THEOREMATIS ARITHMETICI

DEMONSTRATIO NOVA

1.

Quaestiones ex arithmetica sublimiori saepenumero phaenomenon singulare offerunt, quod in analysi longe rarius occurrit, atque ad illarum illecebras augendas multum confert. Dum scilicet in disquisitionibus analyticis plerumque ad veritates novas pertingere non licet, nisi prius principiis, quibus innituntur, quaeque ad eas viam quasi patefacere debent, penitus potiti simus: contra in arithmetica frequentissime per inductionem fortuna quadam inopinata veritates elegantissimae novae prosiliunt, quarum demonstrationes tam profunde latent tantisque tenebris obvolutae sunt, ut omnes conatus eludant, acerrimisque perscrutationibus aditum denegent. Tantus porro adest tamque mirus inter veritates arithmeticas, primo aspectu maxime heterogeneas, nexus, ut haud raro, dum longe alia quaerimus, tandem ad demonstrationem tantopere exoptatam longisque antea meditationibus frustra quaesitam longe alia via quam qua exspectata fuerat felicissime perveniamus. Plerumque autem huiusmodi veritates eius sunt indolis, ut pluribus viis valde diversis adiri queant, nec semper viae brevissimae sint, quae primo se offerunt. In magno itaque certe pretio habendum erit, si, tali veritate longe incassum ventilata, dein demonstrata quidem sed per ambages abstrusiores, tandem viam simplicissimam atque genuinam detegere contigerit.

2.

Inter quaestiones, de quibus in art. praec. diximus, locum insignem tenet theorema omnem fere theoriam residuorum quadraticorum continens, quod in *Disquisitionibus arithmeticis* (Sect. IV.) *theorematis fundamentalis* nomine dis-

tinctum est. Pro *primo* huius elegantissimi theorematis inventore ill. LEGENDRE absque dubio habendus est, postquam longe antea summi geometrae EULER et LAGRANGE plures eius casus speciales iam per inductionem detexerant. Conatibus horum virorum circa demonstrationem enumerandis hic non immoror; adeant quibus volupe est opus modo commemoratum. Adiicere liceat tantummodo, in confirmationem eorum, quae in art. praec. prolata sunt, quae ad meos conatus pertinent. In ipsum theorema proprio marte incideram anno 1795, dum omnium, quae in arithmetica sublimiori iam elaborata fuerant, penitus ignarus et a subsidiis literariis omnino praeclusus essem: sed per integrum annum me torsit, operamque enixissimam effugit, donec tandem demonstrationem in Sectione quarta operis illius traditam nactus essem. Postea tres aliae principiis prorsus diversis innixae se mihi obtulerunt, quarum unam in Sectione quinta tradidi, reliquas elegantia illa haud inferiores alia occasione publici iuris faciam. Sed omnes hae demonstrationes, etiamsi respectu rigoris nihil desiderandum relinquere videantur, e principiis nimis heterogeneis derivatae sunt, prima forsan excepta, quae tamen per ratiocinia magis laboriosa procedit, operationibusque prolixioribus premitur. Demonstrationem itaque *genuinam* hactenus haud affuisse non dubito pronunciare: esto iam penes peritos iudicium, an ea, quam nuper detegere successit, quamque pagellae sequentes exhibent, hoc nomine decorari mereatur.

3.

THEOREMA. *Sit p numerus primus positivus; k integer quicunque per p non divisibilis;*

$$A \text{ complexus numerorum } 1,\ 2,\ 3 \ldots \tfrac{1}{2}(p-1)$$
$$B \text{ complexus horum } \tfrac{1}{2}(p+1),\ \tfrac{1}{2}(p+3),\ \tfrac{1}{2}(p+5) \ldots p-1$$

Capiantur residua minima positiva productorum ex k in singulos numeros A secundum modulum p, quae manifesto omnia diversa erunt, atque partim ad A partim ad B pertinebunt. Iam si ad B omnino μ residua pertinere supponantur, erit k vel residuum vel non-residuum quadraticum ipsius p, prout μ par est vel impar.

Dem. Sint residua ad A pertinentia haec a, a', a'' ... reliqua ad B pertinentia b, b', b''..., patetque posteriorum complementa $p-b$, $p-b'$, $p-b''$... cuncta a numeris a, a', a''... diversa esse, cum his vero simul sumta complexum

A explere. Habemus itaque

$$1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, \tfrac{1}{2}(p-1) = aa'a'' \ldots \,.\, (p-b)(p-b')(p-b'') \,.\, \ldots$$

Productum posterius autem manifesto fit

$$\equiv (-1)^{\mu} aa'a'' \,.\, \ldots \,.\, bb'b'' \,.\, \ldots \,.\, \equiv (-1)^{\mu} k \,.\, 2k \,.\, 3k \,.\, \ldots \,.\, \tfrac{1}{2}(p-1)k$$
$$\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)} \, 1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, \tfrac{1}{2}(p-1) \pmod{p}$$

Hinc erit

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

sive $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, prout μ par est vel impar, unde theorema nostrum protinus demanat.

4. Ratiocinia sequentia magnopere abbreviare licebit per introductionem quarundam designationum idonearum. Exprimet igitur nobis character (k, p) multitudinem productorum ex his

$$k, \; 2k, \; 3k \,.\, \ldots \,.\, (p-1)k$$

quorum residua minima positiva secundum modulum p huius semissem superant. Porro existente x quantitate quacunque non integra, per signum $[x]$ exprimemus integrum ipsa x proxime minorem, ita ut $x - [x]$ semper fiat quantitas positiva intra limites 0 et 1 sita. Levi iam negotio relationes sequentes evolventur:

I. $[x] + [-x] = -1$

II. $[x] + h = [x + h]$, quoties h est integer.

III. $[x] + [h - x] = h - 1$

IV. If $x - [x]$ est fractio minor quam $\frac{1}{2}$, erit $[2x] - 2[x] = 0$; si vero $x - [x]$ est maior quam $\frac{1}{2}$, erit $[2x] - 2[x] = 1$.

V. Iacente itaque residuo minimo positivo integri h secundum modulum p infra $\frac{1}{2}p$, erit $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 0$; iacente autem residuo illo ultra $\frac{1}{2}p$, erit $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 1$.

VI. Hinc statim sequitur $(k,p) =$

$$\begin{aligned}&\left[\tfrac{2k}{p}\right] + \left[\tfrac{4k}{p}\right] + \left[\tfrac{6k}{p}\right] + \cdots + \left[\tfrac{(p-1)k}{p}\right]\\ -2&\left[\tfrac{k}{p}\right] - 2\left[\tfrac{2k}{p}\right] - 2\left[\tfrac{3k}{p}\right] - \cdots - 2\left[\tfrac{\frac{1}{2}(p-1)k}{p}\right].\end{aligned}$$

VII. Ex VI. et I. nullo negotio derivatur

$$(k,p) + (-k,p) = \tfrac{1}{2}(p-1)$$

Unde sequitur, $-k$ vel eandem vel oppositam relationem ad p habere (quatenus huius residuum aut non-residuum quadraticum est) ut $+k$, prout p vel formae $4n+1$ fuerit, vel formae $4n+3$. In casu priori manifesto -1 residuum, in posteriori non-residuum ipsius p erit.

VIII. Formulam in VI. traditam sequenti modo transformabimus. Per III. fit

$$\left[\tfrac{(p-1)k}{p}\right] = k-1-\left[\tfrac{k}{p}\right], \left[\tfrac{(p-3)k}{p}\right] = k-1-\left[\tfrac{3k}{p}\right], \left[\tfrac{(p-5)k}{p}\right] = k-1-\left[\tfrac{5k}{p}\right] \ldots.$$

Applicando hasce substitutiones ad $\frac{p\mp 1}{4}$ membra ultima seriei superioris in illa expressione, habebimus

primo, quoties p est formae $4n+1$

$$\begin{aligned}(k,p) =&\tfrac{1}{4}(k-1)(p-1)\\ &-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] + \cdots + \left[\tfrac{\frac{1}{2}(p-3)k}{p}\right]\right\}\\ &-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{4k}{p}\right] - \cdots - \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

secundo, quoties p est formae $4n+3$

$$\begin{aligned}(k,p) =&\tfrac{1}{4}(k-1)(p+1)\\ &-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] + \cdots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}\\ &-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{4k}{p}\right] - \cdots - \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}\end{aligned}$$

IX. Pro casu speciali $k = +2$ e formulis modo traditis sequitur $(2,p) = \frac{1}{4}(p \mp 1)$, sumendo signum superius vel inferius, prout p est formae $4n+1$ vel $4n+3$. Erit itaque $(2,p)$ par, adeoque $2Rp$, quoties p est formae $8n+1$ vel $8n+7$; contra erit $(2,p)$ impar atque $2Np$, quoties p est formae $8n+3$ vel $8n+5$.

5.

THEOREMA. *Sit x quantitas positiva non integra, inter cuius multipla x, $2x$, $3x$ . . . . usque ad nx nullum fiat integer; ponatur $[nx] = h$, unde facile concluditur, etiam inter multipla quantitatis reciprocae $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x}$ . . . . . usque ad $\frac{h}{x}$ integrum non reperiri. Tum dico fore*

$$\left.\begin{array}{l} [x] + [2x] + [3x] + \ .. \ + [nx] \\ + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \left[\frac{3}{x}\right] \ .... \ + \left[\frac{h}{x}\right] \end{array}\right\} = nh.$$

Dem. Seriei $[x] + [2x] + [3x] \ .... \ + [nx]$, quam ponemus $= \Omega$, membra prima usque ad $\left[\frac{1}{x}\right]^{tum}$ inclus. manifesto omnia erunt $= 0$; sequentia usque ad $\left[\frac{2}{x}\right]^{tum}$ cuncta $= 1$; sequentia usque ad $\left[\frac{3}{x}\right]^{tum}$ cuncta $= 2$ et sic porro. Hinc fit

$$\left.\begin{array}{rl} \Omega = & 0 \times \left[\frac{1}{x}\right] \\ + & 1 \times \left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} \\ + & 2 \times \left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\} \\ + & 3 \times \left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} \\ & \text{etc.} \\ + & (h-1)\left\{\left[\frac{h}{x}\right] - \left[\frac{h-1}{x}\right]\right\} \\ + & h\left\{n - \left[\frac{h}{x}\right]\right\} \end{array}\right\} = hn - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] \ .... \ - \left[\frac{h}{x}\right]$$

Q.E.D.

6.

THEOREMA. *Designantibus k, p numeros positivos impares inter se primos quoscunque, erit*

$$\left.\begin{array}{rl} & \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] \ .... \ + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] \\ + & \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] \ .... \ + \left[\frac{\frac{1}{2}(k-1)p}{k}\right] \end{array}\right\} = \tfrac{1}{4}(k-1)(p-1)$$

Demonstr. Supponendo, quod licet, $k < p$, erit minor quam $\frac{\frac{1}{2}(p-1)k}{p}$, sed maior quam $\frac{1}{2}(k-1)$, adeoque $\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = \frac{1}{2}(k-1)$. Hinc patet, theorema praesens ex praec. protinus sequi, statuendo illic $\frac{k}{p} = x$, $\frac{1}{2}(p-1) = n$, adeoque $\frac{1}{2}(k-1) = h$.

Ceterum simili modo demonstrari potest, si k fuerit numerus *par* ad p

primus, fore

$$\left.\begin{array}{rl} & \left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ \ldots.\ +\left[\frac{\frac{1}{2}(p-1)k}{p}\right] \\ + & \left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ \ldots.\ +\left[\frac{\frac{1}{2}kp}{k}\right] \end{array}\right\} = \tfrac{1}{4}k(p-1)$$

At huic propositioni ad institutum nostrum non necessariae non immoramur.

7.

Iam ex combinatione theorematis praec. cum propos. VIII, art. 4. theorema fundamentale protinus demanat. Nimirum denotantibus k, p numeros primos positivos inaequales quoscunque, et ponendo

$$(k,p)+\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ \ldots.\ +\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = L$$
$$(p,k)+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ \ldots.\ +\left[\frac{\frac{1}{2}(k-1)p}{k}\right] = M.$$

per VIII. art. 4. patet, L et M semper fieri numeros pares. At per theorema art. 6. erit

$$L+M=(k,p)+(p,k)+\tfrac{1}{4}(k-1)(p-1)$$

Quoties igitur $\frac{1}{4}(k-1)(p-1)$ par evadit, quod fit, si vel uterque k, p vel saltem alteruter est formae $4n+1$, necessario (k,p) et (p,k) vel ambo pares vel ambo impares esse debent. Quoties autem $\frac{1}{4}(k-1)(p-1)$ impar est, quod evenit, si uterque k, p est formae $4n+3$, necessario alter numerorum (k,p), (p,k) par, alter impar esse debebit. In casu priori itaque relatio ipsius k ad p et relatio ipsius p ad k (quatenus alter alterius residuum vel non-residuum est) identicae erunt, in casu posteriori oppositae.

Q.E.D.