133. Si igitur M et N fuerint numeri inter se primi, atque multitudo numerorum ab 1 ad M, primorum ad M, sit $=m$, multitudo vero numerorum ab 1 ad N, primorum ad N, sit $=n$, tum multitudo numerorum ad productum MN primorum ipsoque non majorum, erit $=mn$.

134. Hinc patet multitudinem omnium numerorum primorum, quemadmodum jam Euclides demonstravit, finitam esse non posse. Si enim ultimus et maximus numerus primus esset $=p$, statuatur numerus M aequalis producto omnium numerorum primorum $M=2.3.5.7\ldots p$, qui ergo ad omnes plane numeros esset compositus: cum igitur idem numerus M ad $M-1$, vel $M+1$ certe sit primus, patet assertionem esse absurdam.

135. Ex superioribus autem patet, inter numeros ipso M minores non solum numerum $M-1$, sed etiam plures alios ad M certe esse primos, cum multitudo horum numerorum ad M primorum sit $=1.2.4.6\ldots(p-1)$, quae eo est major, quo plures numeri primi in se invicem multiplicentur.

136. Ponamus $m=1.2.4.6\ldots(p-1)$, existente $M=2.3.5.7\ldots p$; et cum ab 1 ad M tot sint numeri ad M primi, quot m continet unitates, hi vel ipsi erunt primi, vel compositi ex primis, qui sint ipso p majores.

137. Si ab 1 ad M fuerint m numeri ad M primi, ab 1 ad $2M$ erunt $2m$ numeri ad M primi, et in genere ab 1 ad NM erunt Nm numeri ad M primi. In quovis enim intervallo

$$1\ldots M,\quad M+1\ldots 2M,\quad 2M+1\ldots 3M,\quad 3M+1\ldots 4M,\text{ etc.}$$

multitudo numerorum ad M primorum est eadem.

138. Si N designet alium numerum quemcunque, atque ab 1 ad N fuerint n numeri ad N primi, ab 1 ad MN erunt Mn numeri ad N primi. At in eodem intervallo sunt Nm numeri ad M primi. Qui autem sunt primi ad MN, ii quoque sunt primi tam ad M quam ad N.

139. Ante autem ostendimus, si hi numeri M et N fuerint primi inter se, tum in intervallo $1\ldots.MN$ tot dari numeros ad MN primos, quot mn contineat unitates; hique numeri in utraque praecedente multitudine Mn et Nm occurrunt. (*)

Caput V.

De residuis ex divisione natis.

140. Si numerus a non sit multiplum numeri b, divisio illius per hunc non succedit, et excessus numeri a supra multiplum ipsius b proxime minus vocatur *residuum* ex divisione ortum. Ita si sit $a=mb+r$, erit r residuum ex divisione numeri a per b natum.

(*) *Notae Ill. Auctoris margini adscriptae.* De maximo communi divisore ejusque inventione. — Si A et B sint numeri primi, inveniri potest multiplum ipsius A, quod per B divisum relinquat datum numerum C. — Qui numeri inter se fuerint primi, eorum potestates quaecunque inter se erunt primi. — Si A sit primus ad B, atque etiam ad C, erit quoque ad BC primus. — Si productum AB sit divisibile per primum p, alteruter factor per eum erit divisibilis. — Si A et B sint primi inter se, inveniri possunt numeri m et n, ut fiat $mA-nB=1$, vel alii cuivis numero dato. — Si sit φ maximus communis factor numerorum A et B, tum $\frac{A}{\varphi}$ et $\frac{B}{\varphi}$ erunt primi inter se. — Si a per b divisum det residuum r, tum na per nb divisum dabit residuum nr. — Si a per b divisum det residuum r, communis factor numerorum a et b, si quem habent praeter unitatem, simul erit factor residui r. Vicissim, si b et r habeant communem factorem, idem quoque factor erit ipsius a. — Si a et b sint numeri inter se primi et $a>b$, erit $a=mb+p$; et $b>p$, tum vero $b=np+q$ et $p>q$, sicque tandem ad unitatem pervenietur.

141. Hinc patet residuum r semper minus esse numero b seu divisore; si enim esset aequale, seu $r = b$, aucto indice multipli m unitate, foret a verum multiplum ipsius b, scilicet $a = (m+1)b$; et si esset $r > b$, augendo indicem m reduceretur infra b.

142. Proposito ergo divisore quocunque b, si dividendus a fuerit multiplum ipsius b, residuum erit $= 0$; sin autem a non fuerit multiplum ipsius b, residuum erit vel 1, vel 2, vel 3, vel quicunque alius numerus minor quam b, ita ut multitudo residuorum, quae oriri possunt, sit $b - 1$, vel adeo b, si cyphra simul numeretur.

143. Pro quovis ergo divisore b omnes numeri in tot classes distribui possunt, quot b continet unitates. Prima nempe classis continebit omnes numeros multiplos ipsius b, seu formae mb; secunda eos, qui per b divisi pro residuo relinquunt 1, tertia eos, qui 2, quarta eos, qui 3, et denique ultima, qui relinquunt $b - 1$.

144. Ita sumto 2 pro divisore, duae habentur classes, quarum prima continet numeros formae $2m$, altera vero numeros formae $2m+1$. Numeri prioris classis vocantur *pares*, posterioris vero *impares*.

145. Si ternarius pro divisore assumatur, omnes numeri in tres classes distinguentur: prima complectitur numeros formae $3m$, secunda numeros formae $3m+1$, ac tertia numeros formae $3m+2$.

146. Si divisor statuatur $= 4$, quaternae classes omnium numerorum his quatuor formis comprehenduntur: I. $4m$, II. $4m+1$, III. $4m+2$, IV. $4m+3$, ubi prima classis nomen sortita est numerorum *pariter parium*; tertia vero numerorum *impariter parium*. At secunda et quarta numeros impares in duas classes subdivisos exhibent.

147. Simili modo divisor 5 has quinque numerorum classes suppeditat: I. $5m$, II. $5m+1$, III. $5m+2$, IV. $5m+3$, V. $5m+4$: ac divisor 6 praebet has sex classes:

I. $6m$, II. $6m+1$, III. $6m+2$, IV. $6m+3$, V. $6m+4$, VI. $6m+5$,

et ita porro pro quovis alio divisore.

148. Sic igitur quilibet numerus pro quovis divisore ad certam quandam classem refertur, seu certa quadam forma exprimitur, quod, cum divisorum numerus in infinitum augeri queat, infinitis modis fieri potest.

149. Si enim numerus fuerit minor divisore proposito, ipse ut residuum spectari potest, indice multipli evanescente: ita si sit $a < b$, erit $a = mb + a$ existente $m = 0$, numerus ergo 3 respectu divisoris 5 pertinet ad classem $5m+3$.

150. Quaelibet classis infinitos continet numeros in arithmetica progressione crescentes, secundum differentiam divisori aequalem. Ita in genere si divisor sit b et residuum r, omnes numeri ad classem $mb+r$ relati sunt: r, $b+r$, $2b+r$, $3b+r$, $4b+r$, $5b+r$, etc. cujus progressionis arithmeticae terminus generalis est ipsa formula $mb+r$, unde est nata.

151. Formula $mb+r$ etiam hoc modo $(m+1)b - b + r$ potest repraesentari, sicque residuo positivo r aequivalens censendum est residuum negativum $-(b-r)$, unde patet ideam residuorum latius extensam etiam numeros negativos complecti.

152. Hinc divisore b existente $=2$, formula numerorum imparium $2m+1$ etiam ita $2m-1$ repraesentari potest; atque si divisor b sit $=3$, classis numerorum, qui per 3 divisi relinquunt binarium, etiam formula $3m-1$ continetur; sicque omnes numeros in una harum trium formularum $3m$, $3m+1$ et $3m-1$ contineri necesse est.

153. Quare si residua negativa admittere velimus, omnes formulas $mb \pm r$ ita repraesentare poterimus, ut residuum r semissem divisoris b non superet. Si enim esset $r > \frac{1}{2}b$, pro r sumamus $-(b-r)$ eritque $b-r < \frac{1}{2}b$.

154. Simili modo cum sit $mb+r=(m-1)b+b+r$, residuo r etiam aequivalet residuum $b+r$, vocabulo in latiori sensu accepto. Generatim ergo residua minus proprie ita dicta $b+r$, $2b+r$, $3b+r$, etc. aequivalent residuo r proprie sic dicto.

155. Scilicet divisore existente b, omnis numerus, etiamsi sit major quam b, tanquam residuum spectari potest, qui ad residuum proprie ita dictum reducetur, divisorem b inde toties auferendo, quoties fieri licet, quod adeo negativa admittendo infra semissem ipsius b deprimi poterit.

156. Ita si divisor sit 6 et residuum 16, hoc residuum improprium reducetur ad proprium 4, atque adeo ad negativum -2, sive istae formulae $6m+16$, $6m+4$, $6m-2$ pro aequivalentibus sunt habendae, quia omnes numeri in una contenti simul in reliquis continentur.

157. Circa residua plures insignes proprietates perpendi oportet. Si numerus A per divisorem d divisus, praebeat residuum α, numeri quoque $A+d$, $A+2d$, $A+3d$, etc. idem relinquent residuum α, at numerus $A+1$ per eundem divisus dabit residuum $\alpha+1$, et generaliter numerus $A+n$ residuum dabit $\alpha+n$, quod si excedat divisorem d, eo subtrahendo quoties fieri potest, ad minimam formam reducetur.

158. Simili modo, si sumto divisore d, numero A residuum conveniat α, numeri quoque $A-d$, $A-2d$, $A-3d$, etc. idem relinquent residuum, at numero $A-1$ residuum conveniet $\alpha-1$, et numero $A-n$ residuum $\alpha-n$, quod si forte sit negativum, additione divisoris d ad positivum reducetur.

159. Sumto divisore d, si numero A conveniat residuum α, numero vero B residuum β, aggregato horum numerorum $A+B$ conveniet residuum $\alpha+\beta$, quod congruit cum $\alpha+\beta-d$, si forte sit $\alpha+\beta > d$. Hinc patet si sit $\alpha+\beta=d$, fore $A+B$ multiplum ipsius d.

160. Iisdem positis, differentiae numerorum $A-B$ conveniet residuum $\alpha-\beta$, vel etiam $\alpha-\beta+d$, si forte sit $\beta > \alpha$. Unde si sit $\alpha=\beta$, seu si numeri A et B paria relinquant residua, eorum differentia erit per divisorem d divisibilis.

161. Sumto divisore d, si numerus A praebeat residuum α, ejus duplum $2A$ dabit residuum 2α, vel etiam $2\alpha-d$, triplum vero $3A$ dabit residuum 3α, cujus, si sit majus quam d, minima forma erit vel $3\alpha-d$, vel $3\alpha-2d$. Atque in genere multipli cujusvis nA residuum erit $n\alpha$, sive $n\alpha-md$.

162. Si divisore posito $=d$, numero A respondeat residuum α, numero vero B residuum β, producto AB residuum conveniet $\alpha\beta$, quod si forte majus fuerit quam divisor d, reducitur ad $\alpha\beta-d$, vel $\alpha\beta-md$.

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.