esse vnum e numeris primis a, b, c etc. vel saltem per aliquem eorum diuisibilem (art. 17), ex. gr. per a, de reliquis enim simile est ratiocinium. Metietur itaque t ipsum $\frac{p-1}{a}$; quare productum ABC etc. etiam ad potestatem $\frac{p-1}{a}$ tam eleuatum vnitati erit congruum (art. 46). Sed perspicuum est singulos B, C, etc. (exemto ipso A) ad potestatem $\frac{p-1}{a}$ tam eleuatos vnitati congruos fieri, quum exponentes $b^{\mathfrak{G}}$, c^{γ}, etc. ad quos singuli pertinent ipsum $\frac{p-1}{a}$ metiantur. Hinc erit $A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}}$ etc. $\equiv A^{\frac{p-1}{a}} \equiv 1$. Vnde sequitur exponentem ad quem A pertinet ipsum $\frac{p-1}{a}$ metiri debere (art. 48), i. e. $\frac{p-1}{a^{\alpha+1}}$ esse integrum; at $\frac{p-1}{a^{\alpha+1}} = \frac{b^{\mathfrak{G}} c^{\gamma} \text{ etc.}}{a}$ integer esse nequit (art. 15). Vnde tandem concludere oportet, suppositionem nostram consistere non posse, i. e. productum ABC etc. reuera ad exponentem $p-1$ pertinere. *Q. E. D.*

Demonstratio posterior priori aliquantulum prolixior esse videtur, prior contra posteriori minus directa.

56. Hoc theorema insigne exemplum suppeditat, quanta circumspectione in theoria numerorum saepenumero opus sit, ne, quae non sunt, pro certis assumamus. Celeb. Lambert in diss. iam supra laudata *Acta Erudit.* 1769 p. 127 huius propositionis mentionem facit seddemonstrationis ne necessitatem quidem attigit. Nemo vero demonstrationem tentauit praeter summum Eulerum *Comment. nou. Ac. Petrop. T. XVIII* ad annum

1773 *Demonstrationes circa residua ex diuisione potestatum per numeros primos resultantia* p. 85 seqq. vid. imprimis art. 37 vbi de demonstrationis necessitate fusius locutus est. At demonstratio quam Vir sagacissimus exhibuit duos defectus habet. Alterum quod art. 31 et sqq. tacite supponit, congruentiam $x^n \equiv 1$ (translatis ratiociniis illic adhibitis in nostra signa) reuera n radices diuersas habere, quamquam ante nihil aliud fuerit demonstratum quam quod *plures* habere nequeat; alterum, quod formulam art. 34 per inductionem tantummodo deduxit.

57. Numeros ad exponentem $p-1$ pertinentes *radices primitiuas* cum ill. Eulero vocabimus. Si igitur a est radix primitiua, potestatum a, aa, a^3 ... a^{p-1} residua minima omnia erunt diuersa; vnde facile deducitur, inter haec omnes numeros 1, 2, 3, ... $p-1$, qui totidem sunt multitudine quot illa residua minima, reperiri debere, *i. e.* quemuis numerum per p non diuisibilem potestati alicui ipsius a congruum esse. Insignis haec proprietas permagnae est vtilitatis, operationesque arithmeticas, ad congruentias pertinentes, haud parum subleuare potest, simili fere modo, vt logarithmorum introductio operationes arithmeticae vulgaris. Radicem aliquam primitiuam, a, ad lubitum pro *basi* adoptabimus, ad quam omnes numeros per p non diuisibiles referemus, et si fuerit $a^e \equiv b$ (mod. p), e ipsius b *indicem* vocabimus. Ex. gr. si pro modulo 19, radix primitiua 2 pro basi assumatur respondebunt

numeris	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.
indices	0.	1.	13.	2.	16.	14.	6.	3.	8.	17.	12.	15.	5.	7.	11.	4.	10.	9.

Ceterum patet, manente basi, cuique numero plures indices conuenire, sed hos omnes secundum modulum $p - 1$ fore congruos; quamobrem quoties de indicibus sermo erit, qui secundum modulum $p - 1$ sunt congrui pro aequiualentibus habebuntur, simili modo vti numeri ipsi, quando secundum modulum p sunt congrui, tamquam aequiualentes spectantur.

58. Theoremata ad indices pertinentia prorsus analoga sunt iis quae ad logarithmos spectant.

Index producti e quotcunque factoribus conflati congruus est summae indicum singulorum factorum secundum modulum $p - 1$.

Index potestatis numeri alicuius congruus est producto ex indice numeri dati in exponentem potestatis, secundum mod. $p - 1$.

Demonstrationes propter facilitatem omittimus.

Hinc perspicitur si tabulam construere velimus ex qua omnium numerorum indices pro modulis diuersis desumi possint, ex hac tum omnes numeros modulo maiores, tum omnes compositos omitti posse. Specimen huius modi tabulae ad calcem operis huius adiectum est, *Tab. I*, vbi in prima columna verticali positi sunt numeri primi primorumque potestates a 3 vsque ad 97, qui tamquam moduli sunt spectandi, iuxta hos singulos numeri pro basi as-