us arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupauisse, tam notum est, vt de hac re copiose loqui superfluum foret. Nihilominus fateri oportet, omnes methodos hucusque prolatas vel ad casus valde speciales restrictas esse, vel tam operosas et prolixas, vt iam pro numeris talibus, qui tabularum a viris meritis constructarum limites non excedunt, i. e. pro quibus methodi artificiales superuacuae sunt, calculatoris etiam exercitati patientiam fatigent, ad maiores autem plerumque vix applicari possint. Etsi vero illae tabulae, quae in omnium manibus versantur, et quas subinde adhuc vlterius continuatum iri sperare licet, in plerisque casibus vulgo occurrentibus vtique sufficiant: tamen calculatori perito occasio haud raro se offert, e numerorum magnorum resolutione in factores magna emolumenta capiendi, quae temporis dispendium mediocre largiter compensent; praetereaque scientiae dignitas requirere videtur, vt omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur. Propter has rationes non dubitamus, quin duae methodi sequentes, quarum efficaciam ac breuitatem longa experientia confirmare possumus, arithmeticae amatoribus haud ingratae sint futurae. Ceterum in problematis natura fundatum est, vt methodi *quaecunque* continuo prolixiores euadant, quo maiores sunt numeri ad quos applicantur; attamen pro methodis sequentibus difficultates perlente increscunt, numerique e septem, octo vel adeo adhuc pluribus figuris constantes praesertim per secundam felici semper successu tra-

ctati fuerunt, omnique celeritate, quam pro tantis numeris exspectare aequum est, qui secundum omnes methodos hactenus notas laborem, etiam calculatori indefatigabili intolerabilem, requirerent.

Antequam methodi sequentes in vsum vocentur, semper vtilissimum est, diuisionem numeri cuiusque propositi per aliquot numeros primos minimos tentare, puta per 2, 3, 5, 7 etc. vsque ad 19 aut adhuc vlterius, non solum, ne poeniteat, talem numerum quando diuisor est per methodos subtiles ac artificiosas eruisse, qui multo facilius per solam diuisionem inueniri potuisset *), sed etiam, quod tunc, vbi nulla diuisio successit, applicatio methodi secundae *residuis* ex illis diuisionibus ortis magno cum fructu vtitur. Ita e. g. si numerus 314159265 in factores suos resoluendus est, diuisio per 3 bis succedit, posteaque etiam diuisiones per 5 et 7, vnde habetur $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$, sufficitque numerum 997331, qui per 11, 13, 17, 19 non diuisibilis inuenitur, examini subtiliori subiicere. Similiter proposito numero 43429448, factorem 8 auferemus, methodosque magis artificiales ad quotientem 5428681 applicabimus.

330. Fundamentum METHODI PRIMAE est theorema, *quemuis numerum positiuum seu negatiuum, qui alius numeri M residuum quadraticum sit, etiam residuum cuiusuis diuisoris*

*) Eo magis, quod inter sex numeros, generaliter loquendo, vix *vnus* per omnes 2, 3, 5 ... 19 non diuisibilis reperitur.

ipsius M esse. Vulgo notum est, si M per nullum numerum primum infra $\sqrt{M}$ diuisibilis sit, certo M esse primum; si vero omnes numeri primi infra hunc limitem, ipsum M metientes sint p, q etc., numerum M vel ex his *solis* (ipsorumue potestatibus) compositum esse, vel *vnum* tantum alium factorem primum maiorem quam $\sqrt{M}$ implicare posse, qui inuenitur, diuidendo ipsum M per p, q etc. quoties licet. Designando itaque complexum omnium numerorum primorum infra $\sqrt{M}$ (exclusis iis, per quos diuisio frustra iam tentata est) per Ω, manifesto sufficit, si omnes diuisores primi ipsius M, in Ω contenti, habeantur. Iam si alicunde constat, numerum aliquem r (non-quadratum) esse residuum quadraticum ipsius M, nullus certo numerus primus cuius NR est r diuisor ipsius M esse poterit; quare ex Ω omnes huiusmodi numeros primos (qui plerumque omnium semissem fere efficient) eiicere licebit. Si insuper de alio numero non quadrato, r', constat, ipsum esse residuum ipsus M, e numeris primis in Ω post primam exclusionem relictis iterum eos excludere poterimus, quorum $N.R$ est r', qui rursus illorum semissem fere conficient, siquidem residua r et r' sunt independentia, (*i. e.* nisi alterum necessario per se est residuum omnium numerorum, quorum residuum est alterum, quod eueniret quando rr' esset quadratum). Si adhuc alia residua ipsius M noti sunt, r'', r''' etc., quae omnia a reliquis sunt independentia *), cum singulis ex-

*) Si productum e numeris quotcunque r, r', r'' etc. quadratum est; quisque ipsorum e, g, r erit residuum cuiusuis