b^\mu - b^\lambda c^\mu) = \alpha$, $\Sigma (\lambda, \mu) (a^\lambda c^\mu - c^\lambda a^\mu) = \epsilon$, $\Sigma (\lambda, \mu) (d^\lambda b^\mu - b^\lambda d^\mu) = \gamma$, $\Sigma (\lambda, \mu) (a^\lambda d^\mu - d^\lambda a^\mu) = \delta$: hi $\alpha, \epsilon, \gamma, \delta$ proprietatibus praescriptis erunt praediti.

Dem. I. Denotante ν numerum quemcunque integrum inter 0 et n , erit $\alpha a^\nu + \epsilon b^\nu = \Sigma (\lambda, \mu) (c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu) = \frac{1}{k} \Sigma (\lambda, \mu) (c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu) = \frac{1}{k} c^\nu \Sigma (\lambda, \mu) (c^\lambda d^\mu - d^\lambda c^\mu) = c^\nu \Sigma (\lambda, \mu) (a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu$. Et per calculum similem eruitur $\gamma a^\nu + \delta b^\nu = d^\nu$. Q. E. P.

II. Quoniam igitur $c^\lambda = \alpha a^\lambda + \epsilon b^\lambda$, $c^\mu = \alpha a^\mu + \epsilon b^\mu$, fit $c^\lambda b^\mu - b^\lambda c^\mu = \alpha (a^\lambda b^\mu - b^\lambda a^\mu)$, similique modo $a^\lambda c^\mu - c^\lambda a^\mu = \epsilon (a^\lambda b^\mu - b^\lambda a^\mu)$; $d^\lambda b^\mu - b^\lambda d^\mu = \gamma (a^\lambda b^\mu - b^\lambda a^\mu)$; $a^\lambda d^\mu - d^\lambda a^\mu = \delta (a^\lambda b^\mu - b^\lambda a^\mu)$; ex quibus formulis valores ipsorum $\alpha, \epsilon, \gamma, \delta$ multo facilius erui possunt, si modo λ, μ ita accipiuntur ut $a^\lambda b^\mu - b^\lambda a^\mu$ non sit $= 0$, quod certo fieri poterit, quia omnes $a^\lambda b^\mu - b^\lambda a^\mu$ per hyp. diuisorem communem non habent, adeoque omnes $= 0$ esse nequeunt. — Ex iisdem aequationibus deducitur, multiplicando primam