Disquitiones Arithmeticae

auctore

D. Carolo Friderico Gauss

I. DE NUMERORUM CONGRUENTIA IN GENERE

Numeri congrui, moduli, residua et nonresidua

1.

Si numerus a numerorum b, c differentiam metitur, b et c *secundum a congrui* dicuntur, sin minus, *incongrui*: ipsum a *modulum* appellamus. Uterque numerorum b, c priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis valent[1], neque vero ad fractos sunt extendendae. E. g. -9 et 16 secundum modulum 5 sunt congrui; -7 ipsius 15 secundum modulum 11 residuum, secondum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2.

Omnia numeri dati a residua secundum modulum m sub formula $a + km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post trademus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quivis intuendo poterit perspicere.

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes: $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$[2].

3.

Theorema. *Propositis m numeris integris successivis*

$$a, a+1, a+2, \ldots, a+m-1$$

alioque A, illorum aliquis huic secundum modulum m congruus erit, et quidem unicus tantum.

Si enim $\frac{a-A}{m}$ integer, erit $a \equiv A$, sin fractus, sit integer proxime maior (aut quando est negativus, proxime *minor*, si ad signum non respiciatur) aequalis k, cadetque $A + km$ inter a et $a + m$, quare erit numerus quaesitus. Et manifestum est omnes quotientes $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$ etc. inter $k-1$ et $k+1$ sitos esse; quare plures quam unus integri esse nequeunt.

Residua minima

4.

Quisque igitur numerus residuum habebit tum in hac serie, $0, 1, 2, \ldots, m-1$, tum in hac, $0, -1, -2, \ldots, -(m-1)$, quae *residua minima* dicemus, patetque, nisi 0 fuerit residuum, bina semper dari, *positivum* alterum, alterum *negativum*. Quae si magnitudine sunt inaequalia, alterum erit minus quam $\frac{m}{2}$, sin secus utrumque $\frac{m}{2}$ aequalis, signi respectu non habito. Unde patet, quemvis numerum residuum habere moduli semissem non superans quod *absolute minimum* vocabitur.

E. g. -13 secundum modulum 5, habet residuum minimum positivum 2, quod simul est absolute minimum, -3 vero residuum minimum negativum; 5 secundum modulum 7 sui ipsius est residuum minimum positivum, -2 negativum, simulque absolute minimum.

---

[1] Modulus manifesto semper *absolute* i. e. sine omni signo est sumendus.

[2] Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam invenitur adoptavimus. Ob eandem caussam ill. Le Gendre in comment. infra saepius laudanda ipsum aequalitatis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur imitari dubitavimus.

Propositiones elementares de congruentiis

5.

His notionibus stabilitis eas numerorum congruorum propietates quae prima fronte se offerunt colligamus.

Qui numeri secundum modulum compositum sunt congrui, etiam secundum quemvis eius divisorem congrui. Si plures numeri eidem numero secundum eundem modulum sunt congrui, inter se erunt congrui (secundum eundem modulum).

Haec modulorum indentitas etiam in sequentibus est subintelligenda.

Numeri congrui residua minima habent eadem, incongrui diversa.

6.

Si habentur quotcunque numeri A, B, C etc. totidemque alii a, b, c etc. illus secundum modulum quemque congrui

$$A \equiv a, B \equiv b, \text{etc., erit } A + B + C + \text{etc.} \equiv a + b + c + \text{etc.}$$

Si $A \equiv a, B \equiv b$, erit $A - B \equiv a - b$.

7.

Si $A \equiv a$, erit quoque $kA \equiv ka$.

Si k numerus positivus, hoc est tantummodo casus particularis propos. art. praec. ponendo ibi $A = B = C =$ etc., $a = b = c$ etc. Si k negativus, erit $-k$ positivus, adeoque $-kA \equiv -ka$, unde $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, erit $AB \equiv ab$. Namque $AB \equiv Ab \equiv ba$.

8.

Si habentur quotcunque numeri $A, B, C,$ etc. totidemque alii $a, b, c,$ etc. his congrui, $A \equiv a$, $B \equiv b,$ etc., producta ex utrisque erunt congrua, ABC etc. $\equiv abc$ etc.

Ex artic. praec. $AB \equiv ab$, et ob eandem rationem $ABC \equiv abc$; eodemque modo quotcunque alii factores accedere possunt.

Si omnes numeri $A, B, C, \ldots$ aequales assumuntur, nec non respondentes $a, b, c, \ldots$ habetur hoc theorema: *Si $A \equiv a$ et k integer positivus, erit $A^k \equiv a^k$.*