

## 18.

# Nova solutio problematis determinandi multitudinem numerorum, qui ad numerum aliquem sint primi eoque minores.

(Auctore Friderico Arndt, Sundiae.)

Miretur fortasse aliquis, quod problematis ab Ill. geometris, *Eulero*, *Gaussio*, *Grunerto*, aliisque jam soluti, novam disquisitionem instituam. *Euleri* quidem solutio, de qua confer. Nov. Comm. Acad. Petrop. T. VIII. p. 74. et Nov. Act. Petrop. T. VIII. p. 17., non sine multis ambagibus perficitur, qua de causa *Gaussius* in Disq. Arith. Lips. 1801. p. 30. et *Grunertus* in Opere „Archiv der Mathematik etc. T. III. n. XX. aliam tamque simplicem viam inierunt, ut nihil amplius in hac re desiderandum esse videatur. Sed quum novae solutiones novam saepissime lucem alicujus rei afferant, solutionem, quam inveni, quod in lucem proferam, a lectore benigno, ut excuset, peto.

## 1.

Si numerus propositus est potestas aliqua numeri primi, scilicet  $p^n$ , omnes numeri ad eum primi sunt ii, qui factorem  $p$  non involvant. Quorum multitudo quum sit  $p - 1$  inter limites 1 et  $p$ , eademque inter limites  $p$  et  $2p$ ,  $2p$  et  $3p$ , etc., manifesto multitudo talium numerorum ipso  $p^n$  minorum erit  $p^{n-1}(p - 1)$  vel  $p^n\left(1 - \frac{1}{p}\right)$ .

## 2.

*Theorema.* Si numeri  $a$ ,  $b$  sunt inter se primi, designatque omnino  $\varphi N$  multitudinem numerorum ad  $N$  primorum eoque minorum, erit

$$\varphi(ab) = \varphi a \times \varphi b.$$

Demonstrationem hujus theorematis, quod ipsum in Disq. Arith. legitur hoc modo instituo.

a) Quando  $x$  ad  $a$ ,  $y$  ad  $b$  primus est, residuum minimum summae  $ay + bx$  secundum modulum  $ab$  ad hunc ipsum primum esse debet.

Si enim illud residuum, quod per  $r$  designemus, et modulus  $ab$  factorem aliquem primum  $\vartheta$  simul haberent, manifesto  $\vartheta$  numerum  $ay + bx$  metiretur. Atqui alter certe numerorum  $a$ ,  $b$  factorem  $\vartheta$  involveret, ex. gr.  $a$ , ergo hic factor numerum  $bx$  metiretur. Quia autem  $x$  ad  $a$  primus est,  $x$  per  $\vartheta$  non potest esse divisibilis, ideoque  $\vartheta$  factor esset numeri  $b$ , quod fieri nequit, quoniam  $a$  et  $b$  sunt inter se primi. Ergo residuum  $r$  ad  $ab$  primum est.

b) Quando pro numero  $x$  ponuntur omnes numeri ad  $a$  primi eoque minores, pro  $y$  autem omnes ad  $b$  primi eoque minores, residua minima exortarum inde summarum  $ay + bx$  secundum modulum  $ab$  inaequalia esse debent.

Nam si esset  $ay + bx \equiv ay' + bx' \pmod{ab}$ , haberetur  $a(y - y') + b(x - x') \equiv 0 \pmod{a}$ , ergo  $b(x - x') \equiv 0 \pmod{a}$ , ideoque  $x - x' \equiv 0 \pmod{a}$ , quod fieri nequit, si differentia  $x - x'$  ipso  $a$  est minor.

c) Duo quique numeri resp. ad  $a$  et  $b$  primi sunt  $x' + ka$  et  $y' + \lambda b$ , ita ut sit  $x' < a$  ad eumque primus,  $y' < b$  et ad eum primus. Valoribus his pro  $x$  et  $y$  positis habetur  $ay + bx = ay' + bx' + (k + \lambda)ab$ , i. e.  $ay + bx \equiv ay' + bx' \pmod{ab}$ . Ex quo sequitur, omnia nasci residua diversa summae  $ay = bx$ , si pro  $x$ ,  $y$  accipiantur resp. omnes numeri ad singulos  $a$ ,  $b$  primi iisque inferiores.

d) Si igitur determinantur residua minima summae  $ay + bx$  sec. mod.  $ab$ , dum pro  $x$  et  $y$  sumantur omnes numeri resp. ad  $a$  et  $b$  primi iique inter se combinantur, habebuntur  $\varphi a \times \varphi b$  numeri diversi ad  $ab$  primi eoque inferiores.

e) Quando numerus  $r$  ad  $ab$  primus est, semper numeri  $x$ ,  $y$ , quorum alter ad  $a$ , alter ad  $b$  primus, inveniri possunt, congruentiae satisfaciennes

$$ay + bx \equiv r \pmod{ab}.$$

Quum enim  $b$  sit ad  $a$  primus, congruentiam

$$bx \equiv r \pmod{a}$$

resolvi posse constat, quo loco, ut facile patebit,  $x$  ad  $a$  primus erit. Similimodo congruentia

$$ay \equiv r \pmod{b}$$

resolvi potest, eritque  $y$  ad  $b$  primus.

Propter primam congruentiam  $bx - r$  per  $a$  divisibilis est, ergo etiam  $ay + bx - r$ ; propter secundam simili modo  $ay + bx - r$  per  $b$  divisibilis

est. Itaque, quum  $a$  et  $b$  sint inter se primi, modulus  $ab$  numerum  $ay + bx - r$  metietur, i. e.  $ay + bx \equiv r \pmod{ab}$ .

f) Sequitur ex d) et e) multitudinem omnium numerorum ad  $ab$  primorum eoque minorum esse  $\varphi a \times \varphi b$ .

## 3.

Jam facile intelligitur, esse pro quotiunque factoribus

$$\varphi(abc\dots) = \varphi a \times \varphi b \times \varphi c \dots,$$

dummodo duo quique novum factorum sint inter se primi.

## 4.

Numero igitur quocunque  $N$  in factores primos resoluto, ita ut sit

$$N = A^{\alpha} B^{\beta} C^{\gamma} \dots,$$

ex 3. habetur  $\varphi N = \varphi(A^{\alpha}) \cdot \varphi(B^{\beta}) \cdot \varphi(C^{\gamma}) \dots$ , ergo ex 1.

$$\varphi N = A^{\alpha-1}(A-1) \cdot B^{\beta-1}(B-1) \cdot C^{\gamma-1}(C-1) \dots,$$

$$\text{vel } \varphi N = N \left(1 - \frac{1}{A}\right) \left(1 - \frac{1}{B}\right) \left(1 - \frac{1}{C}\right) \dots$$

Scrib. Sundiae d. 8. M. Mart, 1845.