

sumti; tum sequuntur indices numerorum primorum successiuorum, quorum quini semper per paruulum interuallum sunt disiuncti, eodemque ordine supra dispositi sunt numeri primi; ita vt quis index numero primo dato secundum modulum datum respondeat, facile tuoque inueniri possit.

Ita ex. gr. si $p=67$ index numeri 60, assumto 12 pro basi erit $\equiv 2 \text{ Ind. } 2 + \text{Ind. } 3 - \text{Ind. } 5 \pmod{66} \equiv 58 + 9 + 39 \equiv 40$.

59. *Index valoris cuiuscunque expressionis $\frac{a}{b}$ (mod. p), (art. 31) congruus est secundum modulum $p-1$ differentiae indicum numeratoris a et denominatoris b , siquidem numeri a, b per p non sunt diuisibiles.*

Sit enim valor quicunque c ; eritque $bc \equiv a \pmod{p}$; hinc $\text{Ind. } b + \text{Ind. } c \equiv \text{Ind. } a \pmod{p-1}$ adeoque $\text{Ind. } c \equiv \text{Ind. } a - \text{Ind. } b$.

Si itaque tabula habetur, ex qua index cuique numero respondens pro quouis modulo primo, aliaque ex qua numerus ad indicem datum pertinens deriuari possit, omnes congruentiae primi gradus facillimo negotio solui poterunt, quoniam omnes reduci possunt ad tales, quarum modulus est numerus primus (art. 30). E. g. proposita congruentia $29x + 7 \equiv 0 \pmod{47}$ erit $x \equiv \frac{-7}{29} \pmod{47}$. Hinc $\text{Ind. } x \equiv \text{Ind. } -7 - \text{Ind. } 29 \equiv \text{Ind. } 40 - \text{Ind. } 29 \equiv 15 - 43 \equiv 18 \pmod{46}$. At numerus cuius index 18 inuenitur 3. Quare

$x \equiv 3 \pmod{47}$. — Tabulam secundam quidem non adiecimus: at huius vice alia defungi poterit vti Sect. VI ostendemus.

60. Simili modo vt art. 31 radices congruentiarum primi gradus designauimus, in sequentibus etiam congruentiarum purarum altiorum graduum radices per signum exhibebimus. Vti scilicet $\sqrt[n]{A}$ nihil aliud significat quam radicem aequationis $x^n = A$; ita appposito modulo per $\sqrt[n]{A} \pmod{p}$ denotabitur radix quaecunque congruentiae $x^n \equiv A \pmod{p}$. Hanc expressionem $\sqrt[n]{A} \pmod{p}$ tot valores habere dicemus, quot habet secundum p incongruos, omnes enim qui secundum p sunt congrui tamquam aequiuales spectandi (art. 26). Ceterum patet, si A, B secundum p fuerint congrui, expressiones $\sqrt[n]{A}, \sqrt[n]{B} \pmod{p}$ aequiuales fore.

Iam si ponitur $\sqrt[n]{A} \equiv x \pmod{p}$, erit n Ind. $x \equiv$ Ind. $A \pmod{p-1}$. Ex hac congruentia deducuntur ad praecepta sectionis praec. valores ipsius Ind. x atque ex his valores respondentes ipsius x . Facile vero perspicitur x habere totidem valores, quot radices congruentia n Ind. $x \equiv A \pmod{p-1}$. Manifesto igitur $\sqrt[n]{A}$ vnum tantummodo valorem habebit quando n ad $p-1$ est primus; quando vero numeri $n, p-1$ diuisorem communem habent δ , atque hic est maximus, Ind. x habebit δ valores incongruos secundum $p-1$, adeoque $\sqrt[n]{A}$ totidem valores incongruos secundum p , siquidem Ind. A per δ est diuisibilis. Qua con-

ditione deficiente $\sqrt[n]{A}$ nullum valorem realem habebit.

Exemplum. Quaeruntur valores expressio-
nis $\sqrt[15]{11} \pmod{19}$. Solui itaque debet con-
gruentia $15 \text{ Ind. } x \equiv \text{Ind. } 11 \equiv 6 \pmod{18}$;
inuenienturque tres valores ipsius $\text{Ind. } x \equiv 4,$
 $10, 16 \pmod{18}$. His vero respondent valores
ipsius $x, 6, 9, 4$.

61. Quantumvis expedita sit methodus
haec quando tabulae necessariae adsunt,
debemus tamen non obliuisci, indirectam
eam esse. Operae igitur pretium erit in-
quirere quantum methodi directae polleant:
trademusque hic ea quae ex praecedentibus
hauriri possunt: alia, quae considerationes re-
conditiores postulant, ad sectionem VIII reser-
uantes. Initium facimus a casu simplicissimo,
vbi $A=1$, siue vbi radices congruentiae $x^n \equiv 1$
 \pmod{p} quaeruntur. Hic itaque, assumpta ra-
dice quacunque primitiua pro basi, debet esse
 $n \text{ Ind. } x \equiv 0 \pmod{p-1}$. Quae congruen-
tia, quando n ad $p-1$ est primus, vniam tan-
tummodo radicem habebit, scilicet $\text{Ind. } x \equiv 0$
 $\pmod{p-1}$: quare in hocce casu $\sqrt[n]{1} \pmod{p}$
vnicum valorem habet, scilicet $\equiv 1$. Quan-
do autem numeri $n, p-1$ habent diuisorem
communem (maximum) δ , congruentiae $n \text{ Ind.}$
 $x \equiv 0 \pmod{p-1}$ solutio completa erit Ind.
 $x \equiv 0 \pmod{\frac{p-1}{\delta}}$ V. art. 30., i. e. $\text{Ind. } x$ se-
cundum modulum $p-1$ alicui ex his numeris,
 $0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \frac{3(p-1)}{\delta}, \dots, \frac{(\delta-1)(p-1)}{\delta}$ congruus
esse debebit, siue δ valores secundum modu-