74. Per exemplum praecepta haec clariora fient. Sit $p = 73$, pro quo radix primitiua quaeratur. Tentemus primo numerum 2, cuius periodus prodit haec:

1. 2. 4. 8. 16. 32. 64. 55. 37. 1. etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. etc.

Quum igitur iam potestas exponentis 9 vnitati congrua fiat, 2 non est radix primitiua. Tentetur alius numerus in periodo ipsius 2 non occurrens ex. gr. 3, cuius periodus est haec:

1. 3. 9. 27. 8. 24. 72. 70. 64. 46. 65. 49. 1 etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12 etc.

Quare neque 3 est radix primitiua. Exponentium autem ad quos 2, 3 pertinent, (i. e. numerorum 9, 12) diuiduus communis minimus est 36, qui in factores 9 et 4 ad praecepta art. praec. resoluitur. Euehendus itaque 2 ad potestatem exponentis $\frac{9}{9}$, i. e. numerus 2 ipse retinendus; 3 autem ad potestatem exponentis 3: productum ex his est 54, quod itaque ad exponentem 36 pertinebit. Si denique ipsius 54 periodus computatur numerusque in hac non contentus ex. gr. 5 denuo tentatur, hunc esse radicem primitiuam, reperietur.

75. Antequam hoc argumentum deseramus, propositiones quasdam trademus, quae ob simplicitatem suam attentione haud indignae videntur.

Productum ex omnibus terminis periodi numeri cuiusuis est $\equiv 1$, *quando ipsorum multitudo, siue exponens ad quem numerus pertinet, est impar, et* $\equiv -1$, *quando ille exponens est par.*

Ex. Pro modulo 13, periodus numeri 5 constat ex his terminis, 1, 5, 12, 8 quorum productum $480 \equiv -1 \pmod{13}$.

Secundum eundem modulum periodus numeri 3 constat e terminis 1, 3, 9 quorum productum $27 \equiv 1 \pmod{13}$.

Demonstr. Sit exponens, ad quem numerus pertinet, t, atque index numeri, $\frac{p-1}{t}$, id quod si basis rite determinatur semper fieri potest (art. 71). Tum index producti ex omnibus periodi terminis erit $\equiv (1 + 2 + 3 + \text{etc.} + t - 1) \frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$ i. e. $\equiv 0 \pmod{p-1}$ quando t impar, et $\equiv \frac{p-1}{2}$, quando t par; hinc in priori casu productum illud $\equiv 1 \pmod{p}$; in posteriori vero $\equiv -1 \pmod{p}$, (art. 62). *Q. E. D.*

76. Si numerus iste in theor. praecedente est radix primitiua, eius periodus omnes numeros $1, 2, 3, \ldots\ldots p-1$ comprehendet, quorum productum itaque semper $\equiv -1$ (namque $p-1$ semper par, vnico casu $p=2$ excepto in quo -1 et $+1$ aequiualent). Theorema hoc elegans quod ita enunciari solet: *productum ex omnibus numeris numero primo dato minoribus, vnitate auctum per hunc primum est diuisibiles*, primum a cel. Waring est prolatum armigeroque Wilson adscriptum, *Meditt. algebr. Ed.* 3, *p.* 380. Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla *notatio* fingi possit, quae numerum primum exprimat. — At nostro quidem iudi-

cio huiusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. Postea ill. La Grange demonstrationem dedit, *Nouv. Mem. de l'Ac. de Berlin*, 1771. Innititur ea considerationi coefficientium ex euolutione producti $x+1$. $x+2$. $x+3$ .... $x+p-1$ oriundarum. Scilicet posito hoc producto $= x^{p-1} + Ax^{p-2} + Bx^{p-3} +$ etc. $+ Mx + N$, coefficientes A, B, *etc.*, M per p erunt diuisibiles, N vero erit $= 1.2.3 .... p-1$. Iam pro $x = 1$, productum per p diuisibile; tunc autem erit $\equiv 1 + N \pmod{p}$; quare necessario $1 + N$ per p diuidi poterit.

Denique ill. Euler in *Opusc. analyt. T. I. p.* 329 demonstrationem dedit, cum ea quam nos hic exposuimus conspirantem. Quodsi tales viri theorema hoc meditationibus suis non indignum censuerunt, non improbatum iri speramus, si aliam adhuc demonstrationem apponimus.

77. Quando secundum modulum p, productum duorum numerorum a, b vnitati est congruum, numeros a, b cum ill. Euler, *socios* vocemus. Tum secundum sect. praec. quiuis numerus positiuus ipso p minor socium habebit positiuum ipso p minorem et quidem vnicum. Facile autem probari potest ex numeris $1, 2, 3 .... p-1$; 1 et $p-1$ esse vnicos qui sibi ipsis sint socii: numeri enim sibi ipsis socii, radices erunt congruentiae $xx \equiv 1$; quae quoniam est secundi gradus plures quam duas radices, i. e. alias quam 1 et $p-1$ habe-