

23.

Demonstratio duorum theorematum Gaussianis his generaliorum:

- I. *Productum ex omnibus radicibus primitivis moduli imparis p unitate sec. p congruum est, excepto casu, in quo $p = 3$.*
- II. *Summa omnium radicum primitivarum moduli primi imparis p est $\equiv 0$, quando $p-1$ per quadratum aliquod divisibilis est; quando vero per nullum quadratum divisibilis, summa est $\equiv \pm 1$, prout multitudo factorum ipsius $p-1$ primorum est par
aut impar* }

(Auctore Friderico Arndt, Sundiae).

Theoremata, quae demonstraturus sum, haec sunt:

- I. *Productum ex omnibus ad eundem exponentem t sec. mod. p^n vel $2p^n$ pertinentibus, denotante p num. primum imparem, unitati congruum est sec. mod. prop., excepto casu, in quo $t = 2$;*
- II. *Summa omnium numerorum ad eundem exponentem t sec. mod. p pertinentium, denotante p num. primum imparem, est $\equiv 0$, quando t per quadratum aliquod divisibilis est, quando vero t per nullum quadratum divisibilis, summa est $\equiv \pm 1$, prout multitudo factorum ipsius t primorum est par
aut impar* }.

Demonstratio ad I.

Denotante a numerum quemcunque ad exponentem t sec. mod. p^n vel $2p^n$ pertinentem, omnes numeri ad t pertinentes residuis potestatum exhibentur:

$$a^{k_1}, a^{k_2}, a^{k_3}, \dots, a^{k_{\varphi t}},$$

ubi sunt $k_1, k_2, k_3, \dots, k_{\varphi t}$ omnes ad t primi eoque minores. Itaque productum P illorum numerorum congruum est potestati

$$a^{k_1+k_2+k_3+\dots+k_{\varphi t}}.$$

Jam vero exponens per t divisibilis est, excepto $t = 2$, ut facile patet, atque $a^t \equiv 1$, ergo etiam $P \equiv 1 \pmod{p^n \text{ vel } 2p^n}$.

Demonstratio ad II.)

(A). Factore primo aliquo, cujus quadratum exponentem t metiatur, per α designato, patet, si k sit numerus ad t primus, etiam $k + \frac{t\varphi}{\alpha}$ ad t primum fore, designante φ integrum quemcunque. Nam primum numeri t , $k + \frac{t\varphi}{\alpha}$ factorem α non simul involvent, quando quidem ex supp. $\frac{t\varphi}{\alpha}$ per α divisibilis est, ergo, si illud fieri posset, numeri t , k factorem communem α haberent, contra supp. Quodsi numeri de quibus agitur, factorem primum communem δ haberent, ab α diversum, esset $k + \frac{t\varphi}{\alpha}$, ideoque $\alpha k + t\varphi$, ergo k per δ divisibilis, haberentque etiam nunc t et k factorem communem.

Denotante igitur a numerum ad exp. t pertinentem, residua potestatum

$$a^k, a^{k+\frac{t}{\alpha}}, a^{k+\frac{2t}{\alpha}}, \dots, a^{k+\frac{(\alpha-1)t}{\alpha}},$$

quorum multitudo α , ad eundem exponentem t pertinebant. Quae residua incongrua esse perspicuum est. Complexus eorum sit K .

Multitudo numerorum ad t primorum eoque minorum ipsius a multipulum esse debet. Posito enim $t = \alpha^g \beta^h \gamma^i$ etc., ubi $g \geq 2$, habetur $\varphi t = \alpha^{g-1}(\alpha-1)\beta^h(\beta-1)\gamma^i(\gamma-1)$ etc, ubi $g-1 \geq 1$, ex quo φt per α divisibilis.

Jam sit k_1 numerus ad t primus, ab horum quoque diversus

$$k, k + \frac{t}{\alpha}, k + \frac{2t}{\alpha}, \dots, k + \frac{(\alpha-1)t}{\alpha},$$

habenturque denuo α numeri ad t pertinentes potestatibus congrui:

$$a^{k_1}, a^{k_1+\frac{t}{\alpha}}, a^{k_1+\frac{2t}{\alpha}}, \dots, a^{k_1+\frac{(\alpha-1)t}{\alpha}},$$

omnesque sunt incongrui inter se. Complexus eorum sit L .

Porro sit k_2 numerus ad t primus, ab horum quoque diversus

$$k, k + \frac{t}{\alpha}, k + \frac{2t}{\alpha}, \dots, k + \frac{(\alpha-1)t}{\alpha}$$

$$k_1, k_1 + \frac{t}{\alpha}, k_1 + \frac{2t}{\alpha}, \dots, k_1 + \frac{(\alpha-1)t}{\alpha}$$

habenturque denuo α numeri ad t pertinentes potestatibus congrui:

$$a^{k_2}, a^{k_2+\frac{t}{\alpha}}, a^{k_2+\frac{2t}{\alpha}}, \dots, a^{k_2+\frac{(\alpha-1)t}{\alpha}},$$

omnesque incongrui sunt inter se. Complexus eorum sit M .

Hoc modo progredi licet, quoad omnes numeri ad t primi sunt exhausti; scilicet, si $\varphi t = \alpha q$, multitudo complexuum erit q .

Jam summa numerorum cujusque complexus per modulum p divisibilis est. Denotante enim s summam numerorum complexus K , habetur

