re nequit. Abiectis itaque his numerorum reliquorum 2, 3 .... $p-2$ bini semper erunt associati; quare productum ex ipsis erit $\equiv 1$ adeoque productum ex omnibus 1, 2, 3 ... $p-1$, $\equiv p-1$ siue $\equiv -1$. *Q. E. D.*

Ex. gr. pro $p=13$ numeri 2, 3, 4 .... 11 ita associantur: 2 cum 7; 3 cum 9; 4 cum 10; 5 cum 8; 6 cum 11; scilicet $2.7\equiv 1$; $3.9\equiv 1$ etc. Hinc $2.3.4 \ldots 11 \equiv 1$; adeoque $1.2.3 \ldots 12 \equiv -1$.

78. Potest autem theorema Wilsonianum generalius sic proponi. *Productum ex omnibus numeris, numero* quocunque *dato A minoribus simulque ad ipsum primis, congruum est secundum A, vnitati vel negatiue vel positiue sumtae.* Negatiue sumenda est vnitas, quando A est formae p^m, aut huiusce, $2p^m$, designante p numerum primum a 2 diuersum, insuperque quando $A=4$; positiue autem in omnibus casibus reliquis. Theorema, quale a cel. Wilson est prolatum, sub casu priori continetur. — Ex. gr. pro $A=15$ productum e numeris 1, 2, 4, 7, 8, 11, 13, 14 est $\equiv 1$ (mod. 15). Demonstrationem breuitatis gratia non adiungimus: obseruamus tantum, eam simili modo perfici posse vt in art. praec., excepto quod congruentia $xx\equiv 1$ plures quam duas radices habere potest, quae considerationes quasdam peculiares postulant. Posset etiam demonstratio ex consideratione indicum peti, similiter vt in art. 75, si ea quae mox de modulis non primis trademus conferantur.

79. Reuertimur ad enumerationem aliarum propositionum (art. 75).

Summa omnium terminorum periodi numeri cuiusuis est $\equiv o$, vti in ex art. 75, $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$.

Dem. Numerus de cuius periodo agitur, sit $= a$, atque exponens ad quem pertinet, $= t$, eritque summa terminorum omnium periodi, $\equiv 1 + a + aa + a^3 + \text{etc.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}$. At $a^t - 1 \equiv 0$: quare summa haec semper erit $\equiv 0$ (art. 22), nisi forte $a - 1$ per p sit diuisibilis, siue $a \equiv 1$; hunc igitur casum excipere oportet, si vel vnum terminum, *periodum* vocare velimus.

80. *Productum ex omnibus radicibus primitiuis est* $\equiv 1$, excepto vnico casu, $p = 3$; tum enim vna tantum datur radix prima, 2.

Demonstr. Si radix primitiua quaecunque pro basi assumitur, indices radicum omnium primitiuarum erunt numeri ad $p - 1$ primi simulque ipso minores. At horum numerorum summa, i. e. index producti ex omnibus radicibus primitiuis, est $\equiv 0 \pmod{p - 1}$ adeoque productum $\equiv 1 \pmod{p}$; facile enim perspicitur, si k fuerit numerus ad $p - 1$ primus, etiam $p - 1 - k$ ad $p - 1$ primum fore adeoque binos numeros ad $p - 1$ primos summam constituere per $p - 1$ diuisibilem; (k autem ipsi $p - 1 - k$ numquam aequalis esse potest, praeter casum, $p - 1 = 2$, siue $p = 3$, quem exce-

pimus; manifesto enim $\frac{p-1}{2}$ in omnibus reliquis casibus ad $p-1$ non est primus).

81. *Summa omnium radicum primitiuarum est aut* $\equiv 0$ (quando $p-1$ per *quadratum* aliquod est diuisibilis), *aut* $\equiv \pm 1$ (*mod.* p), (quando $p-1$ est productum e numeris primis inaequalibus; quorum multitudo si est par signum positiuum, si vero impar, negatiuum sumendum).

Ex. 1° pro $p=13$, habentur radices primitiuae 2, 6, 7, 11, quarum summa $26 \equiv 0$ (mod. 13). 2° pro $p=11$, radices primitiuae sunt 2, 6, 7, 8 quarum summa $23 \equiv +1$ (mod. 11). 3° pro $p=31$, radices primitiuae sunt 3, 11, 12, 13, 17, 21, 22, 24, quarum summa, $123 \equiv -1$ (mod. 31).

Demonstr. Supra demonstrauimus (art. 55, II), si p fuerit $= a^\alpha b^\beta c^\gamma$ etc. (designantibus a, b, c etc. numeros primos inaequales) atque A, B, C numeri quicunque ad exponentes a^α, b^β, c^γ etc. respectiue pertinentes, omnia producta ABC etc. exhibere radices primitiuas. Facile vero etiam demonstrari potest, quamuis radicem primitiuam per huiusmodi productum exhiberi posse et quidem vnico tantum modo *).

*) Determinentur scilicet numeri $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. ita, vt sit $\mathfrak{a} \equiv 1$ (mod. a^α) et $\equiv 0$ (mod. $b^\beta c^\gamma$ etc.); $\mathfrak{b} \equiv 1$ (mod. b^β) et $\equiv 0$ (mod. $a^\alpha c^\gamma$ etc.) etc. (vid. art. 32), vnde fiet $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} +$ etc. $\equiv 1$ (mod. $p-1$), (art. 19). Iam si radix primitiua quaecunque r, per productum ABC etc. exhiberi debet accipiatur $A \equiv r\mathfrak{a}$, $B \equiv r\mathfrak{b}$, $C \equiv r\mathfrak{c}$ etc., atque pertinebunt A ad exponentem a^α, B ad exponentem b^β etc.; productumque ex omnibus A, B, C etc. erit $\equiv r$ (mod. p); denique facile perspicitur A, B, C etc, alio modo determinari non posse.