lis, theorema adhuc verum esse, at si loco ipsius t substituatur tp, falsum. Habemus itaque

$$(\alpha + hp^\mu)^t \equiv \alpha^t + \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\varphi}}$$

siue $= \alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varphi}$ denotante u numerum indeterminatum. At quia pro $\nu = 1$ theorema iam est demonstratum, erit $(\alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1} hp^{\mu+1} t + \alpha^{tp-t} up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$,

adeoque etiam

$(\alpha + hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1} hp^\mu tp \pmod{p^{\mu+\varphi+1}}$ i. e. theorema etiam verum, si loco ipsius t substituitur tp, i. e. etiam pro $\nu = \varphi + 1$, contra hypothesin. Vnde manifestum pro omnibus ipsius ν valoribus theorema verum esse.

87. Superest casus vbi $\mu = 1$. Per methodum prorsus similem ei qua in art. praec. vsi sumus, sine adiumento theorematis binomialis demonstrari potest, esse

$$(\alpha + hp)^{t-1} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-1)\,hp \pmod{p^2}$$
$$\alpha\,(\alpha + hp)^{t-2} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-2)\,hp$$
$$\alpha\alpha\,(\alpha + hp)^{t-3} \equiv \alpha^{t-1} + \alpha^{t-2}\,(t-3)\,hp$$

etc.

vnde aggregatum erit (quia partium multitudo $= t$)

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\,\alpha^{t-2} hp \pmod{p^2}$$

At quoniam t per p diuisibilis, etiam $\frac{(t-1)t}{2}$ per p diuisibilis erit in omnibus casibus excepto eo vbi $p = 2$ de quo iam in art.

praec. monuimus. In reliquis autem casibus erit $\frac{(t-1)t}{2} \alpha^{t-2} hp \equiv 0 \pmod{p^2}$, adeoque etiam illud aggregatum $\equiv t\alpha^{t-2} \pmod{p^2}$ vt in art. praec. In reliquis demonstratio hic eodem modo procedit vt istic.

Colligimus igitur generaliter vnico casu $p = 2$ excepto, esse
$(\alpha + hp^\mu)^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$ et
$(\alpha + hp^\mu)^t$ *non* $\equiv \alpha^t$ pro quouis modulo quisit altior potestas ipsius p, quam haec, $p^{\mu+\nu}$, quoties quidem h per p non est diuisibilis, atque p^ν potestas suprema ipsius p quae numerum t diuidit.

Hinc protinus deriuantur propositiones 1. et 2. quas art. 85 demonstrandas nobis proposueramus: scilicet

primo, si $\alpha^t \equiv 1$, erit etiam $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

secundo si numerus aliquis α' ipsi A adeoque etiam ipsi α secundum modulum p congruus, neque vero huic secundum modulum $p^{n-\nu}$, congruentiae $x^t \equiv 1 \pmod{p^n}$ satisfaceret, ponamus α' esse $= \alpha + lp^\lambda$, ita vt l per p non sit diuisibilis, eritque $\lambda < \mu - \nu$, tunc autem $(\alpha + lp^\lambda)^t$ secundum modulum $p^{\lambda+\nu}$ ipsi α^t congruus erit, non autem secundum modulum p^μ, quae est altior potestas, quare α' radix congruentiae $x^t \equiv 1$ esse nequit.

88. *Tertium* vero fuit radicem aliquam congruentiae $x^t \equiv 1 \pmod{p_n}$, ipsi A con-

gruam, inuenire. Ostendemus hic tantummodo quomodo hoc fieri possit, si iam radix eiusdem congruentiae secundum modulum p^{n-1} innotuerit; manifesto hoc sufficit, quum a modulo p pro quo A est radix, ad modulum p^2, sicque deinceps ad omnes potestates consecutiuas progredi possimus.

Esto itaque α radix congruentiae $x^t \equiv 1 \pmod{p^{n-1}}$ quaeriturque radix eiusdem congruentiae secundum modulum p^n, ponatur haec $= \alpha + hp^{n-\nu-1}$, quam formam eam habere debere ex art. praec. sequitur (casum vbi $\nu = n-1$ postea seorsim considerabimus: maior vero quam $n-1$, ν esse nequit). Debet itaque esse $(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^n}$. At $(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$ Si itaque h ita demerminatur, vt fiat $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1} \pmod{p^n}$; siue (quia per hyp. $1 \equiv \alpha^t \pmod{p^{n-1}}$ atque t per p^ν diuisibilis) ita vt fiat $\frac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1} h\frac{t}{p^\nu}$ per p diuisibilis, quaesito satisfactum erit. Hoc autem semper fieri posse ex Sect. praec. manifestum, quum t per altiorem ipsius p potestatem quam p^ν diuidi non posse hic supponamus, adeoque $\alpha^{t-1}\frac{t}{p^\nu}$ ad p sit primus.

Si vero $\nu = n-1$ i. e. t per p^{n-1} siue etiam per altiorem ipsius p potestatem diuisibilis quiuis valor A, congruentiae $x^t \equiv 1$ secundum modulum p satisfaciens eidem etiam secundum modulum p^n satisfaciet. Sit enim