

sumti; tum sequuntur indices numerorum primorum successuorum, quorum quini semper per parvulum interuum sunt disiuncti, eodemque ordine supra dispositi sunt numeri primi; ita ut quis index numero primo dato secundum modulum datum respondeat, facile tu-toque inueniri possit.

Ita ex. gr. si $p = 67$ index numeri 60, assumto 12 pro basi erit $\equiv 2$ Ind. 2 + Ind. 3 — Ind. 5 (mod. 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 divisibles.

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

Si itaque tabula habetur, ex qua index cuique numero respondens pro quovis modulo primo, aliaque ex qua numerus ad indicem datum pertinens deriuari possit, omnes congruentiae primi gradus facillimo negotio solvi poterunt, quoniam omnes reduci possunt ad tales, quarum modulus est numerus primus (art. 50). E. g. proposita congruentia $29x + 7 \equiv 0$ (mod. 47) erit $x \equiv \frac{-7}{29} \equiv \frac{40}{29} \equiv 15 - 43 \equiv 18$ (mod. 46).

Hinc Ind. $x \equiv \text{Ind. } -7 - \text{Ind. } 29 \equiv \text{Ind. } 40 - \text{Ind. } 29 \equiv 15 - 43 \equiv 18$ (mod. 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 apposito 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 aequivalentes spectandi (art. 26). Ceterum patet, si A, B secundum p fuerint congrui, expressiones $\sqrt[n]{A}, \sqrt[n]{B} \pmod{p}$ aequivalentes 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 expressionis $\sqrt[15]{11}$ (mod. 19). Solui itaque debet congruentia 15 Ind. $x \equiv$ Ind. 11 \equiv 6 (mod. 18), inuenienturque tres valores ipsius Ind. $x \equiv 4, 10, 16$ (mod. 18). His vero respondent valores ipsius $x, 6, 9, 4$.

61. Quantumuis expedita sit methodus haec, quando tabulae necessariae adsunt, debemus tamen non obliuisci, indirectam eam esse. Operae igitur pretium erit inquirere quantum methodi directae polleant: trademusque hic ea quae ex praecedentibus hauriri possunt: alia, quae considerationes reconditiores postulant, ad sectionem VIII reseruantes. Initium facimus a casu simplicissimo, vbi $A = 1$, siue vbi radices congruentiae $x^n \equiv 1$ (mod. p) quaeruntur. Hic itaque, assumta radice quacunque primitiva pro basi, debet esse n Ind. $x \equiv 0$ (mod. $p - 1$). Quae congruentia, quando n ad $p - 1$ est primus, vnam tantummodo radicem habebit, scilicet Ind. $x \equiv 0$ (mod. $p - 1$): quare *in hocce casu* $\sqrt[n]{1}$ (mod p) vnicum valorem habet, scilicet $\equiv 1$. Quando autem numeri $n, p - 1$ habent diuisorem communem (maximum) δ , congruentiae n Ind. $x \equiv 0$ (mod. $p - 1$) solutio completa erit Ind. $x \equiv 0$ (mod. $\frac{p-1}{\delta}$) V. art. 30., i. e. Ind. x secundum 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 debet, siue δ valores secundum modu-