summas divisorum $\int A, \int B, \int C, \int D$ unica debet esse impariter par, reliquae omnes impares: omnes ergo factores A, B, C, D, praeter unum, erunt potestates pares numerorum primorum, unus autem ille vel numerus primus formae $4n+1$, vel ejusdem potestas, cujus exponens sit $4\lambda+1$. Sicque talis numerus perfectus hujusmodi habebit formam $(4n+1)^{4\lambda+1} PP$, existente P numero impari, et $4n+1$ primo.

110. Plurima alia problemata huc referenda, quibus alia proponitur relatio inter numeros investigandos eorumque summas divisorum hic praetermitto, quoniam ex traditis principiis methodus ea solvendi non difficulter elicitur.

Caput IV.

De numeris inter se primis et compositis.

111. Duo numeri, qui praeter unitatem nullum alium habent factorem seu divisorem communem, vocantur numeri *primi inter se*; qui autem praeter unitatem alium habent divisorem communem, vocantur *compositi inter se*. Ita 8 et 15 sunt numeri inter se primi, at 9 et 15 numeri inter se compositi.

112. Unitas ergo est ad omnes numeros primus. Scilicet denotante n numerum quemcunque, numeri 1 et n sunt numeri primi inter se, quia praeter unitatem nullum alium admittunt divisorem communem.

113. Pari modo duo numeri unitate differentes n et $n+1$ sunt primi inter se; quoscunque enim divisores habuerit numerus n, nullus eorum dividere potest numerum $n+1$. Namque si p sit divisor numeri n, numerus proxime major per p divisibilis erit $n+p$, neque vero $n+1$ divisionem per p admittet.

114. Numerus primus p ad omnes numeros, nisi qui ejus sunt multipla, est primus; hinc numeri a et p sunt primi inter se, nisi sit vel $a=p$, vel $a=np$. Ergo numerus primus p ad omnes numeros se minores est primus.

115. Multitudo numerorum, dato numero a minorum, est $a-1$, inter quos quot sint ad a vel primi, vel compositi, operae pretium est definire; quoniam inde judicium ad omnes numeros ipso a majores facile extenditur.

116. Sit enim $b<a$, ac si b et a fuerint primi inter se, etiam omnes hi numeri $b+a$, $b+2a$, $b+3a$, etc. ad a erunt primi; ac si b et a habuerint communem divisorem, idem erit divisor numerorum $b+a$, $b+2a$, etc.

117. Si ergo a sit numerus primus $=p$, quia omnes numeri ipso minores ad eum sunt primi, horum multitudo est $=p-1$.

118. Si sit $a=2p$, ab 1 ad a dantur p numeri pares, qui ergo ad a non sunt primi, deinde ipse numerus p ad a etiam non est primus. Auferantur hi a numeris omnibus ab 1 usque ad a, quorum multitudo est $=p$, ac relinquentur $p-1$, totidemque ad a erunt primi.

119. Si sit $a=3p$, inter numeros ipso non majores primum ii, qui sunt per 3 divisibiles, ad eum non sunt primi, quorum multitudo est $=p$, deinde insuper p et $2p$ ad a non sunt primi; reliqui, quorum multitudo est $3p-p-2=2(p-1)$, omnes ad $a=3p$ erunt primi.

120. Simili modo si $a = 5p$, numeri, qui cum a communem habent divisorem, sunt primo omnes per 5 divisibiles, quorum multitudo est $= p$, ac praeterea qui per p sunt divisibiles, nempe $p, 2p, 3p$ et $4p$; ipse enim numerus $5p$ jam ante est notatus: unde multitudo numerorum ad a compositorum est $p + 4$, ideoque multitudo numerorum ad a primorum $= 4p - 4 = 4(p - 1)$, qui scilicet ipso a non sunt majores.

121. Generalius si sit $a = pq$, existente utroque factore p et q primo, ab unitate ad a dantur p numeri per q divisibiles, scilicet $q, 2q, 3q \ldots pq$; deinde dantur q numeri per p divisibiles, scilicet $p, 2p, 3p, \ldots qp$, quorum ultimus qp jam est numeratus. Multitudo ergo omnium numerorum a non superantium, qui ad a sunt compositi, erit $= p + q - 1$, unde reliqui, quorum multitudo est

$$= qp - p - q + 1 = (p - 1)(q - 1),$$

ad a erunt primi.

122. Hic autem pro p et q numeros primos diversos sumsimus. Nam si esset $a = pp$, alii numeri ad a non essent compositi, nisi qui sunt per p divisibiles, quorum multitudo cum sit $= p$, reliquorum, qui ad a sunt primi, multitudo erit $= pp - p = p(p - 1)$.

123. Simili modo si sit $a = p^3$, quia alium divisorem primum praeter p non habet, omnes numeri ab 1 ad a, ad a compositi sunt $p, 2p, 3p \ldots p^2p$, quorum multitudo cum sit p^2, reliqui numeri omnes, quorum multitudo est $p^3 - p^2 = p^2(p - 1)$, ad a erunt primi.

124. Hinc in genere patet, si a fuerit potestas quaecunque p^n numeri primi p, multitudinem numerorum ad a primorum, qui quidem ipso a non sint majores, fore $= p^{n-1}(p - 1)$.

125. Sit $a = p^2q$, existentibus p et q numeris primis diversis, et cum a alios non habeat divisores primos praeter p et q, numeri ad a compositi vel erunt per p divisibiles, qui sunt $p, 2p, 3p \ldots pq.p$, multitudine $= pq$, vel per q divisibiles, qui sunt $q, 2q, 3q, \ldots p^2.q$ multitudine $= p^2$. Inter hos vero occurunt, qui ibi jam sunt numerati $pq, 2pq, 3pq \ldots p.pq$ multitudine $= p$, ita ut multitudo omnium ad a compositorum sit $= pq + p^2 - p$. Quare reliqui, quorum multitudo est $= ppq - pq - pp + p = p(p - 1)(q - 1)$, omnes ad a erunt primi.

126. Sit $a = pqr$, existentibus p, q, r numeris primis diversis, ac numeri ad a compositi sunt divisibiles

1) per p, scilicet $p, 2p, 3p \ldots qr.p$ multitudine qr
2) per q, « $q, 2q, 3q \ldots pr.q$ « pr
3) per r, « $r, 2r, 3r \ldots pq.r$ « pq.

Hic autem bis numerantur divisibiles per pq multitudine r, tum divisibiles per pr multitudine q, ac denique divisibiles per qr multitudine p, qui inde auferantur; at hoc modo numerus ipse pqr penitus tolleretur, qui ergo iterum est adjiciendus. Sicque multitudo numerorum ad a compositorum erit $qr + pr + pq - r - q - p + 1$; unde reliqui, quorum multitudo est

$$pqr - qr - pr - pq + r + q + p - 1 = (p - 1)(q - 1)(r - 1),$$

ad numerum $a = pqr$ erunt primi.

127. Ex his colligetur pro omnibus numerorum generibus fore

si sit numerus propositus	multitudinem numerorum ipso a minorum ad eumque primorum
$a = p$	$p - 1$
$a = p^2$	$p(p-1)$
$a = pq$	$(p-1)(q-1)$
$a = p^3$	$p^2(p-1)$
$a = p^2q$	$p(p-1)(q-1)$
$a = pqr$	$(p-1)(q-1)(r-1)$
$a = p^4$	$p^3(p-1)$
$a = p^3q$	$p^2(p-1)(q-1)$
$a = p^2q^2$	$p(p-1)q(q-1)$
$a = p^2qr$	$p(p-1)(q-1)(r-1)$
$a = pqrs$	$(p-1)(q-1)(r-1)(s-1)$

128. Quo autem haec conclusio firmius corroboretur neque inductioni nimium indulgeatur, consideremus hanc formam $a = Mp$, ubi M sit numerus quicunque, et p primus in M non contentus. Ponamus autem ad 1 ab M multitudinem numerorum ad M primorum esse $= \mu$, ideoque multitudinem numerorum ad M compositorum $= M - \mu$.

129. Cum ergo ab 1 ad M sint $M - \mu$ numeri compositi ad M, ab 1 ad Mp erunt $p(M-\mu)$ numeri compositi ad M, qui ergo etiam erunt compositi ad Mp, sed praeterea ad Mp compositi sunt isti: p, $2p$, $3p \ldots Mp$, multitudine M, unde autem expungendi sunt ii, qui jam ad M sunt compositi, quorum multitudo est $M - \mu$; sicque tantum relinquentur μ numeri, qui tantum ad Mp, non vero ad M sunt compositi. Quare ab 1 ad Mp omnino ad Mp compositi erunt tot: $p(M-\mu) + \mu$, et reliqui, quorum multitudo est $Mp - p(M-\mu) - \mu = \mu(p-1)$, ad numerum Mp erunt primi.

130. Simili modo ostenditur, si numerus propositus sit $= Mp^n$, existente p numero primo in M non contento, atque μ fuerit multitudo numerorum ad M primorum, qui quidem inter limites 1 et M contineantur, tum multitudinem omnium numerorum infra Mp^n, ad hunc ipsum numerum Mp^n primorum, fore $= p^{n-1}\mu(p-1)$.

131. Quaeramus enim numeros compositos ad Mp^n, qui vel ad M, vel ad p erunt compositi. At ab 1 ad Mp^n multitudo numerorum ad M compositorum est $= p^n(M-\mu)$, qui vero ad p sunt compositi erunt: p, $2p$, $3p \ldots Mp^{n-1}.p$, multitudine $= Mp^{n-1}$. Hinc autem excludi oportet eos, qui jam ad M sunt compositi, quorum multitudo est $p^{n-1}(M-\mu)$: sicque multitudo eorum, qui ad Mp^n, non vero ad M sunt compositi, erit $= Mp^{n-1} - p^{n-1}(M-\mu) = p^{n-1}\mu$, unde omnino ab 1 ad Mp^n multitudo numerorum ad Mp^n compositorum est $= p^n(M-\mu) + p^{n-1}\mu$. Quocirca reliqui, quorum multitudo est $Mp^n - p^n(M-\mu) - p^{n-1}\mu = p^{n-1}\mu(p-1)$ erunt ad Mp^n primi.

132. Cum ergo multitudo numerorum ad p^n primorum ipsoque minorum sit $= p^{n-1}(p-1)$, ex praecedente propositione summo rigore concludimus: Si numerus propositus sit $= p^\lambda q^\mu r^\nu s^\xi$ etc. fore multitudinem omnium numerorum ad eum primorum ipsoque minorum

$$= p^{\lambda-1}(p-1).q^{\mu-1}(q-1).r^{\nu-1}(r-1).s^{\xi-1}(s-1) \text{ etc.}$$

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 $M = 2.3.5.7...p$, 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 $= 1.2.4.6...(p - 1)$, quae eo est major, quo plures numeri primi in se invicem multiplicentur.

136. Ponamus $m = 1.2.4.6...(p - 1)$, existente $M = 2.3.5.7...p$; 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

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

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 $1....MN$ 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.