(mod. m.) exhibere resolutionem completam congruentiae $ax + b \equiv c$.

Quia resolutiones congruentiae per valores ipsius x congruos per se sunt obuiae, atque, hoc respectu, numeri congrui tamquam aequiualentes considerandi, tales congruentiae resolutiones pro vna eademque habebimus. Quamobrem quum nostra congruentia $ax + b \equiv c$ alias resolutiones non admittat, pronunciabimus, vnico tantum modo eam esse resolubilem seu vnam tantum radicem habere. Ita $e.\ g.$ congruentia $6x + 5 \equiv 13$ (mod. 11) alias radices non admittit, quam quae sunt $\equiv 5$ (mod. 11). Haud perinde res se habet in congruentiis altiorum graduum, siue etiam in congruentiis primi gradus, vbi incognita per numerum est multiplicata, ad quem modulus non est primus.

27. Superest, vt de inueniendа resolutione ipsa congruentiae huiusmodi, quaedam adiiciamus. Primo obseruamus, congruentiam formae $ax + t \equiv u$, cuius modulum ad a primum supponimus, ab hac, $ax \equiv \pm 1$, pendere: si enim huic satisfacit $x \equiv r$, illi satisfaciet $x \equiv \pm (u - t)\ r$. At congruentiae $ax \equiv \pm 1$, modulo per b designato, aequiualet aequatio indeterminata $ax = by \pm 1$, quae quomodo sit soluenda hoc quidem tempore abunde est notum; quare nobis sufficiet, calculi algorithmum huc transscripsisse.

Si quantitates A, B, C, D, E etc. ita ab his α, β, γ, δ, etc. pendent, vt habeatur $A = \alpha$, $B = \beta A + 1$, $C = \gamma B + A$, $D = \delta C + B$, $E = \varepsilon D$

$+ C$ etc., breuitatis gratia ita eas designamus, $A = [\alpha]$; $B = [\alpha, \beta]$; $C = [\alpha, \beta, \gamma]$, $D = [\alpha, \beta, \gamma, \delta]$ etc. *). Iam proposita sit aequatio indeterminata $ax = by \pm 1$, vbi a, b positiui. Supponamus, id quod licet, a esse non $< b$. Tum ad instar algorithmi noti, secundum quem duorum numerorum diuisor communis maximus inuestigatur, formentur per diuisionem vulgarem aequationes,

$a = \alpha b + c$
$b = \beta c + d$
$c = \gamma d + e$ etc.

ita vt α, β, γ etc. c, d, e etc. sint integri positiui, et b, c, d, e continuo decrescentes, donec perueniatur ad

$m = \mu n + 1$, quod tandem euenire debere constat. Erit itaque $a = [n, \mu, \ldots \gamma, \beta, \alpha]$; $b = [n, \mu \ldots \gamma, \beta]$. Tum fiat $x = [\mu, \ldots \gamma, \beta]$, $y = [\nu, \ldots \gamma \beta, \alpha]$, eritque $ax = by + 1$, quando numerorum $\alpha, \beta, \gamma \ldots \mu, n$ multitudo est par, aut $ax = by - 1$, quando est impar. *Q. E. F.*

28. Resolutionem generalem huiusmodi aequationum indeterminatarum ill. Euler pri-

*) Multo generalius haecce relatio considerari potest, quod negotium alia forsan occasione suscipiemus. Hic duas tantum propositiones adiicimus, quae vsum suum in praesenti inuestigatione habent; scilicet,

1°. $[\alpha, \beta, \gamma \ldots \lambda, \mu] \cdot [\beta, \gamma \ldots \lambda] - [\alpha, \beta, \gamma \ldots \lambda] [\beta, \gamma, \ldots \lambda, \mu] = \pm 1$, vbi signum superius accipiendum quando numerorum $\alpha, \beta, \gamma \ldots \lambda, \mu$ multitudo par, inferius quando impar.

2°. Numerorum α, β, γ etc. ordo inuerti potest, $[\alpha, \beta, \gamma \ldots, \lambda, \mu] = [\mu, \lambda \ldots \gamma, \beta, \alpha]$. Demonstrationes quae non sunt difficiles hic supprimimus.

mus docuit, *Comment. Petrop. T. VII. p.* 46. Methodus qua vsus est consistit in substitutione aliarum incognitarum loco ipsarum x, y, atque hoc quidem tempore satis est nota. Ill. la Grange paullo aliter rem aggressus est: scilicet ex theoria fractionum continuarum constat si fractio $\frac{b}{a}$ in fractionem continuam

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{etc.} + \cfrac{1}{\mu + \frac{1}{n}}}}}$$

conuertatur, haecque deleta vltima sui parte $\frac{1}{n}$ in fractionem communem $\frac{x}{y}$ restituatur, fore $ax = by \pm 1$, siquidem fuerit a ad b primus. Ceterum ex vtraque methodo idem algorithmus deriuatur. Inuestigationes ill. la Grange exstant *Hist. de l' Ac. de Berlin Année* 1767 *p.* 175, et cum aliis in *Supplementis versioni gallicae Algebrae Eulerianae adiectis.*

29. Congruentia $ax + t \equiv u$ cuius modulus ad a non primus, facile ad casum praecedentem reducitur. Sit modulus m, maximusque numerorum a, m diuisor communis δ. Primo patet quemuis valorem ipsius x congruentiae secundum modulum m satisfacientem eidem etiam secundum modulum δ satisfacere (art. 5). At semper $ax \equiv 0 \pmod{\delta}$ quoniam δ ipsum a metitur. Quare, nisi $t \equiv u \pmod{\delta}$ i. e. $t - u$ per δ diuisibilis, congruentia proposita non est resolubilis.