183. Totum ergo negotium huc redit, ut numeri b id investigetur multiplum pb, quod per d divisum unitatem relinquat. Cum itaque $pb-1$ per d sit divisibile, posito $pb-1=qd$, numeros p et q investigari oportet, ut fiat $pb-qd=1$. Semper autem p infra d assignari poterit.

184. Saepe ejusmodi productum πb facilius reperitur, quod per d divisum relinquat $d-1$, seu -1; tum autem hoc productum $(d-\pi)b$ residuum praebebit $=+1$, ita ut invento π futurum sit $p=d-\pi$. Tum igitur terminus $a+((\alpha-r)\pi\pm\mu d)b$ datum residuum r relinquat.

185. Consideremus nunc etiam residua, quae oriuntur si differentia progressionis b et divisor d non fuerint numeri inter se primi. Atque jam vidimus, si factor communis sit φ, ut sit $b=B\varphi$ et $d=D\varphi$, jam terminum $a+Db$ idem praebere residuum, quod primus a.

186. Quare si φ fuerit maximus factor communis numerorum b et d, quoniam primum residuum a, vel α demum in termino $a+Db$ recurrit, plura residua diversa locum habere nequeunt, quam numero D: neque ergo omnes numeri divisore d minores inter residua occurrent.

187. Quo haec residua facilius scrutemur, ponamus esse $a=0$, sintque termini progressionis cum suis residuis:

Indices	1	2	3	4	D
Termini	0,	$B\varphi$,	$2B\varphi$,	$3B\varphi$,	$\ldots\ldots(D-1)B\varphi$
Residua	0,	$\beta\varphi$,	$\gamma\varphi$,	$\delta\varphi$,	$\lambda\varphi$

manifestum enim est, si hi termini per $d=D\varphi$ dividantur, residua quoque per φ esse divisibilia.

188. Nam si mB divisum per D praebeat residuum r, erit $mB=nD+r$, ideoque $mB\varphi=nD\varphi+r\varphi$. Unde si $mB\varphi$ per $D\varphi=d$ dividatur, residuum erit $r\varphi$, multiplum ipsius φ. Cum igitur pro r omnes numeri ipso D minores prodire queant, etiam inter illa residua omnia multipla ipsius φ, quae quidem divisorem $d=D\varphi$ non superant, occurrere debent, quorum multitudo utique est $=D$.

189. Si ad singulos terminos adjiciamus numerum a, eodem singula residua augebuntur, quae ergo ita se habebunt, existente $b=B\varphi$ et $d=D\varphi$:

Indices	1	2	3	4	5	D
Termini	a,	$a+b$,	$a+2b$,	$a+3b$,	$a+4b\ldots\ldots$	$a+(D-1)b$
Residua	a,	$a+\beta\varphi$,	$a+\gamma\varphi$,	$a+\delta\varphi$,	$a+\varepsilon\varphi$,	$a+\lambda\varphi$

ubi series β, γ, δ, $\varepsilon\ldots\lambda$ omnes numeros ipso D minores continet.

190. Hoc ergo casu ex serie residuorum excluduntur omnes numeri, qui numero a minuti non sunt divisibiles per φ, seu maximum communem divisorem differentiae b et divisoris d.

191. Cum numeri B et D sint primi inter se, ejusmodi multiplum prioris, puta mB, exhiberi potest, quod per D divisum, datum relinquat residuum r; tum autem nostrae progressionis terminus $a+mB\varphi$, seu $a+mb$ per $D\varphi=d$ divisus, relinquet residuum $a+r\varphi$ (*).

Caput VII.

De residuis ex divisione terminorum progressionis geometricae ortis.

192. Progressionem geometricam in genere ita repraesentamus: a, ab, ab^2, ab^3, ab^4, ab^5, etc.

(*) *Script. ad marg.* Methodus definiendi formulam $ax+b$, ut ea per datum numerum d fiat divisibilis.

cujus termini, si per numerum quemcunque d dividantur, ejusmodi dabunt residua, quae facile ex residuis hujus progressionis $1, b, b^2, b^3$, etc. colligi possunt, his scilicet per a multiplicandis.

193. Haec ergo de residuis quaestio ad meras potestates revocatur, ita ut residuum definiendum sit, quod potestas quaecunque b^n per datum numerum d divisa relinquit. Ubi quidem casus distingui convenit, quibus numeri b et d sunt vel primi inter se, vel compositi.

194. Si sit $b = p\varphi$ et $d = q\varphi$, quaeratur residuum ex $p^n\varphi^{n-1}$ ortum, si per q dividatur; illudque per φ multiplicatum dabit residuum ortum ex divisione numeri $p^n\varphi^n$ per $q\varphi$, hocque modo deducimur ad divisionem ejusmodi potestatis b^n per d, ubi b et d sint numeri inter se primi.

195. Sint ergo b et d numeri inter se primi, et residua ex divisione potestatum ipsius b oriunda ita indicentur:

Potestates $1, b, b^2, b^3, b^4, b^5, b^6, b^7$, etc.
Residua $1, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta$, etc.

quae omnia ad divisorem d quoque erunt prima, quia d ad omnes potestates ipsius b est primus.

196. Quia haec residua $1, \alpha, \beta, \gamma, \delta$, etc. omnia sunt minora quam d, ea omnia a se invicem diversa esse non possunt. Quin si multitudo numerorum, ad d primorum eoque simul minorum, sit μ, plura residua diversa resultare nequeunt, quam μ continet unitates.

197. Cum ergo innumerabiles potestates paria praebeant residua, si ponamus b^m et b^{m+n} idem dare residuum, harum potestatum differentia $b^{m+n} - b^m = b^m(b^n - 1)$ per d erit divisibilis. Quia igitur b^m ad d est primus, sequitur $b^n - 1$ per d esse divisibile, seu potestatem b^n dare residuum $= 1$.

198. Quia plura quam μ residua diversa occurrere nequeunt, si progressio ad terminum b^μ continuetur, ob terminorum numerum $= \mu + 1$, unum saltem residuum bis occurret, sicque casus ante positus contingat, antequam $m + n$ superet μ, unde potestas b^n residuum $= 1$ reproducens dabitur, ita ut n non superet μ.

199. Ponamus post unitatem b^n infimam esse potestatem, quae per d divisa unitatem relinquat, atque sequentes potestates b^{n+1}, b^{n+2}, b^{n+3}, etc. eadem praebebunt residua, quae potestates initiales b, b^2, b^3, etc. donec perveniatur ad potestatem b^{2n}, quae iterum unitatem pro residuo relinquet.

200. Cum igitur a potestate b^n progrediendo eadem residua recurrant, atque ab initio, non solum omnes potestates b^0, b^n, b^{2n}, b^{3n}, b^{4n}, etc. idem relinquent residuum 1, sed etiam hae b^1, b^{n+1}, b^{2n+1}, b^{3n+1}, b^{4n+1}, etc. idem habebunt residuum, quin etiam istae b^m, b^{n+m}, b^{2n+m}, b^{3n+m}, etc. per d divisae aequalia residua relinquent.

201. Posita ergo b^n infima potestate unitatem pro residuo relinquente, ita ut n non excedat μ, multitudinem numerorum ipso d minorum ad eumque primorum, omnes antecedentes potestates $1, b, b^2, b^3, \ldots b^{n-1}$ disparia praebebunt residua, quae deinceps eodem ordine recurrent. Si enim duo eorum essent paria, minor valor pro n haberetur, contra hypothesin.

202. Quodsi ergo in residuis omnes numeri ad divisorem d primi eoque minores occurrant, quorum multitudo est $= \mu$, erit $n = \mu$, atque $b^\mu - 1$ per d erit divisibile. Sin autem non omnes illi numeri ad d primi inter residua occurrant, necesse est, ut sit $n < \mu$. Ostendemus autem his casibus n esse partem aliquotam ipsius μ.

203. Si non omnes numeri ad d primi eoque minores, quorum multitudo est $= \mu$, inter residua, quorum multitudo est $= n$, occurrant, eos, qui ex ordine residuorum excluduntur, nomine *non-residuorum* appellabo, ita ut multitudo residuorum n cum multitudine non-residuorum exhaurire debeat numerum μ.

204. Si in serie residuorum $1, \alpha, \beta, \gamma$, etc. occurrant numeri r et s, in ea quoque occurret numerus rs, seu residuum ipsi aequivalens. Si enim residua r et s respondeant potestatibus b^ϱ et b^σ, potestati $b^{\varrho+\sigma}$ respondebit residuum rs. Hinceque inter residua occurret numerus $r^f s^g$, sumtis exponentibus f et g utcunque.

205. Vicissim si potestati b^ϱ conveniat residuum r, potestati vero $b^{\varrho+\sigma}$ residuum rs, vel $rs - \lambda d$, tum potestati b^σ conveniet residuum s. Nam producto $b^\varrho s$ conveniet residuum rs, idem quod potestati $b^{\varrho+\sigma}$; hinc differentia $b^{\varrho+\sigma} - b^\varrho s = b^\varrho (b^\sigma - s)$ per d erit divisibilis. Quare cum b^ϱ ad d sit primus, necesse est sit $b^\sigma - s$ per d divisibile, sicque potestati b^σ respondebit residuum s.

206. Si ergo numeri r et rs inter residua reperiantur, certum est et numerum s ibidem repertum iri. Quodsi jam series residuorum $1, \alpha, \beta, \gamma, \delta$, etc., quorum numerus est $= n$, non omnes numeros ipso d minores, ad eumque primos complectatur, quorum multitudo est $= \mu$, dabitur unus pluresve, quos in classem non-residuorum referri oportet.

207. Sit x tale non-residuum, ac manifestum est etiam hos numeros $\alpha x, \beta x, \gamma x, \delta x$, etc. inter non-residua reperiri, nam si αx in residuis inveniretur, quia α ibidem extat, etiam x ibidem reperiri deberet, contra hypothesin. Ex unico ergo non-residuo necessario sequuntur tot non-residua quot habentur residua, scilicet numero n. Sunt enim haec non-residua inter se aeque disparia ac ipsa residua $1, \alpha, \beta, \gamma, \delta$, etc. ac si ibi duo aequalia darentur, etiam hic talia esse deberent, quod foret absurdum (*).

208. Statim ergo atque est $n < \mu$, ad minimum dantur n non-residua, quae si omnia complectantur, erit tam residuorum quam non-residuorum numerus $= n + n$, ipsi μ aequandus, unde fit $n = \frac{\mu}{2}$; hinc si $n < \mu$, fieri nequit, ut numerus residuorum n semissem numeri μ superet.

209. Si in modo expositis non-residuis $x, \alpha x, \beta x, \gamma x$, etc. non omnia occurrant, sit y numerus $< d$ ad eumque primus, qui neque in his non-residuis neque residuis reperiatur, atque simili modo etiam hi numeri $\alpha y, \beta y, \gamma y$, etc. a praecedentibus diversi, ad non-residua referri debent, sicque denuo n numeri ad non-residua accedunt.

210. Si his duobus ordinibus nondum omnia non-residua exhauriantur, novus ordo accedet, pariter n terminis constans, ac fortasse denuo novus totidem constans terminis; unde colligitur numerum omnium non-residuorum, nisi sit nullus, vel ipsi numero n, vel ejus duplo, vel triplo, vel in genere multiplo cuicunque aequari.

211. Cum igitur omnia non-residua una cum residuis multitudinem omnium numerorum ipso divisore d minorum ad eumque primorum exhaurire debeant, erit vel $n = \mu$, vel $2n = \mu$, vel $3n = \mu$ etc. sicque semper exponens n est pars aliquota numeri μ.

(*) *Script. ad marg.* Si x et y non-residua, erit $y = \alpha x$ et $xy = \alpha xx$; jam si numerus non-residuorum = numero residuorum, demonstrandum est xx inter residua contineri.

212. Quodsi ergo b et d sint numeri inter se primi, et μ denotet multitudinem omnium numerorum ad d primorum ipsoque minorum, tum vero b^n fuerit minima potestas post casum $n=0$, quae per d divisa unitatem relinquat, tum erit vel $n=\mu$, vel n aequabitur parti cuipiam aliquotae ipsius μ, ita ut sit $n=\frac{\mu}{m}$, existente m divisore quopiam ipsius μ.

213. Cum autem post potestatem b^n etiam omnes istae b^{2n}, b^{3n}, b^{4n}, etc. unitatem pro residuo agnoscant, semper potestas $b^{mn}=b^{\mu}$ per d divisa unitatem relinquet. Hinc dum b et d fuerint numeri inter se primi, haec formula $b^{\mu}-1$ semper per numerum d erit divisibilis.

214. Si praeterea etiam c et d fuerint numeri inter se primi, quoniam $c^{\mu}-1$ divisionem per d admittit, harum formularum differentia $b^{\mu}-c^{\mu}$ semper per numerum d erit divisibilis, dummodo uterque numerus b et c ad d fuerit primus.

215. Si pro d sumamus numerum primum p, erit $\mu=p-1$, atque haec formula $b^{p-1}-1$ semper erit per p divisibilis, nisi ipse numerus b fuerit multiplum ipsius p. Fieri autem potest, ut forma simplicior b^n-1 etiam divisionem per p admittat, ubi autem necessario requiritur, ut exponens n sit pars aliquota ipsius $p-1$.

216. Si divisor sit $d=pq$, existentibus p et q numeris primis inaequalibus, neque b alterutrum horum numerorum complectatur, tum ob $\mu=(p-1)(q-1)$, haec forma $b^{(p-1)(q-1)}-1$ per d erit divisibilis.

217. Ac si existentibus p, q, r, s numeris primis inaequalibus, fuerit $d=p^{\lambda}q^{\mu}r^{\nu}s^{\xi}$, ac b numerus quicunque ad d primus, tum posito

$$m=p^{\lambda-1}(p-1)\,q^{\mu-1}(q-1)\,r^{\nu-1}(r-1)\,s^{\xi-1}(s-1),$$

haec forma b^m-1 semper per d erit divisibilis, atque interdum fieri potest, ut formula simplicior b^n-1, existente n parte quapiam aliquota ipsius m, divisibilis evadat.

218. Sed retineamus divisorem generalem d, sitque μ multitudo numerorum ipso minorum ad eumque primorum, pro b autem sumatur numerus quicunque ad d primus, cujus minima potestas per d divisa unitatem relinquens sit b^n, atque vidimus necessario fore vel $n=\mu$, vel $n=\frac{1}{2}\mu$, vel $n=\frac{1}{3}\mu$, vel $n=\frac{1}{4}\mu$, vel $n=\frac{1}{5}\mu$, siquidem μ tales partes aliquotas admittat; quos casus diligentius evolvi conveniet.

219. Statim quidem suspicari licet, hoc discrimen ab indole numeri b pendere, ita ut pro dato divisore d, certi numeri pro b sumti praebeant $n=\mu$, alii $n=\frac{1}{2}\mu$, alii $n=\frac{1}{3}\mu$, alii $n=\frac{1}{4}\mu$, seu adhuc minori parti aliquotae ipsius μ.

220. Quaecunque autem n sit pars aliquota ipsius μ, si binae potestates b^n et c^n unitatem relinquant, etiam composita $(bc)^n$ unitatem relinquet. Deinde etiam manifestum est potestatem $(b\pm\lambda d)^n$ per d divisam, esse relicturam unitatem.

221. Cum potestas b^{μ} semper unitatem relinquat, quaeramus numeros pro b sumendos, ut etiam $b^{\frac{1}{2}\mu}$ unitatem relinquat, quo casu ante omnia necesse est ut μ sit numerus par, quod quidem semper evenit nisi sit $d=2$.

222. Si jam capiatur $b = ee$, ita ut e sit numerus ad d primus, certum est $b^{\frac{1}{2}\mu} = e^{\mu}$ unitatem relinquere, quod etiam evenit si $b = ee \pm \lambda d$. Minores ergo numeri pro b sumendi sunt residua, quae ex divisione numerorum quadratorum per d resultant, si modo quadrata ad d fuerint prima.

223. Simili modo potestas $b^{\frac{1}{3}\mu}$ per d divisa unitatem relinquet, si fuerit $b = e^3$, et generalius si $b = e^3 \pm \lambda d$. Minores ergo valores ipsius b idonei sunt residua, ex divisione cuborum ad d primorum per ipsum numerum d orta. Evidens autem est hoc evenire non posse, nisi numerus μ sit per 3 divisibilis.

224. Si μ per 4 sit divisibile, tum potestas $b^{\frac{1}{4}\mu}$ per d divisa unitatem relinquet, si fuerit $b = e^4$, et generalius $b = e^4 \pm \lambda d$. Minores ergo numeri sunt residua, quae ex divisione biquadratorum per d oriuntur, iis scilicet tantum biquadratis sumendis, quae ad d sunt prima.

225. In genere ergo, si numerus μ divisibilis sit per ν, potestas $b^{\frac{\mu}{\nu}}$ per d divisa unitatem relinquet, si capiatur $b = e^{\nu}$, vel adeo $b = e^{\nu} \pm \lambda d$, ita ut idonei numeri pro b substituendi sint residua, quae ex divisione potestatum ordinis ν per numerum d oriuntur, potestatibus illis ad d existentibus primis.

226. Sufficit ergo pro b numeros sumsisse ipso d minores, qui quidem ad eum sint primi; atque unitas quidem pro b sumta omnia residua unitati aequalia reddit, ita ut hoc casu semper sit $n = 1$, seu $n = \frac{\mu}{\mu}$. Casus autem iste solus relinquitur, si capiatur divisor $d = 2$, quippe quo fit $\mu = 1$.

227. Sit divisor $d = 3$, erit $\mu = 2$, et praeter casum $b = 1$, quo $n = 1$, habebimus casum $b = 2$, unde oritur progressio geometrica cum suis residuis:

Progr. geom.	1,	2,	2^2,	2^3,	2^4,	etc.,	ubi est $n = 2$,
Residua	1,	2,	1,	2,	1,	etc.,	seu $n = \mu$.

228. Sit divisor $d = 4$, erit $\mu = 2$, et praeter casum $b = 1$, quo $n = 1 = \frac{1}{2}\mu$, habemus casum $b = 3$.

Progr. geom.	1,	3,	3^2,	3^3,	3^4,	etc.,	hinc ergo fit $n = 2 = \mu$
Residua	1,	3,	1,	3,	1,	etc.	

229. Sit divisor $d = 5$, erit $\mu = 4$, et habebimus hos casus

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Progr. geom.	1, 1	1, 2, 2^2, 2^3, 2^4	1, 3, 3^2, 3^3, 3^4	1, 4, 4^2
Residua	1, 1	1, 2, 4, 3, 1	1, 3, 4, 2, 1	1, 4, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

duobus ergo casibus hic est $n = 4$, uno $n = 2$ et uno $n = 1$.

230. Si divisor $d = 6$, erit $\mu = 2$, et duo erunt casus

	$b = 1$	$b = 5$
Progr. geom.	1, 1	1, 5, 5^2
Residua	1, 1	1, 5, 1
	$n = 1$	$n = 2$

231. Si divisor $d = 7$, erit $\mu = 6$ totidemque habentur casus

	$b=1$	$b=2$	$b=3$	$b=4$
Progr. geom.	$1, 1$	$1, 2, 2^2, 2^3$	$1, 3, 3^2, 3^3, 3^4, 3^5, 3^6$	$1, 4, 4^2, 4^3$
Residua	$1, 1$	$1, 2, 4, 1$	$1, 3, 2, 6, 4, 5, 1$	$1, 4, 2, 1$
	$n=1$	$n=3$	$n=6$	$n=3$

	$b=5$	$b=6$
Progr. geom.	$1, 5, 5^2, 5^3, 5^4, 5^5, 5^6$	$1, 6, 6^2$
Residua	$1, 5, 4, 6, 2, 3, 1$	$1, 6, 1$
	$n=6$	$n=2$

232. Si divisor $d = 8$, erit $\mu = 4$ totidemque casus

	$b=1$	$b=3$	$b=5$	$b=7$
Prog. geom.	$1, 1$	$1, 3, 3^2$	$1, 5, 5^2$	$1, 7, 7^2$
Residua	$1, 1$	$1, 3, 1$	$1, 5, 1$	$1, 7, 1$
	$n=1$	$n=2$	$n=2$	$n=2$

nullo ergo casu erit $n = \mu$, sed tribus $n = \frac{1}{2}\mu$, et uno casu $n = \frac{1}{4}\mu$.

233. Si divisor sit $d = 9$, erit $\mu = 6$ totidemque casus

	$b=1$	$b=2$	$b=4$
Prog. geom.	$1, 1$	$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6$	$1, 4, 4^2, 4^3$
Residua	$1, 1$	$1, 2, 4, 8, 7, 5, 1$	$1, 4, 7, 1$
	$n=1$	$n=6$	$n=3$

	$b=5$	$b=7$	$b=8$
Progr. geom.	$1, 5, 5^2, 5^3, 5^4, 5^5, 5^6$	$1, 7, 7^2, 7^3$	$1, 8, 8^2$
Residua	$1, 5, 7, 8, 4, 2, 1$	$1, 7, 4, 1$	$1, 8, 1$
	$n=6$	$n=3$	$n=2$

234. Si sit divisor $d = 10$, erit $\mu = 4$

	$b=1$	$b=3$	$b=7$	$b=9$
Progr. geom.	$1, 1$	$1, 3, 3^2, 3^3, 3^4$	$1, 7, 7^2, 7^3, 7^4$	$1, 9, 9^2$
Residua	$1, 1$	$1, 3, 9, 7, 1$	$1, 7, 9, 3, 1$	$1, 9, 1$
	$n=1$	$n=4$	$n=4$	$n=2$

235. Sit $d = 11$, erit $\mu = 10$ totidemque casus

	$b=1$	$b=2$	$b=3$
Progr. geom.	$1, 1$	$1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$	$1, 3, 3^2, 3^3, 3^4, 3^5$
Residua	$1, 1$	$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$	$1, 3, 9, 5, 4, 1$
	$n=1$	$n=10$	$n=5$

	$b=4$	$b=5$
Progr. geom.	$1, 4, 4^2, 4^3, 4^4, 4^5$	$1, 5, 5^2, 5^3, 5^4, 5^5$
Residua	$1, 4, 5, 9, 3, 1$	$1, 5, 3, 4, 9, 1$
	$n=5$	$n=5$

	$b=6$	$b=7$
Progr. geom.	$1, 6, 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, 6^8, 6^9, 6^{10}$	$1, 7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7, 7^8, 7^9, 7^{10}$
Residua	$1, 6, 3, 7, 9, 10, 5, 8, 4, 2, 1$	$1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1$
	$n=10$	$n=10$

	$b=8$
Progr. geom.	$1, 8, 8^2, 8^3, 8^4, 8^5, 8^6, 8^7, 8^8, 8^9, 8^{10}$
Residua	$1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1$
	$n=10$

	$b=9$	$b=10$
Progr. geom.	$1, 9, 9^2, 9^3, 9^4, 9^5$	$1, 10, 10^2$
Residua	$1, 9, 4, 3, 5, 1$	$1, 10, 1$
	$n=5$	$n=2$

236. Sit $d=12$, erit $\mu=4$ totidemque casus

	$b=1$	$b=5$	$b=7$	$b=11$
Progr. geom.	$1, 1$	$1, 5, 5^2$	$1, 7, 7^2$	$1, 11, 11^2$
Residua	$1, 1$	$1, 5, 1$	$1, 7, 1$	$1, 11, 1$
	$n=1$	$n=2$	$n=2$	$n=2$

hic ergo semper est $n<\mu$, tribus casibus scilicet $n=\frac{1}{2}\mu$, et uno $n=\frac{1}{4}\mu$.

237. Si sit divisor $d=13$; erit $\mu=12$, et pro minima potestate b^n, quae per 13 divisa relinquit unitatem, reperitur

si $b=1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,$
est $n=1, 12, 3, 6, 4, 12, 12, 4, 3, 6, 12, 2.$

238. Quemadmodum semper si $b=1$ fit $n=1$, quicunque fuerit divisor d, ita etiam sumto $b=d-1$, fit $n=2$, seu $(d-1)^2$ per d divisum relinquit unitatem, quod in potestate prima nunquam contingit. De reliquis autem valoribus pro b assumtis difficilius est judicium.

239. Quoniam potestas $(kd+1)^n$ per d divisa relinquit 1, si fuerit $kd+1=bc$, et potestas b^n per d divisa relinquat etiam unitatem, tum quoque potestas c^n unitatem relinquet. Cum enim b^n relinquat 1, productum b^nc^n relinquet c^n, ac per hypothesin b^nc^n relinquit 1; ergo in aestimatione residuorum c^n aequivalet unitati, seu c^n per d divisum unitatem relinquet.

240. Quare si b^n fuerit minima potestas per d divisa unitatem relinquens, sitque $bc=kd+1$, minima potestas ipsius c unitatem relinquens vel erit c^n, vel adhuc minor, exponente existente parte

aliquota ipsius n. At si minor potestas ipsius c, puta $c^{\frac{n}{\nu}}$, relinqueret unitatem, etiam talis potestas ipsius b relinqueret unitatem, quod cum sit contra hypothesin, sequitur, si b^n fuerit minima potestas unitatem relinquens, etiam c^n fore minimam potestatem 1 relinquentem.

241. Ita posito $d = 13$, quia 5^4 est minima potestas unitatem relinquens, si sit $5c = 13k + 1$, erit quoque c^4 minima potestas unitatem relinquens. Verum ut fiat $13k + 1$ per 5 divisibile, sumi debet $k = 5\lambda - 2$, eritque $c = 13\lambda - 5$, cujus minimus valor est $c = 8$, ita ut etiam 8^4 sit minima potestas per 13 divisa unitatem relinquens.

242. Quicunque autem fuerit numerus b minor quam d ad eumque primus, semper quoque dabitur numerus c, etiam minor quam d ad eumque primus, ut sit $bc = kd + 1$, neque plures. Si enim duo dentur, ut esset tam $bc = kd + 1$, quam $be = ld + 1$, foret $bc - be = b(c - e)$ per d divisibile, unde ob b et d primos, esset $c - e$ per d divisibile, quod cum c et e sint minores quam d, fieri nequit, nisi sit $e = c$. Hoc autem evenire potest, ut fiat $c = b$, quod semper contingit, si sit vel $b = 1$, vel $b = d - 1$.

Caput VIII.

De potestatibus numerorum, quae per numeros primos divisae, unitatem relinquunt.

243. Quodcunque residuum potestas a^n per numerum d divisa relinquit, idem etiam relinquent omnes potestates ejusdem exponentis $(a + \lambda d)^n$, atque si n fuerit numerus par, idem residuum relinquet etiam potestas $(\lambda d - a)^n$, unde judicium residuorum ad numeros a divisore d minores revocatur.

244. Sit jam divisor d numerus primus quicunque, et quia binarius nullam habet difficultatem, ponatur $d = 2p + 1$, eritque $2p$ multitudo numerorum ipso d minorum ad eumque primorum. Jam si a sit numerus quicunque ad d primus, quod fit dummodo a non sit d ejusve multiplum, vidimus ejus potestatem a^{2p} per $d = 2p + 1$ divisam semper unitatem relinquere.

245. Saepe autem evenire potest, ut etiam potestas inferior a^n, existente $n < 2p$, per eundem numerum $d = 2p + 1$ divisa unitatem relinquat; tum autem exponens n certo est pars aliquota ipsius $2p$. Quod ergo si evenit, non solum formula $a^{2p} - 1$, sed etiam formula $a^n - 1$ per numerum primum $2p + 1$ erit divisibilis.

246. Quod si ergo formula $a^n - 1$ fuerit divisibilis per numerum primum $2p + 1$, erit etiam formula $a^{mn} - 1$ divisibilis, unde cum formula $a^{2p} - 1$ certo sit etiam per $2p + 1$ divisibilis, erit etiam differentia $a^{mn} - a^{2p}$, seu $a^{2p}(a^{mn-2p} - 1)$ divisibilis; quare cum factor a^{2p} divisionen non admittat, alter $a^{mn-2p} - 1$ divisibilis sit necesse est, quicunque numerus pro m sumatur.

247. Sit λ maximus communis divisor numerorum n et $2p$; ac si formula $a^n - 1$ fuerit divisibilis per numerum primum $2p + 1$, etiam haec formula $a^\lambda - 1$ per $2p + 1$ erit divisibilis. Sit enim $n = \alpha\lambda$ et $2p = \beta\lambda$, ut α et β sint numeri primi inter se, et quoniam tam $a^{\alpha\lambda} - 1$ quam $a^{\beta\lambda} - 1$ sunt multipla ipsius $2p + 1$, etiam hae formulae $a^{\mu\alpha\lambda} - 1$ et $a^{\nu\beta\lambda} - 1$ erunt multipla. At ob α et β numeros primos, μ et ν ita accipi possunt, ut fiat $\mu\alpha = \nu\beta + 1$, unde differentia erit