ſmo duo moduli, A, B, secundum quos numerus quaesitus, z, numeris a, b respectiue congruus esse debeat. Omnes itaque valores ipsius z sub forma $Ax + a$ continentur, vbi x est indeterminatus sed talis vt fiat $Ax + a \equiv b$ (mod. B). Quodsi iam numerorum A, B diuisor communis maximus est δ, resolutio completa huius congruentiae hanc habebit formam: $x \equiv v$ (mod. $\frac{B}{\delta}$) siue quod eodem redit, $x = v + \frac{kB}{\delta}$, denotante k numerum integrum arbitrarium. Hinc formula $Av + \frac{kAB}{\delta}$ omnes ipsius z valores comprehendet, i. e. $z \equiv Av$ (mod. $\frac{AB}{\delta}$) erit resolutio completa problematis. Si ad modulos A, B, tertius accedit, C, secundum quem numerus quaesitus z, debet esse $\equiv c$, manifesto eodem modo procedendum, quum binae priores conditiones in vnicam iam sint conflatae. Scilicet si numerorum $\frac{AB}{\delta}$, C diuisor communis maximus $= \epsilon$, atque congruentiae $\frac{AB}{\delta}x + Av \equiv c$ (mod. C) resolutio: $x \equiv w$ (mod. $\frac{C}{\epsilon}$), problema per congruentiam $z \equiv \frac{ABw}{\delta} + Av$ (mod. $\frac{ABC}{\epsilon}$) complete erit resolutum. Similiter procedendum, quotcunque moduli proponantur. Obseruari conuenit $\frac{AB}{\delta}$, $\frac{ABC}{\delta\epsilon}$ esse numerorum A, B; et A, B, C respectiue minimos communes diuiduos, facileque inde perspicitur, quotcunque habeantur moduli A, B, C etc., si eorum minimus communis diuiduus sit M, resolutionem completam hanc formam habere, $z \equiv r$ (mod. M). Ceterum quando vlla congruentiarum auxiliarum est irresolubilis, problema impossibilitatem inuoluere concludendum est. Perspicuum vero, hoc euenire non posse, quando omnes numeri A, B, C etc. inter se sint primi.

Ex. Sint numeri A, B, C; a, b, c, 504, 35, 16; 17, — 4, 33; hic duae conditiones vt z sit $\equiv 17$ (mod. 504) et $\equiv -4$ (mod. 35) vnicae, vt sit $\equiv 521$ (mod. 2520) aequiualent; ex qua cum hac: $z \equiv 33$ (mod. 16) coniuncta, promanat $z \equiv 3041$ (mod. 5040).

33. Quando omnes numeri A, B, C etc. inter se sunt primi, constat, productum ex ipsis esse minimum omnibus communem diuiduum. In quo casu manifestum est, omnes congruentias $z \equiv a$ (mod. A); $z \equiv b$ (mod. B) etc. vnicae $z \equiv r$ (mod. R) prorsus aequiualere, denotante R numerorum A, B, C etc. productum. Hinc vero vicissim sequitur, vnicam conditionem $z \equiv r$ (mod. R) in plures dissolui posse; scilicet si R quomodocunque in factores inter se primos A, B, C etc. resoluitur, conditiones $z \equiv r$ (mod. A), $z \equiv r$ (mod. B), $z \equiv r$ (mod. C), etc. propositam exhaurient. Haec obseruatio methodum nobis aperit non modo impossibilitatem, si quam forte conditiones propositae implicent, statim detegendi, sed etiam calculum commodius atque concinnius instituendi.

34. Sint vt supra conditiones propositae, vt sit $z \equiv a$ (mod. A) $z \equiv b$ (mod. B), $z \equiv c$ (mod. C). Resoluantur omnes moduli in factores inter se primos, A in A' A'' A''' etc.; B in B' B'' B''' etc. etc. et quidem ita vt numeri A', A'' etc. B', B'' etc. etc. sint aut primi, aut primorum potestates. Si vero aliquis numerorum A, B, C etc. iam per se est primus, aut primi potestas, nulla resolutione in factores pro hocce opus est. Tum vero ex praecedentibus pa-

tescit, pro conditionibus propositis hasce substitui posse: $z \equiv a$ (mod. A'), $z \equiv a$ (mod. A''), $z \equiv a$ (mod. A''') etc., $z \equiv b$ (mod. B'), $z \equiv b$ (mod. B'') etc. etc. Iam nisi omnes numeri A, B, C etc. fuerint inter se primi, ex. gr. si A ad B non primus, manifestum est, omnes diuisores primos ipsorum A, B diuersos esse non posse, sed inter factores A', A'', A''' etc. vnum aut alterum esse debere, qui inter B', B'', B''' etc. aut aequalem aut multiplum aut submultiplum habeat. Si *primo* $A' = B'$, conditiones $z \equiv a$ (mod. A'), $z \equiv b$ (mod. B') identicae esse debent, siue $a \equiv b$ (mod. A' vel B'), quare alterutra reiici poterit. Si vero non $a \equiv b$ (mod. A'), problema impossibilitatem implicat. Si *secundo* B' multiplum ipsius A', conditio $z \equiv a$ (mod. A') in hac $z \equiv b$ (mod. B') contenta esse debet, siue haec $z \equiv b$ (mod. A') quae ex posteriori deducitur cum priori identica esse debet. Vnde sequitur conditionem $z \equiv a$ (mod. A'), nisi alteri repugnet (in quo casu problema impossibile) reiici posse. Quando omnes conditiones superfluae ita reiectae sunt, patet, omnes modulos ex his A', A'', A''' etc., B', B'', B''' etc. etc. remanentes inter se primos fore: tum igitur de problematis possibilitate certi esse et secundum praecepta ante data procedere possumus.

35. Ex. Si ut supra esse debet $z \equiv 17$ (mod. 504); $\equiv -4$ (mod. 35), et $\equiv 33$ (mod. 16); hae conditiones in sequentes resolui possunt, $z \equiv 17$ (mod 8), $\equiv 17$ (mod. 9), $\equiv 17$ (mod. 7); $\equiv -4$ (mod. 5), $\equiv -4$ (mod. 7); $\equiv 33$ (mod. 16). Ex his conditiones $z \equiv 17$ (mod. 8), $z \equiv 17$ (mod. 7) reiici possunt,