163. Erit enim $A = md + \alpha$ et $B = nd + \beta$, unde fit productum

$$AB = mnd^2 + (m\beta + n\alpha)\, d + \alpha\beta,$$

cujus partes priores cum sint per d divisibiles, postrema $\alpha\beta$ pro residuo haberi potest.

164. Hinc colligimus, si numerus A per d divisus relinquat residuum α, ejus quadrato A^2 respondere residuum $\alpha\alpha$, ejusque cubo A^3 residuum α^3, et potestati cuicunque A^n residuum α^n, quod, divisione per d facta, porro ad minimam formam reducetur.

165. Quare si numero A per d diviso relinquatur residuum $= 1$, omnes ejus potestates A^2, A^3, A^4, etc. per eundem divisorem d divisi idem residuum relinquent $= 1$. At si residuum numeri A sit -1, aequipollens ipsi $d - 1$, potestatum parium A^2, A^4, A^6, A^8, etc. residua erunt $+1$, imparium vero -1.

166. Denique notandum est, si numerus A per d divisus praebeat residuum α, tum fore $A - \alpha$ per numerum d divisibile. Unde cum A^n pro divisore d det residuum α^n, erit quoque $A^n - \alpha^n$ per d divisibile.

Caput VI.

De residuis ex divisione terminorum progressionis arithmeticae ortis.

167. Incipiamus a serie numerorum naturalium, cujus termini 1, 2, 3, 4, etc. per divisorem quemcunque d divisi, dabunt residua 1, 2, 3, 4, etc. donec perveniatur ad terminum d, cui residuum convenit $= 0$, sequentes vero termini $d + 1$, $d + 2$, $d + 3$, etc. eodem ordine residua 1, 2, 3, etc. reddent, usque ad $2d$, cujus residuum iterum evanescit, et ita porro.

168. Sit jam proposita progressio arithmetica quaecunque

$$a,\ a + b,\ a + 2b,\ a + 3b,\ a + 4b,\ a + 5b,\ \text{etc.}$$

cujus singuli termini per divisorem d dividantur, et ex primo oritur residuum a, quod idem ante non recurret, quam perveniatur ad terminum $a + nb$, cujus pars nb per d divisibilis existat, et post hunc terminum residua eodem ordine prodibunt atque ab initio (*).

169. Primo quidem statim liquet, hinc plura diversa residua resultare non posse, quam divisor d contineat unitates. Unde, si ab initio jam tot diversa residua prodierint, necesse est, ut deinceps priores iterum redeant. Semper autem terminus $a + db$, cujus index est $d + 1$, idem praebet residuum ac primus a.

170. Si differentia progressionis b fuerit factor divisoris d, vel si saltem b et d communem habeant factorem φ, ut sit $b = B\varphi$ et $d = D\varphi$, tum antequam ad terminum $a + db$ perveniatur, primum residuum a revertetur, scilicet hoc continget in termino $a + Db$, cujus index est $D + 1$, quoniam $Db = BD\varphi = Bd$ per d est divisibile.

171. Hic ergo duos casus evolvi conveniet, alterum, quo divisor d et differentia progressionis b sunt numeri inter se primi, alterum vero, quo sunt numeri inter se compositi, seu quo habent quempiam factorem communem, praeter unitatem.

(*) *Script. ad marg.* Haec residua excedent numero a residua orta ex progressione $0, b, 2b, 3b, 4b,$ etc. quare hanc evolvisse sufficiet.

172. Si divisor d et differentia progressionis b fuerint numeri primi inter se, primum residuum a ante non recurrit, quam in termino $a + db$; si enim ex termino quodam antecedente resultaret, puta $a + (d - n)\,b$, esset $(d - n)\,b$, ac proinde etiam nb per d divisibile, ideoque etiam n, quod foret absurdum.

173. Ad definienda ergo residua considerari oportet terminos progressionis, a primo a usque ad $a + (d - 1)\,b$, quorum multitudo est d, quos terminos ordine dispositos cum suis residuis ita repraesentemus:

Indices:	1,	2,	3,	4,	5,	d
Progressio:	a,	$a + b$,	$a + 2b$,	$a + 3b$,	$a + 4b$, ...	$a + (d - 1)\,b$
Residua:	α,	β,	γ,	δ,	ε,	λ

174. Primum ergo observo cuncta haec residua, quorum multitudo est $= d$, inter se esse diversa. Quemadmodum enim primum α non amplius occurrere ostensum est, ita etiam secundum β semel tantum adesse docetur. Si enim ex termino $a + nb$, existente $n < d$, idem oriretur residuum, foret differentia terminorum $(n - 1)\,b$ per d divisibilis, ideoque et $n - 1$, quod repugnat.

175. Cum igitur omnia residua α, β, γ, δ, ... λ sint inter se diversa, eorumque multitudo sit $= d$, inter ea omnes numeri ipso d minores una cum cyphra occurrent, numeri scilicet $0, 1, 2, 3, \ldots (d - 1)$ occurrent, quorum multitudo pariter est $= d$.

176. Quare si r fuerit numerus quicunque minor quam divisor d, dabitur certe progressionis terminus $a + nb$, existente $n < d$, qui per d divisus relinquat residuum r. Ac sumto $r = 0$, dabitur ejusmodi terminus $a + nb$ per d divisibilis.

177. Si terminus $a + nb$ residuum praebeat r, erit $a + nb - r$ per d divisibile. Unde si b et d sint numeri inter se primi, et $a - r$ denotet numerum quemcunque, semper dabitur numerus n minor quam d, ita ut numerus $a - r + nb$ fiat per d divisibilis.

178. Sit $a + mb$ terminus per d divisibilis, existente $m < d$, ac terminus sequens $a + (m + 1)\,b$ residuum dabit b, praecedens vero $a + (m - 1)\,b$ residuum $- b$, seu $d - b$. Sit porro $a + nb$ terminus, qui per d divisus unitatem relinquat, atque illo numero hinc ablato differentia $(n - m)\,b$ etiam unitatem relinquet.

179. Ponamus $n - m = p$, ut numerus pb per d divisus unitatem relinquat, sumtoque termino $a + mb$ per d divisibili, termino $a + (m + p)\,b$ conveniet residuum $= 1$, termino $a + (m + 2p)\,b$ residuum $= 2$, termino $a + (m + 3p)\,b$ residuum $= 3$, et in genere termino $a + (m + np)\,b$ residuum $= n$.

180. Si $m + np$ fuerit majus divisore d, hic toties inde auferatur, donec remaneat numerus $k < d$, et terminus $a + kb$ per d divisus relinquet residuum $= n$.

181. Facilius autem termini data residua relinquentes definiri possunt, dum innotuerit productum pb, quod per d divisum relinquat unitatem. Cum enim terminus primus a relinquat α, terminus $a + npb$ relinquet $\alpha + n$.

182. Si ergo datum residuum fuerit $= r$, ponatur $\alpha + n = r$, et ob $n = r - \alpha$, invento p, terminus residuum r praebens erit $a + (r - \alpha)\,pb$; vel etiam generaliter $a + ((r - \alpha)\,p \pm \mu d)\,b$, ubi μ ita assumere licet, ut fiat $(r - \alpha)\,p \pm \mu d < d$.

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 $\beta, \gamma, \delta, \varepsilon \ldots \lambda$ 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.