Vnde sequitur haec producta loco ipsarum radicum primitiuarum accipi posse. At quoniam in his productis omnes valores ipsius A cum omnibus ipsius B etc. combinari oportet, omnium horum productorum summa aequalis est producto ex summa omnium valorum ipsius A, in summam omnium valorum ipsius B, in summam omnium valorum ipsius C etc. vti ex doctrina combinationum notum est. Designentur omnes valores ipsorum A; B etc., per A, A', A'' etc.; B, B', B'' etc. etc., eritque summa omnium radicum primitiuarum $\equiv (A + A' +$ etc.) $(B + B' +$ etc.) etc. Iam dico, si exponens α fuerit $= 1$, summam $A + A' + A'' +$ etc. fore $\equiv -1 \pmod{p}$, si vero α fuerit > 1, summam hanc fore $\equiv 0$. similiterque de reliquis $\mathfrak{C}, \gamma$ etc. Simulac haec erunt demonstrata, theorematis nostri veritas manifesta erit. Quando enim $p - 1$ per quadratum aliquod diuisibilis est, aliquis exponentium $\alpha, \mathfrak{C}, \gamma$ etc. vnitatem superabit, adeoque aliquis factorum, quorum producto congrua est summa omnium radicum primitiuarum, erit $\equiv 0$, et proin etiam productum ipsum: quando vero $p - 1$ per nullum quadratum diuidi potest, omnes exponentes $\alpha, \mathfrak{C}, \gamma$ etc. erunt $= 1$, vnde summa omnium radicum primitiuarum congrua erit producto ex tot factoribus, quorum quisque $\equiv -1$, quot habentur numeri a, b, c etc., adeoque erit $\equiv \pm 1$, prout horum numerorum multitudo par vel impar. Illa autem ita probantur.

1°. Quando $\alpha = 1$ atque A numerus ad exponentem a pertinens, reliqui numeri ad hunc

exponentem pertinentes erunt A^2, A^3 .... A^{a-1}. At $1 + A + A^2 + A^3 .... + A^{a-1}$ est summa periodi completae, adeoque $\equiv 0$ (art. 79), quare $A + A^2 + A^3 .... + A^{a-1} \equiv -1$.

2°. Quando autem $\alpha > 1$, atque A numerus ad exponentem a^α pertinens, reliqui numeri ad hunc exponentem pertinentes habebuntur, si ex his A^2, A^3, A^4 .... $A^{a^\alpha-1}$ reiiciuntur A^a, A^{2a}, A^{3a} etc., vid. art. 53; quare summa eorum erit $\equiv 1 + A + A^2 .... + A^{a^\alpha-1} - (1 + A^a + A^{2a} .... + A^{a^\alpha-a})$ i. e. congrua differentiae duarum periodorum, adeoque $\equiv 0$. *Q. E. D.*

82. Omnia quae hactenus exposuimus innituntur suppositioni, modulum esse numerum primum. Superest vt eum quoque casum consideremus, vbi pro modulo assumitur numerus compositus. Attamen quum hic neque proprietates tam elegantes eniteant, quam in casu priori, neque ad eas inueniendas artificiis subtilibus sit opus, sed potius omnia fere per solam principiorum praecedentium applicationem erui possint, omnes minutias hic exhaurire superfluum atque taediosum foret. Breuiter itaque quae huic casui cum priori sint communia quaeque propria exponemus.

83. Propositiones art. 45 — 48 generaliter iam sunt demonstratae. At prop. art. 49 ita immutari debet:

Si f designat, quot numeri dentur ad m primi simulipso m minores, i. e. si $f = \varphi m$ (art. 38): exponens, t, infimae potestatis numeri dati, a, ad m primi, quae secundum modulum m vnitati est congrua, vel erit $= f$ vel pars aliquota huius numeri.