DISQVISITIONES ARITHMETICAE

SECTIO PRIMA

DE NVMERORVM CONGRVENTIA IN GENERE.

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

Hae notiones de omnibus numeris integris tam positiuis quam negatiuis *) valent, neque

*) Modulus manifesto semper *absolute* i. e. sine omni signo est sumendus.

vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum 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 quiuis intuendo poterit perspicere.

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum vbi opus erit in clausulis adiungentes, $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11) *).

3. THEOR. *Propositis m numeris integris successiuis, $a, a+1, a+2 \ldots a+m-1$, alioque A, illorum aliquis huic secundum modulum m congruus erit, et quidem vnicus tantum.*

Si enim $\frac{A-a}{m}$ integer, erit $a \equiv A$, sin fractus, sit integer proxime maior, (aut quando est negatiuus, proxime *minor*, si ad signum non respiciatur) $= k$, cadetque $A+km$ inter a et

*) Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam inuenitur adoptauimus. Ob eandem caussam ill. Le Gendre in comment. infra saepius laudanda ipsum aequalitatis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur imitari dubitauimus.

$a+m$, 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 vnus integri esse nequeunt.

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, *positiuum* alterum, alterum *negatiuum*. Quae si magnitudine sunt inaequalia, alterum erit $< \frac{m}{2}$, sin secus vtrumque $= \frac{m}{2}$, signi repectu non habito. Vnde patet, quemuis numerum residuum habere moduli semissem non superans quod *absolute minimum* vocabitur.

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

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

Qui numeri secundum modulum compositum sunt congrui, etiam secundum quemuis eius diuisorem congrui.

Si plures numeri eidem numero secundum eundem modulum sunt congrui, inter se erunt congrui (secundum eundem modulum).

Haec modulorum identitas etiam in sequentibus est subintelligenda.