non respicimus), illi t termini, residuorum periodum constituentes omnes erunt diuersi, vti ex demonstratione art. 45 nullo negotio perspicitur. Tum autem propositio art. 46 conuerti potest; scilicet si $a^m \equiv a^n$ (mod. p) erit $m \equiv n$ (mod. t). Si enim m, n secundum modulum t incongrui essent, residua eorum minima, μ, ν diuersa forent. At $a^\mu \equiv a^m$, $a^\nu \equiv a^n$, quare $a^\mu \equiv a^\nu$ i. e. non omnes potestates infra a^t incongrui forent contra hypoth.

Si itaque $a^k \equiv 1$, (mod. p), erit $k \equiv 0$ (mod. t) *i. e.* k per t diuisibilis.

Hactenus de modulis quibuscunque si modo ad a sint primi diximus. Iam modulos qui sunt numeri absolute primi seorsim consideremus atque huic fundamento inuestigationem generaliorem postea superstruamus.

49. Theorema. *Si p est numerus primus ipsum a non metiens, atque a^t infima ipsius a potestas secundum modulum p vnitati congrua, exponens t aut erit $= p - 1$ aut pars aliquota huius numeri.*

Conferantur exempla art. praec.

Demonstr. Quum iam ostensum sit, t esse aut $= p - 1$, aut $< p - 1$, superest, vt in posteriori casu t semper ipsius $p - 1$ partem aliquotam esse euincatur.

I. Colligantur residua minima positiua omnium horum terminorum, $1, a, aa \ldots a^{t-1}$, quae per $\alpha, \alpha', \alpha''$ etc. designentur, ita vt sit $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv aa$ etc. Perspicuum est, haec omnia fore diuersa, si enim duo termini a^m, a^n

eadem praeberent, foret (supponendo $m > n$), $a^{m-n} \equiv 1$ atque $m - n < t$, *Q. E. A.* quum nulla inferior potestas quam a^t vnitati sit congrua, *hyp.* Porro omnes $\alpha, \alpha', \alpha''$ etc. in serie numerorum 1, 2, 3 ... $p - 1$ continentur, quam tamen non exhaurient, quum $t < p - 1$. Complexum omnium $\alpha, \alpha', \alpha''$ etc. per (A) designabimus. Comprehendet igitur (A) terminos t.

II. Accipiatur numerus quicunque β ex his 1, 2, 3 ... $p - 1$, qui in (A) desit. Multiplicetur β per omnes $\alpha, \alpha', \alpha''$ etc., sintque residua minima inde oriunda β, β', β'' etc., quorum numerus etiam erit t. At haec residua tum inter se quam ab omnibus $\alpha, \alpha', \alpha''$ etc. erunt diuersa. Si enim *prior* assertio falsa esset, haberetur $\beta a^m \equiv \beta a^n$ adeoque diuidendo per β, $a^m \equiv a^n$, contra ea quae modo demonstrauimus; si vero *posterior*, haberetur $\beta a^m \equiv a^n$, vnde, quando $m < n$, $\beta \equiv a^{n-m}$ i. e. β alicui ex his $\alpha, \alpha', \alpha''$ etc. congruus contra hyp.; quando vero $m > n$, sequitur multiplicando per a^{t-m}, $\beta a^t \equiv a^{t+n-m}$, siue propter $a^t \equiv 1$, $\beta \equiv a^{t+n-m}$, quae est eadem absurditas. Designetur complexus omnium β, β', β'' etc. quorum multitudo $= t$, per (B), habebunturque iam $2t$ numeri ex his 1, 2, 3 ... $p - 1$. Quodsi igitur (A) et (B) omnes hos numeros complectuntur, fit $\frac{p-1}{2} = t$ adeoque theorema demonstratum.

III. Si vero aliqui adhuc deficiunt, sit horum aliquis γ. Per hunc multiplicentur omnes $\alpha, \alpha', \alpha''$ etc., productorumque residua minima sint $\gamma, \gamma', \gamma''$ etc.; omnium complexus per (C) designetur. (C) igitur comprehendet t numeros ex his 1, 2, 3 ... $p-1$, quae omnes tum inter se quam a numeris in (A) et (B) contentis erunt diuersi. Assertiones priores eodem modo demonstrantur vt in II, tertia ita. Si esset $\gamma a^m \equiv \mathfrak{b} a^n$, fieret $\gamma \equiv \mathfrak{b} a^{n-m}$, aut $\equiv \mathfrak{b} a^{t+n-m}$ prout $m < n$, aut $> n$, in vtroque casu γ alicui ex (B) congrua contra hyp. Habentur igitur $3t$ numeri ex his 1, 2, 3 ... $p-1$, atque si nulli amplius desunt, fiet $t = \frac{p-1}{3}$ adeoque theorema erit demonstratum.

IV. Si vero etiamnum aliqui desunt eodem modo ad quartum numerorum complexum, (D), progrediendum erit etc. Patet vero quoniam numerorum 1, 2, 3.... $p-1$ multitudo est finita, tandem eam exhaustum iri, adeoque multiplum ipsius t fore: quare t erit pars aliquota numeri $p-1$. *Q. E. D.*

50. Quum igitur $\frac{p-1}{t}$ sit integer, sequitur euehendo vtramque partem congruentiae $a^t \equiv 1$ ad potestatem exponentis $\frac{p-1}{t}$, $a^{p-1} \equiv 1$, *siue* $a^{p-1} - 1$ *semper per p diuisibilis est, quando p est primus ipsum a non metiens.*

Theorema hoc quod tum propter elegantiam tum propter eximiam vtilitatem omni attentione dignum, ab inuentore *theorema Fermatianum* appellari solet. Vid. *Fermatii Opera Mathem. Tolosae* 1679 *fol. p.* 163. Demonstrationem inuentor non adiecit, quam tamen in potestate sua esse professus est. Ill. Euler primus demonstrationem publici iuris fecit, in diss. cui titulus *Theorematum quorundam ad numeros primos spectantium demonstratio*, *Comm. Acad. Petrop.* T.