lum $p-1$ incongruos habebit; quare etiam x in hocce casu δ valores diuersos (secundum modulum p incongruos) habebit. Hinc perspicitur, expressionem $\sqrt[\delta]{1}$ etiam δ valores diuersos habere, quorum indices cum ante allatis prorsus conueniant. Quocirca expressio $\sqrt[\delta]{1}$ (mod. p) huic $\sqrt[n]{1}$ (mod. p) omnino aequiualet, i. e. congruentia $x^\delta \equiv 1$ (mod. p) easdem radices habet quas haec, $x^n \equiv 1$ (mod. p). Prior autem inferioris erit gradus siquidem δ et n sunt inaequales.

Ex. $\sqrt[15]{1}$ (mod. 19) tres habet valores, quia 3 maxima numerorum 15, 18 mensura communis, hique simul erunt valores expressionis $\sqrt[3]{1}$ (mod. 19). Sunt autem hi, 1, 7, 11.

62. Per hanc igitur reductionem id lucramur vt alias congruentias formae $x^n \equiv 1$ soluere non sit opus, quam vbi n moduli est diuisor. Infra vero ostendemus, congruentias huius formae semper vlterius adhuc deprimi posse, licet praecedentia ad hoc non sufficiant. Vnum tamen casum iam hic absoluere possumus scilicet vbi $n=2$. Manifesto enim valores expressionis $\sqrt[2]{1}$ erunt $+1$ et -1 quia plures quam duos habere nequit, hique $+1$ et -1 semper sunt incongrui nisi modulus sit $=2$, in quo casu $\sqrt[2]{1}$ vnam tantum valorem habere posse, per se clarum. Hinc sequitur, $+1$ et -1 etiam fore valores expressionis $\sqrt[2m]{1}$ quando m ad $\frac{p-1}{2}$ sit primus. Hoc semper eueniet, quoties modulus est eius indolis vt $\frac{p-1}{2}$ fiat numerus absolute primus (nisi forte $p-1=2m$ in

quo casu omnes numeri 1, 2, 3 .... $p-1$ sunt radices) ex. gr. quando $p=3$, 5, 7, 11, 23, 47, 59, 83, 107 etc. - Tamquam corollarium hic annotetur, indicem ipsius -1 semper esse $\equiv \frac{p-1}{2}$ (mod. $p-1$), quaecunque radix primitiua pro basi accipiatur. Namque 2 Ind. $(-1) \equiv 0$ (mod. $p-1$). Quare Ind. (-1) erit vel $\equiv 0$, vel $\equiv \frac{p-1}{2}$ (mod. $p-1$): 0 vero semper index ipsius $+1$, atque $+1$, et -1 semper indices diuersos habere debent (praeter casum $p=2$ ad quem hic respicere operae non est pretium).

63. Ostendimus art. 60 expressionem $\sqrt[n]{A}$ (mod. p) habere δ valores diuersos, aut omnino nullum, si fuerit δ diuisor communis maximus numerorum n, $p-1$. Iam vti modo docuimus $\sqrt[n]{A}$ et $\sqrt[\delta]{A}$ aequiualentes esse, si fuerit $A\equiv 1$, generalius probabimus, expressionem $\sqrt[n]{A}$ semper ad aliam $\sqrt[\delta]{B}$ reduci posse cui aequiualeat. Illius enim valore quocunque denotato per x erit $x^n \equiv A$; iam sit t valor quicunque expressionis $\frac{\delta}{n}$ (mod. $p-1$), quam valores reales habere ex art. 31 perspicuum; eritque $x^{tn} \equiv A^t$ at $x^{tn} \equiv x^\delta$ propter $tn \equiv \delta$ mod. $(p-1)$. Quare $x \equiv A^t$ adeoque quicunque ipsius $\sqrt[n]{A}$ valor erit etiam valor ipsius $\sqrt[\delta]{A^t}$. Quoties igitur $\sqrt[n]{A}$ valores reales habet, expressioni $\sqrt[\delta]{A^t}$ prorsus aequiualens erit, quoniam illa neque alios habet quam haec neque pauciores, licet quando $\sqrt[n]{A}$ nullum valorem realem habet, fieri tamen possit vt $\sqrt[\delta]{A^t}$ valores reales habeat.

Ex. Si valores expressionis $\sqrt[21]{2}$ (mod. 31) quaeruntur, erit numerorum 21 et 30 diuisor communis maximus 3, expressionisque $\frac{3}{21}$ (mod. 30) valor aliquis 3, quare si $\sqrt[21]{2}$ valores reales habet, huic expressioni $\sqrt[3]{2^3}$ siue $\sqrt[3]{8}$ aequiualebit, inuenieturque reuera, posteriores expressionis valores qui sunt 2, 10, 19 etiam priori satisfacere.

64. Ne autem hanc operationem incassum suscepisse periclitemur, regulam inuestigare oportet, per quam statim diiudicari possit vtrum $\sqrt[n]{A}$ valores reales admittat necne. Quodsi tabula indicum habetur, res in promtu est; namque ex art. 60 manifestum est, valores reales dari, si ipsius A index, radice quacunque primitiua pro basi accepta, per δ sit diuisibilis, sin vero minus, non dari. Attamen hoc etiam absque tali tabula inueniri potest. Posito enim indice ipsius $A = k$, si hic fuerit per δ diuisibilis, erit $\frac{k(p-1)}{\delta}$ per $p-1$ diuisibilis et vice versa. Atqui numeri $A^{\frac{p-1}{\delta}}$ index erit $\frac{k(p-1)}{\delta}$. Quare si $\sqrt[n]{A}$ (mod. p) habet valores reales, $A^{\frac{p-1}{\delta}}$ vnitati congruus erit, sin minus, incongruus. Ita in exemplo art. praec. habetur $2^{10} = 1024 \equiv 1$ (mod. 31), vnde concluditur $\sqrt[21]{2}$ (mod. 31) valores reales habere. Similiter certiores hinc fimus, $\sqrt[2]{-1}$ (mod. p) semper valores binos reales habere, quando p sit formae $4m+1$, nullum vero, quando p sit formae $4m+3$; propter $(-1)^{2m} = 1$ et $(-1)^{2m+1} = -1$. Elegans hoc theorema, quod vulgo ita profertur: *Si p est numerus primus formae $4m+1$, inueniri potest quadratum aa, ita vt $aa+1$ per p fiat diuisibilis; si vero p est formae*