Ponamus itaque $a = \delta e$, $m = \delta f$, $t - u = \delta k$, eritque e ad f primus. Tum vero congruentiae propositae $\delta ex + \delta k \equiv 0$ (mod. δf) aequiualebit haec $ex + k \equiv 0$ (mod. f), i. e. quicunque ipsius x valor huic satisfaciat, etiam illi satisfaciet et vice versa. Manifesto enim $ex + k$ per f diuidi poterit, quando $\delta ex + \delta k$ per δf diuidi potest, et vice versa. At congruentiam $ex + k \equiv 0$ (mod. f) supra soluere docuimus; vnde simul patet, si v sit vnus ex valoribus ipsius x, $x \equiv v$ (mod. f) exhibere resolutionem completam congruentiae propositae.

30. Quando modulus est compositus, nonnumquam praestat sequenti methodo vti.

Sit modulus $= mn$, atque congruentia proposita $ax \equiv b$. Soluatur primo congruentia haec secundum modulum m, ponamusque ei satisfieri, si $x \equiv v$ (mod. $\frac{m}{\delta}$), designante δ diuisorem communem maximum numerorum m, a. Iam manifestum est, quemuis valorem ipsius x congruentiae $ax \equiv b$ secundum modulum mn satisfacientem eidem etiam secundum modulum m satisfacere debere: adeoque in forma $v + \frac{m}{\delta}x'$ contineri, designante x' numerum indeterminatum, quamuis non vice versa omnes numeri in forma $v + \frac{m}{\delta}x'$ contenti congruentiae secundum mod. mn satisfaciant. Quomodo autem x' determinari debeat, vt $v + \frac{m}{\delta}x'$ fiat radix congruentiae $ax \equiv b$ (mod. mn), ex solutione congruentiae $\frac{am}{\delta}x' + av \equiv b$ (mod. mn) deduci potest, cui aequiualet haec $\frac{a}{\delta}x' \equiv \frac{b-av}{m}$ (mod. n). Hinc colligitur solutionem congruentiae cuiuscunque primi gradus secundum modulum mn

reduci posse ad solutionem duarum congruentiarum secundum modulum m et n. Facile autem perspicietur, si m iterum sit productum e duobus factoribus, solutionem congruentiae secundum modulum n pendere a solutione duarum congruentiarum quarum moduli sint illi factores. Generaliter solutio congruentiae secundum modulum compositum quemcumque pendet a solutione aliarum congruentiarum, quarum moduli sunt factores illius numeri; hi autem, si commodum esse videtur, ita semper accipi possunt, vt sint numeri primi.

Ex. Si congruentia $19x \equiv 1$ (mod. 140) proponitur: soluatur primo secundum modulum 2, eritque $x \equiv 1$ (mod. 2). Ponatur $x = 1 + 2x'$, fietque $39x' \equiv -18$ (mod. 140) cui aequiualet $19x' \equiv -9$ (mod. 70). Si haec iterum secundum modulum 2 soluitur, fit $x' \equiv 1$ (mod. 2) positoque $x' = 1 + 2x''$, fit $38x'' \equiv -28$ (mod. 70) siue $19x'' \equiv -14$ (mod. 35). Haec secundum 5 soluta dat $x'' \equiv 4$ (mod. 5), substitutoque $x'' = 4 + 5x'''$, fit $95x''' \equiv -90$ (mod. 35) siue $19x''' \equiv -18$ (mod. 7). Ex hac tandem sequitur, $x''' \equiv 2$ (mod. 7), positoque $x''' = 2 + 7x^{IV}$ colligitur $x = 59 + 140x^{IV}$; quare $x \equiv 59$ (mod. 140) est solutio completa congruentiae propositae.

31. Simili modo vt aequationis $ax = b$ radix per $\frac{b}{a}$ exprimitur, etiam congruentiae $ax \equiv b$ radicem quamcunque per $\frac{b}{a}$ designabimus, congruentiae modulum, distinctionis gratia, ap-

ponentes. Ita e. g. $\frac{19}{17}$ (mod. 12) denotat quemuis numerum, qui est $\equiv 11$ (mod. 12) *). Generaliter ex praecedentibus patet, $\frac{b}{a}$ (mod. c) nihil reale significare (aut si quis malit aliquid imaginarii), si a, c habeant diuisorem communem, qui ipsum b non metiatur: At hoc casu excepto, expressio $\frac{b}{a}$ (mod. c) semper valores reales habebit, et quidem infinitos: hi vero omnes secundum c erunt congrui quando a ad c primus, aut secundum $\frac{c}{\delta}$, quando δ numerorum c, a diuisor communis maximus.

Hae expressiones similem fere habent algorithmum vt fractiones vulgares. Aliquot proprietates quae facile ex praecedentibus deduci possunt hic apponimus.

1. Si secundum modulum c, $a \equiv \alpha$, $b \equiv \beta$ expressiones $\frac{a}{b}$ (mod. c) et $\frac{\alpha}{\beta}$ (mod. c) sunt aequiualentes.
2. $\frac{a\delta}{b\delta}$ (mod. $c\delta$) et $\frac{a}{b}$ (mod. c) sunt aequiualentes.
3. $\frac{ak}{bk}$ (mod. c) et $\frac{a}{b}$ (mod. c) sunt aequiualentes quando k ad c est primus.

Multae aliae similes propositiones afferri possent: at quum nulli difficultati sint obnoxiae, neque ad sequentia adeo necessariae, ad alia properamus.

32. Problema quod magnum in sequentibus vsum habebit, *inuenire omnes numeros, qui secundum modulos quotcunque datos residua data praebent*, facile ex praecedentibus solui potest. Sint pri-

*) id quod ex analogia per $\frac{11}{1}$ (mod. 12) designari potest.