dem principio omnia similia praecepta facile deducuntur.

Nec minus ex praecedentibus petenda est ratio regularum, quae ad verificationem operationum arithmeticarum vulgo commendantur. Scilicet si ex numeris datis alii per additionem, subtractionem, multiplicationem aut eleuationem ad potestates sunt deducendi: substiuuntur datorum loco residua ipsorum minima secundum modulum arbitrarium (vulgo 9 aut 11, quoniam in nostro systemate decadico secundum hos, vti modo ostendimus, residua tam facile possunt inueniri). Numeri hinc oriundi illis, qui ex numeris propositis deducti fuerunt, congrui esse debent; quod nisi eueniat, vitium in calculum irrepsisse concluditur.

Sed quum haec hisque similia abunde sint nota, diutius iis immorari superfluum foret.

SECTIO SECVNDA

DE

CONGRVENTIIS PRIMI GRADVS.

13. THEOREMA. *Productum e duobus numeris positiuis numero primo dato minoribus per hunc primum diuidi nequit.*

Sit p primus, et a positiuus $< p$: tum nullus numerus positiuus b ipso p minor dabitur, ita vt sit $ab \equiv 0 \pmod{p}$.

Dem. Si quis neget, supponamus dari numeros b, c, d, etc. omnes $< p$, ita vt $ab \equiv 0$; $ac \equiv 0$; $ad \equiv 0$ etc. (mod. p). Sit omnium minimus b, ita vt omnes numeri ipso b minores hac proprietate sint destituti. Manifesto erit $b > 1$: si enim $b = 1$, foret $ab = a < p$ (*hyp.*), adeoque per p non diuisibilis. Quare p tamquam primus per b diuidi non poterit, sed inter duo ipsius b multipla proxima mb et $(m+1)b$ cadet. Sit $p - mb = b'$, eritque b' numerus positiuus et $< b$. Iam quia supposuimus, $ab \equiv 0 \pmod{p}$, habebitur quoque $mab \equiv 0$ (art. 7), et hinc, subtrahendo ab $ap \equiv 0$, erit $a(p - mb) = ab' \equiv 0$; i. e. b' inter nu-

meros b, c, d, etc. referendus, licet minimo eorum b sit minor. *Q. E. A.*

14. *Si nec a nec b per numerum primum p diuidi potest: etiam productum ab per p diuidi non poterit.*

Sint numerorum a, b, secundum modulum p residua minima positiua α, β, quorum neutrum erit o (*hyp.*). Iam si esset $ab \equiv o \pmod{p}$, foret quoque, propter $ab \equiv \alpha\beta$, $\alpha\beta \equiv o$, quod cum theoremate praec. consistere nequit.

Huius theorematis demonstratio iam ab Euclide tradita, *El. VII.* 32. Nos tamen omittere eam noluimus, tum quod recentiorum complures seu ratiocinia vaga pro demonstratione venditauerunt, seu theorema omnino praeterierunt, tum quod indoles methodi hic adhibitae, qua infra ad multo reconditiora enodanda vtemur, e casu simpliciori facilius deprehendi poterit.

15. *Si nullus numerorum a, b, c, d etc. per numerum primum p diuidi potest, etiam productum abcd etc. per p diuidi non poterit.*

Secundum artic. praec. ab per p diuidi nequit; ergo etiam abc; hinc $abcd$, etc.

16. Theorema. *Numerus compositus quicunque vnico tantum modo in factores primos resolui potest.*

Dem. Quemuis numerum compositum in factores primos resolui posse, ex elementis constat, sed pluribus modis diuersis fieri hoc non posse perperam plerumque supponitur tacite. Fingamus numerum compositum A, qui sit $= a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, alio adhuc modo in factores primos esse resolubilem. Primo manife-