44. Quamuis hic supposuerimus, modulum $p$ non metiri coefficientem termini summi, tamen theorema ad hunc casum non restringitur. Si enim primus coefficiens siue etiam aliqui sequentium per $p$ diuisibiles essent, hi termini tuto reiici possent, congruentiaque tandem ad inferiorem gradum deprimeretur, vbi coefficiens primus per $p$ non amplius foret diuisibilis, siquidem non omnes coefficientes per $p$ diuidi possunt; in quo casu, congruentia foret, identica atque incognita prorsus indeterminata.

Theorema hoc primum ab ill. La Grange propositum atque demonstratum est (*Mem. de l'Ac. de Berlin, Année* 1768 *p.* 192.). Exstat etiam in dissert. ill. Le Gendre, *Recherches d'Analyse indeterminée, Hist. de l'Acad. de Paris* 1785. *p.* 466. Ill. Euler in *Nou. Comm. Ac. Petr. XVIII. p.* 93 demonstrauit congruentiam $x^n - 1 \equiv 0$ plures quam $n$ radices diuersas habere non posse. Quae quamuis sit particularis, tamen methodus qua vir summus vsus est omnibus congruentiis facile adaptari potest. Casum adhuc magis limitatum iam antea absoluerat, Comm. Ac. Petr. V. p. 6, sed haec methodus generaliter adhiberi nequit. Infra Sect. VIII, alio adhuc modo theorema demonstrabimus; at quantumuis diuersae primo aspectu omnes hae methodi videri possint, periti qui comparare eas voluerint facile certiores fient omnes eidem principio superstructas esse. Ceterum quum hoc theorema hic tantum tamquam lemma sit considerandum, neque completa expositio huc pertineat: de modulis compositis seorsim agere supersedemus.

## Sectio Tertia

### de

# RESIDVIS POTESTATVM.

45. Theorema. *In omni progressione geometrica*, 1, $a$, $aa$, $a^3$ *etc. praeter primum* 1, *alius adhuc datur terminus*, $a^t$, *secundum modulum* $p$ *ad* $a$ *primum vnitati congruus, cuius exponens* $t < p$.

*Demonstr.* Quoniam modulus $p$ ad $a$, adeoque ad quamuis ipsius $a$ potestatem est primus, nullus progressionis terminus erit $\equiv 0 \pmod{p}$, sed quiuis alicui ex his numeris $1, 2, 3 \ldots p-1$ congruus. Quorum multitudo quum sit $p-1$, manifestum est, si plures quam $p-1$ progressionis termini considerentur, omnes residua minima diuersa habere non posse. Quocirca inter terminos $1$, $a$, $aa$, $a^3 \ldots a^{p-1}$ bini ad minimum congrui inuenientur. Sit itaque $a^m \equiv a^n$ et $m > n$, fietque diuidendo per $a^n$, $a^{m-n} \equiv 1$ (art. 22) vbi $m-n < p$, et $> 0$. *Q. E. D.*

*Ex.* In progressione 1, 2, 4, 8 etc. terminus primus qui secundum modulum 13 vnitati

est congruus, inuenitur $2^{12} = 4096$. At secundum modulum 23 in eadem progressione fit $2^{11} = 2048 \equiv 1$. Similiter numeri 5 potestas sexta, 15625, vnitati congrua secundum modulum 7, quinta vero, 3125, secundum 11. In aliis igitur casibus potestas exponentis minoris quam $p - 1$ vnitati congrua euadit, in aliis contra vsque ad potestatem $p - 1$ tam ascendere necesse est.

46. Quando progressio vltra terminum qui vnitati est congruus continuatur, eadem quae ab initio habebantur residua prodeunt iterum. Scilicet si $a^t \equiv 1$, erit $a^{t+1} \equiv a$, $a^{t+2} \equiv aa$ etc. donec ad terminum $a^{2t}$ perueniatur, cuius residuum minimum iterum erit $\equiv 1$, atque residuorum *periodum* denuo inchoat. Habetur itaque periodus $t$ residua comprehendens, quae simulac finita est ab initio semper repetitur; neque alia residua quam quae in hac periodo continentur in tota progressione occurrere possunt. Generaliter erit $a^{mt} \equiv 1$, et $a^{mt+n} \equiv a^n$, id quod per designationem nostram ita exhibetur:

*Si* $r \equiv s \pmod{t}$ *erit*

$a^r \equiv a^s \pmod{p}$

47. Petitur ex hoc theoremate compendium potestatum quantumuis magno exponente affectarum residua expedite inueniendi, simulac potestas vnitati congrua innotescat. Si ex. gr. residuum e diuisione potestatis $3^{1000}$ per 13 oriundum quaeritur, erit propter $3^3 \equiv 1 \pmod{13}$, $t \equiv 3$; quare quum sit $1000 \equiv 1 \pmod{3}$, erit $3^{1000} \equiv 3 \pmod{13}$.

48. Quando $a^t$ est *infima* potestas vnitati congrua (praeter $a^0 = 1$, ad quem casum hic