Quemadmodum hic ex sola inspectione cognoscitur, ex iis numeris primis *qui in hac schematis parte continentur* solum 127 post exclusiones cum residuis — 6, 13 etc. in Ω relinqui, ita schema integrum vsque ad 997 extensum ostendit, *omnino* nullum alium ex Ω remanere; diuisione autem tentata, 997331 per 127 reuera diuisibilis inuenitur. Hoc itaque modo ille numerus in factores primos 127×7853 resolutus habetur *).

Ceterum ex hac expositone abunde colligitur, praesertim vtilia esse residua non nimis magna, aut saltem in factores primos non nimis magnos resolubilia, quum tabulae auxiliaris vsus immediatus non vltra numeros in facie positos pateat, vsusque mediatus tales tantum complectatur, qui in factores in tabula contentos resolui possunt.

332. Ad inuenienda residua numeri dati M tres methodos diuersas trademus, quarum expositioni duas obseruationes praemittimus, quarum adiumento e residuis minus idoneis simpliciora deriuari possunt. *Primo*, si numerus akk per quadratum kk diuisibilis (quod ad M primum esse supponitur) est residuum ipsius M, etiam a erit residuum; propter hanc rationem residua

*) Auctor apparatum satis amplum tabulae hic descriptae, quem ad vsum suum construendum curauit, publici iuris lubenter faceret, si paucitas eorum, quibus vsui esse potest, sumtibus talis incepti sustentandis sufficeret. Si quis interea arithmeticae amator, principiis probe penetratis, proprio marte talem tabulam sibi condere optat, auctor magnae voluptati sibi ducet, omnia cum eo emolumenta ac artificia per literas communicare.

per magna quadrata diuisibilia aeque vtilia sunt ac parua; omniaque residua per methodos sequentes suppeditata a factoribus suis quadratis statim liberata supponemus. *Secundo* si duo pluresue numeri sunt residua, etiam productum ex ipsis residuum erit. Combinando hanc obseruationem cum praec., persaepe e pluribus residuis quae non omnia sunt satis simplicia aliud admodum simplex deduci potest, si modo illa multos factores communes implicant. Hanc ob caussam talia quoque residua valde sunt opportuna, quae e multis factoribus non nimis magnis composita sunt, conuenietque omnia statim in factores suos resoluere. Vis harum obseruationum melius per exempla vsumque frequentem quam per praecepta percipietur.

I. Methodus simplicissima, iisque, qui per frequentem exercitationem iam aliquam dexteritatem sibi conciliauerunt, commodissima, consistit in eo, vt M aut generalius multiplum quodcunque ipsius M quomodocunque in duas partes decomponatur $kM = a + b$ (siue vtraque sit positiua siue altera positiua altera negatiua) quarum productum signo mutato erit residuum ipsius M; erit enim $-ab \equiv aa \equiv bb$ (mod. M), adeoque $-abRM$. Numeri a, b ita accipiendi sunt, vt productum per quadratum magnum diuisibile quotiensque vel paruus vel saltem in factores non nimis magnos resolubilis euadat, quod semper non difficile effici poterit. Imprimis commendandum est, vt pro a accipiatur vel quadratum, vel quadratum duplex, vel triplex etc. a numero M numero vel paruo vel in factores commodos resolubili discrepans. Ita e. g. inuenitur $997331 = 999^2 - 2.5.67 = 994^2 + 5.11.13^2 = 2.706^2 + 3.17.3^2 = 3.575^2 + 11.31.4^2 = 3.577^2 - 7.13.4^2 = 3.578^2 - 7.19.37 = 11.299^2 + 2.3.5.29.4^2 = 11.301^2 + 5.11^2$ etc. Hinc habentur residua sequentia $2.5.67$, -5.11, $-2.3.17$, $-3.11.31$, $3.7.13$, $3.7.19.37$, $-2.3.5.11.29$; discerptio vltima suppeditat residuum -5.11 quod iam habemus. Pro residuis $-3.11.31$, $2.3.5.11.29$ haec adoptare possumus $3.5.31$, $2.3.29$, ex illorum combinatione cum -5.11 oriunda.

II. Methodus secunda et tertia inde petuntur, quod, si duae formae binariae (A, B, C), (A', B', C') eiusdem determinantis M, aut $-M$, aut generalius $\pm kM$, ad idem genus pertinent, numeri AA', AC', $A'C$ sunt residua ipsius kM; hoc nullo negotio inde perspicitur, quod numerus quiuis characteristicus vnius formae, puta m, etiam est numerus char. alterius, adeoque mA, mC, mA', mC' omnes residua ipsius hM. Si itaque (a, b, a') est forma reducta determinantis positiui M aut generalius kM, atque (a', b', a''), (a'', b'', a''') etc. formae ex ipsius periodo, adeoque ipsi aequiualentes et a potiori sub eodem genere contentae: numeri aa', aa'', aa''' etc. omnes erunt residua ipsius M. Computus multitudinis magnae formarum talis periodi facillime adiumento algorithmi art. 187. instituitur; residua simplicissima plerumque prodeunt statuendo $a = 1$; ea quae factores nimis magnos implicant, erunt reiicienda. Ecce initia periodorum formarum $(1, 998, -1327)$ et $(1, 1412,$