72. Quamuis in genere prorsus arbitrarium sit, quaenam radix primitiua pro basi adoptetur, interdum tamen bases aliae prae aliis commoda quaedam peculiaria praebere possunt. In tabula I semper numerum 10 pro basi assumsimus, quando fuit radix primitiua; alioquin basin ita semper determinauimus vt numeri 10 index euaserit quam minimus, i. e. $= \frac{p-1}{t}$ denotante t exponentem ad quem 10 pertinuit. Quid vero hinc lucremur, in Sect. VI. ostendemus vbi eadem tabula ad alios adhuc vsus adhibebitur. Sed quoniam etiam hic aliquid arbitrarii remanere potest, vt ex art. praec. apparet: vt aliquid certi statueremus, ex omnibus radicibus primitiuis quaesitum praestantibus *minimam* semper pro basi eleximus. Ita pro $p = 73$, vbi $t = 8$ atque $d = 9$, habet $\frac{72.2}{8.3}$ i. e. 6 valores, qui sunt 5, 14, 20, 28, 39, 40. Assumsimus itaque minimum 5 pro basi.

73. Methodi radices primitiuas inueniendi maximam partem tentando innituntur. Si quis ea quae art. 55 docuimus cum iis quae infra de solutione congruentiae $x^n \equiv 1$ trademus confert omnia fere, quae per methodos directas effici possunt, habebit. Ill. Euler confitetur, *Opusc. Analyt. T. I. p.* 152, maxime difficile videri, hos numeros assignare, eorumque indolem ad profundissima numerorum mysteria esse referendam. At tentando satis expedite sequenti modo determinari possunt. Exercitatus operationis prolixitati per multifaria artificia particularia succurrere sciet: haec vero per vsum multo citius quam per praecepta ediscuntur

1°. Assumatur ad libitum numerus ad p (ita semper modulum designamus) primus, a, (plerumque ad calculi breuitatem conducit, si quam minimum accipimus, ex. gr. numerum 2) determineturque eius periodus (art. 46), i. e. residua minima ipsius potestatum, donec ad potestatem a^t perueniatur, cuius residuum minimum sit 1 *). Iam si fuerit $t = p - 1$, a est radix primitiua.

2°. Si vero $t < p - 1$, accipiatur alius numerus b in periodo ipsius a non contentus, inuestigeturque simili modo huius periodus. Designato exponente ad quem b pertinet per u, facile perspicitur u neque ipsi t aequalem neque ipsius partem aliquotam esse posse, in vtroque enim casu fieret $b^t \equiv 1$, quod esse nequit, quum periodus ipsius a omnes numeros amplectatur, quorum potestas exponentis t vnitati congrua (art. 53). Quodsi u fuerit $= p - 1$, erit b radix primitiua; si vero u non quidem $= p - 1$, sed tamen multiplum ipsius t, id lucrati sumus, vt numerus constet ad exponentem maiorem pertinens, adeoque scopo nostro, qui est inuenire numerum ad exponentem *maximum* pertinentem, propiores iam simus. Si vero u neque $= p - 1$, neque ipsius p multiplum, tamen numerum inuenire possumus ad exponentem ipsis t, u maiorem pertinentem, nempe ad exponentem minimo diuiduo communi numerorum t, u, aequalem. Sit hic $= y$, resolua-

*) Quisquis sponte perspiciet, non opus esse has potestates ipsas nouisse, quum cuiusuis residuum minimum facile ex residuo minimo potestatis praecedentis obtineri possit.

turque y ita in duos factores inter se primos, m, n, vt alter ipsum t, alter ipsum u metiatur *). Tum fiat potestas $\frac{t}{m}^{\text{ta}}$ ipsius $a, \equiv A$, potestas $\frac{u}{n}^{\text{ta}}$ ipsius $b, \equiv B \pmod{p}$, eritque productum AB numerus ad exponentem y pertinens; facile enim intelligitur, A ad exponentem m, B ad exponentem n pertinere; adeoque productum AB ad mn pertinebit, quia m, n inter se sunt primi, id quod prorsus eodem modo vti in art. 55, II processimus probari poterit.

3°. Iam si $y = p - 1$, AB erit radix primitiua; sin minus, simili modo vt antea alius numerus adhibendus erit, in periodo ipsius AB non occurrens; eritque hic aut radix primitiua, aut pertinebit ad exponentem ipso y maiorem, aut certe ipsius auxilio (vti ante) numerus ad exponentem ipso y maiorem pertinens inueniri poterit. Quum igitur numeri qui per repetitionem huius operationis prodeunt, ad exponentes continuo crescentes pertineant, manifestum est tandem numerum inuentum iri, qui ad exponentem *maximum* pertineat, i. e. radicem primam, *q. e. f.*

*) Quomodo hoc fieri possit ex art. 18 haud difficulter deriuatur. Resoluatur y in factores tales, qui sint aut numeri primi diuersi aut numerorum primorum diuersorum potestates. Horum quisque alterutrum numerorum t, u metietur (siue etiam vtrumque). Adscribantur singuli aut numero t aut numero u, prout illum aut hunc metiuntur: quando aliquis vtrumque metitur, arbitrarium est, cui adscribatur: productum ex iis qui ipsi t adscripti sunt, sit $= m$, productum e reliquis $= n$, facileque perspicietur m ipsum t, n ipsum u metiri, atque esse $mn = y$.