$t = p^{n-1} r$, eritque $t \equiv r$ (mod. $p - 1$): quare quoniam $A^t \equiv 1$ (mod. p) erit etiam $A^r \equiv 1$ (mod. p). Ponatur itaque $A^r = 1 + hp$ eritque $A^t = (1 + hp)^{p^{n-1}} \equiv 1$ (mod. p^n) art. 87.

89. Omnia quae art. 57 sqq. adiumento therematis, congruentiam $x^t \equiv 1$ plures quam t radices diuersas non habere eruimus, etiam pro modulo qui est numeri primi potestas locum habent, et si *radices primitiuae* vocantur numeri, qui ad exponentem $p^{n-1}(p-1)$ pertinent, siue in quorum periodis omnes numeri per p non diuisiuiles inueniuntur, etiam hic radices primitiuae exstabunt. Omnia autem quae supra de indicibus eorumque vsu tradidimus, nec non de solutione congruentiae $x^t \equiv 1$, ad hunc quoque casum applicari possunt. Quae quum nulli difficultat obnoxia sint omnia ex integro repetere superfluum foret. Praeterea radices congruentiae $x^t \equiv 1$ secundum modulum p^n e radicibus eiusdem congruentiae secundum p deducere docuimus. Sed de eo casu, ubi potestas aliqua numeri 2 est modulus quia supra exceptus fuit, aliqua adhuc sunt adiicienda.

90. *Si potestas aliqua numeri 2, altior quam secunda, puta 2^n pro modulo accipitur, numeri cuiusuis imparis potestas exponentis 2^{n-2}, vnitati est congrua.*

Ex. gr. $3^8 = 6561 \equiv 1$ (mod. 32).

Quiuis enim numerus impar vel sub forma $1 + 4h$, vel sub hac $-1 + 4h$ comprehenditur: vnde propositio protinus sequitur (theor. art. 85).

Quoniam igitur exponens ad quem quicunque numerus impar secundum modulum 2^n pertinet, diuisor ipsius 2^{n-2} esse debet, quiuis ad aliquem horum numerum pertinebit 1, 2, 4, 8 . . . 2^{n-2}, ad quemnam vero pertineat ita facile diiudicatur. Sit numerus propositus $= 4h \pm 1$, atque exponens maximae potestatis numeri 2, quae ipsum h metitur, $= m$ (qui etiam $= 0$ esse potest, quando scilicet h est impar); tum exponens ad quem numerus propositus pertinet, erit $= 2^{n-m-2}$, siquidem $n > m + 2$; si autem $n =$ vel $< m + 2$, numerus propositus est $\equiv \pm 1$ adeoque vel ad exponentem 1 vel ad exponentem 2 pertinebit. Numerum enim formae $\pm 1 + 2^{m+1}k$, (quae huic aequiualet, $4h \pm 1$) ad potestatem exponentis 2^{n-m-2} eleuatum vnitati secundum modulum 2^n congruum fieri, ad potestatem autem exponentis, qui est inferior numeri 2 potestas, incongruum, ex art. 86 nullo negotio deducitur. Numerus itaque quicunque formae $8k + 3$ vel $8k + 5$ ad exponentem 2^{n-2} pertinebit.

91. Hinc patet eo sensu quo supra expressionem accepimus, *radices primitiuas* hic non dari, nullos scilicet numeros, quorum periodus omnes numeros modulo minores ad ipsumque primos amplectatur. Attamen facile perspicitur, analogon hic haberi. Inuenitur enim, numeri formae $8k + 3$ potestatem exponentis imparis semper esse formae $8k + 3$,

potestatem autem exponentis paris, semper formae $8k + 1$; nulla igitur potestas formae $8k + 7$ esse potest. Quare quum periodus numeri formae $8k + 3$, ex 2^{n-2} terminis diuersit constet, quorum quisque aut formae $8k + 3$ aut huius, $8k + 1$, neque plures huiusmodi numeri modulo minores dentur quam 2^{n-2}, manifesto, quiuis numerus formae $8k + 1$ vel $8k + 3$ congruus est secundum modulum 2^n potestati alicui numeri cuiuscunque formae $8k + 3$. Simili modo ostendi potest periodum numeri formae $8k + 5$ comprehendere omnes numeros formarum $8k + 1$ et $8k + 5$. Si igitur numerus formae $8k + 5$ pro basi assumitur, omnes numeri formae $8k + 1$ et $8k + 5$, positiue, omnesque formae $8k + 3$ et $8k + 7$, negatiue sumti, indices reales nanciscentur, et quidem hic indices secundum 2^{n-2} congrui pro aequiualentibus sunt habendi. Hoc modo tabula nostra I intelligenda, vbi pro modulis 16, 32 et 64 (namque pro modulo 8 nulla tabula necessaria erit) semper numerum 5 pro basi accepimus. Ex. gr. numero 19 qui est formae $8n + 3$ adeoque *negatiue* sumendus, respondet pro modulo 64 index 7, id quod significat esse $5^7 \equiv -19$ (mod. 64). Numeris autem formarum $8n + 1$, $8n + 5$ negatiue, atque numeris formarum $8n + 3$, $8n + 7$ positiue acceptis, indices quasi imaginarii tribuendi forent. Quos introducendo calculus indicum ad algorithmum perquam simplicem reduci potest. Sed quoniam, si haec ad omnem rigorem exponere vellemus, nimis longe euagari oporteret, hoc negotium ad aliam occasionem