Demonstratio prop. art. 49 etiam pro hoc casu valere potest, si modo vbique loco ipsius p, m, loco ipsius $p-1$, f, et loco numerorum $1, 2, 3, \ldots p-1$, numeri ad m primi simulque ipso m minores substituantur. Huc itaque lectorem ablegamus. Ceterum demonstrationes reliquae de quibus illic locuti sumus (art. 50, 51) non sine multis ambagibus ad hunc casum applicari possunt. — At respectu propositionum sequentium, art. 52 *sqq.* magna differentia incipit inter modulos, qui numerorum primorum sunt potestates, eosque, qui per plures numeros primos diuidi possunt. Seorsim itaque modulos prioris generis contemplabimur.

84. Si modulus $m = p^n$, designante p numerum primum, erit $f = p^{n-1}(p-1)$ (art. 38.) Iam si disquisitiones in artt. 51, 55 contentae ad hunc casum applicantur, mutatis mutandis vti in art. praec. praescripsimus, inuenietur, omnia quae ibi demonstrata sunt etiam pro hoc casu locum habere, si modo ante probatum esset, congruentiam, formae $x^t - 1 \equiv 0$ (mod. p^n) plures quam t radices diuersas habere non posse. Pro modulo primo hanc veritatem ex propositione generaliori art. 43 deduximus, quae autem in omni sua extensione de modulis primis tantummodo valet, neque adeo ad hunc casum applicanda. Attamen propositionem pro hoc casu particulari veram esse per methodum singularem demonstrabimus. Infra (sect. VIII.) idem facilius inuenire docebimus.

Demonstrandum proponimus nobis hoc theorema: *Si numerorum t et* $p^{n-1}(p-1)$ *diuisor communis maximus est e, congruentia* $x^t \equiv 1 \pmod{p^n}$ *habebit e radices diuersas.*

Sit $e = kp^\nu$ ita vt k factorem p non inuoluat, adeoque numerum $p-1$ metiatur. Tum congruentia $x^t \equiv 1$ secundum modulum p habebit k radices diuersas, quibus per A, B, C etc. designatis, radix quaecunque eiusdem congruentiae secundum modulum p^n, congrua esse debet secundum modulum p alicui numerorum A, B, C etc. Iam demonstrabimus, congruentiam $x \equiv 1 \pmod{p^n}$ habere p^ν radices ipsi A, totidem ipsi B etc. congruas secundum modulum p. Quo facto omnium radicum numerus erit kp^ν siue e, vti diximus. Illam vero demonstrationem ita adornabimus, vt *primo* ostendamus, si α fuerit radix ipsi A secundum modulum p congrua, etiam $\alpha + p^{n-\nu}$, $\alpha + 2p^{n-\nu}$, $\alpha + 3p^{n-\nu}$, ... $\alpha + (p^\nu - 1)\,p^{n-\nu}$ fore radices; *secundo*, numeros ipsi A secundum modulum p congruos alios quam qui in forma $\alpha + hp^{n-\nu}$ sint comprehensi (denotante h integrum quemcunque), radices esse non posse: vnde manifesto p^ν radices diuersae habebuntur, et non plures: atque idem etiam de radicibus, quae singulis B, C etc. sunt congruae, locum habebit: *tertio* docebimus, quomodo semper radix, ipsi A secundum p congrua, inueniri possit.

86. Theorema. *Si vti in art. praec. t est numerus per* p^ν, *neque vero per* $p^{\nu+1}$ *diuisibilis, erit* $(\alpha +$

$hp^\mu)^t - \alpha^t \equiv o \pmod{p^{\mu+\nu}}$, at $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$ Theorematis pars posterior locum non habet, quando $p = 2$ simulque $\mu = 1$.

Demonstratio huius theorematis ex euolutione potestatis binomii peti posset, si ostenderetur omnes terminos post secundum per $p^{\mu+\nu+1}$ diuisibiles esse. Sed quoniam consideratio denominatorum coefficientium in aliquot ambages deducit, methodum sequentem praeferimus.

Ponamus *primo* $\mu > 1$ atque $\nu = 1$, eritque, propter $x^t - y^t = (x - y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{etc.} + y^{t-1})$, $(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha$ etc. $+ \alpha^{t-1})$. At est $\alpha + hp^\mu \equiv \alpha \pmod{p^2}$, quare quisque terminus $(\alpha + hp^\mu)^{t-1}$, $(\alpha + h^\mu)^{t-2}\alpha$ etc. erit $\equiv \alpha^{t-1} \pmod{p^2}$ adeoque omnium summa $\equiv t\,\alpha^{t-1} \pmod{p^2}$ siue formae $t\,\alpha^{t-1} + V p^2$ denotante V numerum quemcunque. Hinc $(\alpha + hp^\mu)^t - \alpha^t$ erit formae $\alpha^{t-1} hp^\mu t + Vhp^{\mu+2}$, i. e. $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+}}$ et $\equiv o \pmod{p^{\mu+1}}$ Pro hoc itaque casu theorema est demonstratum.

Iam si theorema pro aliis ipsius ν valoribus verum non esset, manente etiamnum $\mu > 1$, limes aliquis necessario daretur, vsque ad quem theorema semper verum foret, vltra vero falsum. Sit minimus valor ipsius ν, pro quo falsum est $= \varphi$, vnde facile perspicitur, si t per $p^{\varphi-1}$ non autem per p^φ fuerit diuisibi-