re radices primitiuas, nullosque praeter hos; vnde simul radicum primitiuarum multitudo sponte innotescit. V. art. 53. Quamnam autem radicem primitiuam pro basi adoptare velimus, in genere arbitrio nostro relinquitur; vnde intelligitur, etiam hic, vt in calculo logarithmico, plura quasi systemata dari posse *), quae quo vinculo connexa sint videamus. Sint a, b, duae radices primitiuae, aliusque numerus m, atque, quando a pro basi assumitur, index numeri $b \equiv \beta$, numeri m vero index $\equiv \mu$ (mod. $p-1$); quando autem b pro basi assumitur, index numeri $a \equiv \alpha$, numeri m vero $\equiv \nu$, (mod. $p-1$). Tum erit $\alpha\beta \equiv 1$ (mod. $p-1$); namque $a^\beta \equiv b$, quare $a^{\alpha\beta} \equiv b^\alpha \equiv a$ (mod. p), (hyp.), hinc $\alpha\beta \equiv 1$ (mod. $p-1$). Per simile ratiocinium inuenitur $\nu \equiv \alpha\mu$, atque $\mu \equiv \beta\nu$ (mod. $p-1$). Si igitur tabella indicum pro basi a constructa habetur, facile in aliam conuerti potest, vbi b basis. Si enim pro basi a ipsius b index est $\equiv \beta$, pro basi b ipsius a index erit $\equiv \frac{1}{\beta}$ (mod. $p-1$), multiplicandoque per hunc numerum omnes tabellae indices, habebuntur omnes indices pro basi b.

70. Quamuis autem plures indices numero dato contingere possint, aliis aliisque radicibus primitiuis pro basi acceptis, omnes tamen in eo conuenient, quod omnes eundem diuisorem maximum cum $p-1$ communem ha-

*) In eo autem differunt, quod in logarithmis systematum numerus est infinitus, hic vero tantus, quantus numerus radicum primitiuarum. Manifesto enim bases congruae idem systema generant.

bebunt. Si enim pro basi a, index numeri dati est m, pro basi b vero n, atque diuisores maximi his cum $p-1$ communes, μ, ν supponuntur esse inaequales, alter erit maior, ex. gr. $\mu > \nu$, adeoque μ ipsum n non metietur. At designato indice ipsius a, quando b pro basi assumitur, per α, erit (art. praec.) $n \equiv \alpha m$ (mod. $p-1$) adeoque μ etiam ipsum n metietur. *Q. E. A.*

Hunc diuisorem maximum indicibus numeri dati, ipsique $p-1$ communem, a basi non pendere, etiam inde perspicuum, quod aequalis est ipsi $\frac{p-1}{t}$, designante t exponentem ad quem numerus, de cuius indicibus agitur, pertinet. Si enim index pro basi quacunque est k, erit t minimus numerus per quem k multiplicatus ipsius $p-1$ multiplum euadit, (excepta cifra) vidd. artt. 48, 58, siue minimus valor expressionis $\frac{0}{k}$ (mod. $p-1$) praeter cifram; hunc autem aequalem esse diuisori maximo communi numerorum k et $p-1$ ex art. 29 nullo negotio deriuatur.

71. Porro facile demonstratur, basin ita semper accipere licere, vt numerus ad exponentem t pertinens indicem quemlibet datum nanciscatur, cuius quidem maximus diuisor cum $p-1$ communis $= \frac{p-1}{t}$. Designemus hunc breuitatis gratia per d, sitque index propositus $\equiv dm$, numerique propositi, quando quaelibet radix prima a pro basi accipitur, index $\equiv dn$, eruntque m, n ad $\frac{p-1}{d}$ siue ad t primi. Tum si est valor expressionis $\frac{dn}{dm}$ (mod. $p-1$), simul-

que ad $p-1$ primus, erit a^e radix primitiua, qua pro basi accepta numerus propositus indicem dm adipiscetur (erit enim $a^{edm} \equiv a^{dn} \equiv$ numero proposito), id quod desiderabatur. Sed expressionem $\frac{dn}{dm}$ (mod. $p-1$) valores ad $p-1$ primos admittere, ita probatur. Aequiualet illa expressio huic: $\frac{n}{m}$ (mod. $\frac{p-1}{d}$) siue $\frac{n}{m}$ (mod. t) vid. art. 31, 2, eruntque omnes eius valores ad t primi; si enim aliquis valor e diuisorem cum t communem haberet, hic diuisor etiam ipsum me metiri deberet, adeoque etiam ipsum n, cui me secundum t congruus, contra hypoth., ex qua n ad t primus. Quando igitur omnes diuisores primi ipsius $p-1$ etiam ipsum t metiuntur, *omnes* expr. $\frac{n}{m}$ (mod. t) valores ad $p-1$ primi erunt multitudoque eorum $= d$; quando autem $p-1$ alios adhuc diuisores primos, f, g, h etc. implicat, ipsum t non metientes, ponatur valor quicunque expr. $\frac{n}{m}$ (mod. t) $\equiv e$. Tum autem quia omnes t, f, g, h etc. inter se primi, inueniri potest numerus ε, qui secundum t ipsi e, secundum f, g, h etc. vero numeris quibuscunque ad hos respectiue primos fiat congruus. (art. 32) Talis itaque numerus per nullum factorem primum ipsius $p-1$ diuisibilis adeoque ad $p-1$ primus erit, vti desiderabatur. Tandem haud difficile ex combinationum theoria deducitur, talium valorum multitudinem fore $= \frac{p.\ f-1.\ g-1.\ h-1.\ \text{etc.}}{t.\ f.\ g.\ h.\ \text{etc.}}$; sed ne digressio haec in nimiam molem excrescat, demonstrationem, quum ad institutum nostrum non sit adeo necessaria, omittimus.