VIII *). Innititur ista euolutioni potestatis $(a+1)^p$, vbi ex coefficientium forma facillime deducitur $(a+1)^p - a^p - 1$ semper per p fore diuisibilem, adeoque $(a+1)^p - (a+1)$ per p diuisibilem fore, quando $a^p - a$ per p sit diuisibilis. Iam quia $1^p - 1$ semper per p diuisibilis est, etiam $2^p - 2$ semper erit; hinc etiam $3^p - 3$ etc. generaliterque $a^p - a$. Quodsi itaque p ipsum a non metitur, etiam $a^{p-1} - 1$ per p diuisibilis erit. Haec sufficient ad methodi indolem declarandam. Clar. Lambert similem demonstrationem tradidit in *Actis Erudit.* 1769. *p.* 109. Quia vero euolutio potestatis binomii a theoria numerorum satis aliena esse videbatur, aliam demonstrationem ill. Euler inuestigauit quae exstat *Comment. nou. Petr. T. VII. p.* 70, atque cum ea quam nos art. praec. exposuimus prorsus conuenit. In sequentibus adhuc aliae quaedam se nobis offerent. Hoc loco vnam superaddere liceat, quae similibus principiis innititur, vti prima ill. Euleri. Propositio sequens, cuius casus tantum particularis est theorema nostrum, etiam ad alias inuestigationes infra adhibebitur.

Polynomii $a+b+c+$ *etc. potestas* p *ta secundum modulum* p *est* $\equiv a^p + b^p + c^p +$ *etc., siquidem* p *est numerus primus.*

*) In comment. anteriore vir summus ad scopum nondum peruenerat. *Com. Petr.* T. VI. p. 106. — In controuersia famosa inter Maupertuis et König, a principio actionis minimae orta, sed mox ad res heterogeneas egressa, König in manibus se habere dixit autographum Leibnitianum, in quo demonstratio huius theorematis cum Euleriana prorsus conspirans contineatur. *Appel au public.* p. 106. Licet vero fidem huic testimonio denegare nolimus, certe Leibnitius inuentum suum numquam publicauit. Conf. *Hist. de l'Ac. de Prusse. A.* 1750. *p.* 530.

Demonstr. Constat potestatem p^{tam} polynomii $a + b + c +$ etc. esse compositam e partibus formae $\varkappa a^{\alpha} b^{\beta} c^{\gamma}$ etc. vbi $\alpha + \beta + \gamma$ etc. $= p$, et $\varkappa$ designat, quot modis p res, quarum α, β, γ etc. respectiue sunt $= a$, b, c etc. permutari possint. At supra art. 41 ostendimus, hunc numerum semper esse per p diuisibilem, nisi omnes res sint aequales, i. e. nisi aliquis numerorum α, β, γ etc. sit $= p$ reliqui vero $= 0$. Vnde sequitur omnes ipsius $(a + b + c +$ etc.$)^p$ partes, praeter has a^p, b^p, c^p etc., per p diuisibiles esse; quae igitur quando de congruentia secundum modulum p agitur, tuto omitti poterunt, fietque $(a + b + c +$ etc.$)^p \equiv a^p + b^p + c^p +$ etc. *Q. E. D.*

Quodsi iam omnes quantitates a, b, c etc. $= 1$ ponuntur, numerusque earum $= k$, fiet $k^p \equiv k$ vti in art. praec.

52. Quoniam igitur alii numeri quam qui sunt diuisores ipsius $p - 1$ nequeunt esse exponentes potestatum infimarum ad quas euecti numeri aliqui vnitati congrui fiunt, quaestio sese offert, num omnes ipsius $p - 1$ diuisores ad hoc sint idonei, atque, quando omnes numeri per p non diuisibiles secundum exponentem infimae suae potestatis vnitati congruae classificentur, quot ad singulos exponentes sint peruenturi. Vbi statim observare conuenit, sufficere, si omnes numeri positiui ab 1 vsque ad $p - 1$ considerentur; manifestum enim est, numeros congruos ad eandem potestatem eleuari debere, quo vnitati fiant congruae, adeoque numerum quemcunque ad eundem exponentem esse referendum ad quem residuum suum mi-

nimum positiuum. Quocira in id nobis erit incumbendum, vt quomodo hoc respectu numari 1, 2, 3 .... $p-1$ inter singulos $p-1$ factores distribuendi sint eruamus. Breuitatis gratia, si d est vnus e diuisoribus numeri $p-1$ (ad quos etiam 1 et $p-1$ referendi), per ψd designabimus multitudinem numerorum positiuorum ipso p minorum quorum potestas d^{te} est infima vnitati congrua.

53. Quo facilius haec disquisitio intelligi possit, exemplum apponimus. Pro $p=19$ distribuentur numeri 1, 2, 3 .... 18 inter diuisores numeri 18 hoc modo:

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

In hoc igitur casu fit $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. Vbi exigua attentio docet, totidem ad quemuis exponentem pertinere, quot dentur numeri hoc non maiores ad ipsumque primi, siue esse in hoc certe casu, retento signo art. 40, $\psi d = \varphi d$. Hanc autem obseruationem generaliter veram esse ita demonstramus.

I. Si numerus aliquis habetur, a, ad exponentem d *pertinens* (*i. e.* cuius potestas d^{ta} vnitati congrua, omnes inferiores incongruae), omnes huius potestates, aa, a^3, a^4 .... a^d siue ipsarum residua minima proprietatem priorem etiam possidebunt (vt potestas ipsarum d^{ta} vnitati sit congrua) et quum hoc ita etiam expri-