entia $kn \equiv 1 \pmod{\frac{p-1}{nq}}$ soluitur (quod fieri potest quia n ad $\frac{p-1}{nq}$ primus), valor ipsius k etiam secundum modulum t congruentiae satisfaciet, id quod quaerebatur. Totum hoc artificium in eo versatur, vt numerus eruatur qui ipsius t, quem ignoramus, vice fungi possit. Attamen probe meminisse oportet, nos quando $\frac{p-1}{n}$ ad n non est primus, supposuisse conditionem art. praec. locum habere, quae si deficit omnes conclusiones erroneae erunt; atque si regulas datas temere sequendo pro x valor inuenitur, cuius potestas n^{ta} ipsi A non sit congrua, indicio hoc est, conditionem deficere adeoque methodum hanc omnino adhiberi non posse.

67. Sed in hocce etiam casu saepe prodesse potest, hunc laborem suscepisse; operaeque pretium est, quomodo hic valor falsus ad veros sese habeat inuestigare. Supponamus itaque numeros k, z rite esse determinatos sed z^n non esse $\equiv A \pmod{p}$. Tum si modo valores expressionis $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$ determinari possint, hos singulos per z multiplicando valores ipsius $\sqrt[n]{A}$ obtinebimus. Si enim v est valor aliquis ipsius $\sqrt[n]{\frac{A}{z^n}}$: erit $(vz)^n \equiv A$. Sed expressio $\sqrt[n]{\frac{A}{z^n}}$ eatenus hac $\sqrt[n]{A}$ simplicior, quod $\frac{A}{z^n} \pmod{p}$ ad exponentem minorem plerumque pertinet quam A. Scilicet si numerorum t, q diuisor communis maximus est d, $\frac{A}{z^n} \pmod{p}$ ad exponentem d pertinebit, id quod ita demonstratur. Substituto pro z valore, fit $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \pmod{p}$. At $kn - 1$ per $\frac{p-1}{nq}$ diuisibilis (art. praec.), $\frac{p-1}{n}$ vero per t (ibid.) siue

siue $\frac{p-}{nd}$ per $\frac{t}{d}$. Atqui $\frac{t}{d}$ ad $\frac{q}{d}$ est primus (hyp.), quare etiam $\frac{p-1}{nd}$ per $\frac{tq}{dd}$ siue $\frac{p-1}{nq}$ per $\frac{t}{d}$, adeoque etiam $kn-1$ per $\frac{t}{d}$ et $(kn-1)\,d$ per t erit diuisibilis. Hinc $A^{(kn-1)d} \equiv 1 \pmod{p}$. Vnde facile deducitur, $\frac{A}{z^n}$ ad potestatem d^{tam} euectum vnitati congruum fieri. Quod vero $\frac{A}{z^n}$ ad exponentem minorem quam d pertinere non possit facile quidem demonstrari potest, sed quoniam ad finem nostrum non requiritur, huic rei non immoramur. Certi igitur esse possumus, $\frac{A}{z^n} \pmod{p}$ semper ad minorem exponentem pertinere, quam A, vnico excepto casu, scilicet quando t ipsum q metitur, adeoque $d = t$.

Sed quid iuuat, quod $\frac{A}{z^n}$ ad minorem exponentem pertinet, quam A? Plures numeri dantur qui possunt esse A quam qui possunt esse $\frac{A}{z^n}$, et quando secundum eundem modulum plures huiusmodi expressiones $\sqrt[n]{A}$ euoluere occasio est, id lucramur vt plures ex eodem fonte haurire possimus. Ita ex. gr. semper vnicum saltem valorem expressionis $\sqrt[2]{A}$ (mod. 29) determinare in potestate erit, si modo expressionis $\sqrt[2]{-1}$ (mod. 29) valores (qui sunt ± 12) innotuerint. Facile enim ex art. praec. perspicitur, huiusmodi expressionum vnum valorem semper directe determinari posse, quando t impar, et d fieri $= 2$ quando t par; praeter -1 autem nullus numerus ad exponentem 2 pertinet.

68. *Exempla.*
Quaeritur $\sqrt[3]{31}$ (mod. 37). Hic $p-1=36$, $n=3$, $\frac{p-1}{3}=12$, adeoque $q=3$: debet igitur esse $3k\equiv 1$ (mod. 4) quod obtinetur ponendo $k=3$. Hinc $x\equiv 31^3$ (mod. 37) $\equiv 6$, inueniturque reuera $6^3\equiv 31$ (mod. 37). Si valores expressionis $\sqrt[3]{1}$ (mod. 37) sunt notae, etiam reliqui expr. $\sqrt[3]{6}$ valores determinari possunt. Sunt vero illi 1, 10, 26, per quos multiplicando ipsum 6, prodeunt reliqui $\equiv 23$ et 8.

Si autem quaeritur valor expr. $\sqrt[2]{3}$ (mod. 37), erit $n=2$, $\frac{p-1}{n}=18$; adeoque $q=2$. Hinc debet esse $2k\equiv 1$ (mod. 9), vnde fit $k\equiv 5$ (mod. 9). Quare $x\equiv 3^5\equiv 21$ (mod. 37); at 21^2 non $\equiv 3$, sed $\equiv 34$; est autem $\frac{3}{34}$ (mod. 37) $\equiv -1$, atque $\sqrt[2]{-1}$ (mod. 37) $\equiv \pm 6$; vnde obtinentur valores veri $\pm 6.\ 21\equiv \pm 15$.

Haec fere sunt, quae hic de talium expressionum euolutione tradere licuit. Palam est methodos directas satis prolixas saepe euasuras: at hoc incommodum tantum non omnibus methodis directis in numerorum theoria incumbit; neque ideo negligendum censuimus, quantum hic praestare valeant ostendere. Etiam hic obseruare conuenit, artificia particularia quae exercitato haud raro se offerunt sigillatim explicare, non esse instituti nostri.

69. Reuertimur nunc ad radices quas diximus primitiuas. Ostendimus, radice primitiua quacunque pro basi assumta omnes numeros, quorum indices ad $p-1$ primi, etiam fo-