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

$a^{\nu\beta\lambda+\lambda} - a^{\nu\beta\lambda} = a^{\nu\beta\lambda}(a^\lambda - 1)$, quae cum sit divisibilis per $2p+1$, necesse est sit $a^\lambda - 1$ per $2p+1$ divisibile.

248. Si ergo n sit numerus ad $2p$ primus, forma $a^n - 1$ divisibilis esse nequit per numerum primum $2p+1$, nisi sit $a-1$ per eundem divisibile. Unde si $a-1$ non sit multiplum numeri primi $2p+1$, formula $a^n - 1$ per eum divisibilis esse nequit, nisi n et $2p$ sint numeri inter se compositi, quorum si maximus communis divisor sit λ, adeo haec formula $a^\lambda - 1$ per $2p+1$ erit divisibilis.

249. Si igitur a^n fuerit minima potestas ipsius a, quae per numerum primum $2p+1$ divisa unitatem relinquit, tum certe est n pars aliquota numeri $2p$. Tum autem si fuerit $ab = k(2p+1)+1$, erit etiam b^n minima potestas ipsius b, quae per $2p+1$ divisa unitatem relinquit.

250. Si n sit numerus primus et formula $a^n - 1$ divisibilis per numerum primum $2p+1$, vel erit n pars aliquota ipsius $2p$ (quia alius communis divisor locum non habet), vel si fuerit ad $2p$ primus, numerus $a-1$ per $2p+1$ erit divisibilis. Quare praeter divisores ipsius $a-1$ formula $a^n - 1$ alios divisores primos non admittit, nisi hujusmodi formae $2p+1$, ut $2p$ sit multiplum ipsius n. Unde omnes ejus divisores primi in hac forma $2mn+1$ continebuntur.

251. Quare haec forma $a^3 - 1$ praeter divisorem $a-1$ alios divisores primos non admittit nisi formae $6m+1$, qui sunt 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 etc. Cum ergo $aa+a+1$ sit factor ipsius $a^3 - 1$, etiam is per nullos alios numeros primos est divisibilis.

252. Simili modo forma $a^5 - 1$ praeter divisorem $a-1$ alios non habet, nisi qui in forma $10m+1$ contineantur, quales sunt 11, 31, 41, 61, 71 etc. Quare etiam tales numeri

$$a^4 + a^3 + a^2 + a + 1,$$

nisi sint primi, alios divisores non admittunt.

253. Quoniam numeri perfecti inveniuntur, quoties formula $2^n - 1$ est numerus primus, primum patet hoc evenire non posse, nisi n sit numerus primus. At si n fuerit talis, formula $2^n - 1$ certe alios non habet divisores nisi formae $2mn+1$, unde exploratio utrum sit primus, nec ne? faciliori negotio absolvitur.

254. Cum $a^{2p} - 1$ semper sit divisibile per numerum primum $2p+1$, illa autem forma constet factoribus $a^p - 1$ et $a^p + 1$, necesse est ut alteruter per $2p+1$ sit divisibilis. Vidimus autem, si sit $a = ee \pm \lambda(2p+1)$, fore $a^p - 1$ divisibilem; his ergo casibus formula $a^p + 1$ per $2p+1$ certe non est divisibilis.

255. Hic quaestio oritur, num forte semper formula $a^p - 1$ per $2p+1$ sit divisibilis? ideoque nunquam altera $a^p + 1$, quod casu, quo p est numerus impar, statim negandum esse patet. Quia enim tum $a^p + 1$ factorem habet $a+1$, ista formula sumto $a = 2p$ manifesto per $2p+1$ fit divisibilis.

256. In genere autem sequenti modo ostendi potest formulam $a^n - 1$, existente $n < 2p$, non semper divisibilem esse per numerum primum $2p+1$, sed dari utique ejusmodi numeros pro a adhibendos, quibus divisio formulae $a^n - 1$ non succedat, quod per deductionem ad absurdum sic commodissime demonstrabitur.

257. Qui enim hoc negaverit, affirmare debet omnes has formulas $1^n - 1$, $2^n - 1$, $3^n - 1$, $4^n - 1$, $5^n - 1$, $\ldots . n^n - 1$ per $2p+1$ esse divisibiles, ideoque etiam earum differentias tam primas $2^n - 1$, $3^n - 2^n$, $4^n - 3^n$, $5^n - 4^n$, etc. quam secundas $3^n - 2.2^n + 1^n$, $4^n - 2.3^n + 2^n$, $5^n - 2.4^n + 3^n$, etc. et sequentes omnes.

258. Differentiae autem ordine n sunt constantes, quae si littera N indicentur, ita exprimuntur ut sit $N = (n+1)^n - n.n^n + \frac{n(n-1)}{1.2}(n-1)^n - \frac{n(n-1)(n-2)}{1.2.3}(n-2)^n +$ etc. cujus expressionis valores pro variis valoribus ipsius n facile colliguntur:

Si $n = 1$ est $N = 2 - 1 = 1$
$n = 2$ $N = 3^2 - 2.2^2 + 1 = 2 = 1.2$
$n = 3$ $N = 4^3 - 3.3^3 + 3.2^3 - 1 = 6 = 1.2.3$
$n = 4$ $N = 5^4 - 4.4^4 + 6.3^4 - 4.2^4 + 1 = 24 = 1.2.3.4$
etc.

259. Ad quod clarius ostendendum sit, pro n scribendo $n+1$,
$P = (n+2)^{n+1} - (n+1)(n+1)^{n+1} + \frac{(n+1)n}{1.2}n^{n+1} - \frac{(n+1)n(n-1)}{1.2.3}(n-1)^{n+1} +$ etc.
et a termino anteriori incipiendo

$$P = (n+1)^{n+1} - (n+1)\,n^{n+1} + \frac{(n+1)n}{1.2}(n-1)^{n+1} - \text{etc.}$$

At valor ipsius N ita repraesentari potest

$$N = (n+1)^n - n^{n+1} + \frac{n}{1.2}(n-1)^{n+1} - \frac{n(n-1)}{1.2.3}(n-2)^{n+1} + \text{etc.}$$

quae per $n+1$ multiplicata praebet valorem ipsius P, ita ut sit $P = (n+1)\,N$.

260. Cum igitur casu $n=1$ sit $N=1$, casu $n=2$ erit $N=1.2$, casu $n=3$ erit $N=1.2.3$, et in genere pro numero quocunque n erit $N = 1.2.3\ldots n$. At haec differentia ordinis n non est divisibilis per numerum primum $2p+1$, ob $n < 2p$, unde sequitur non omnes terminos seriei § 257 expositae per eum esse divisibiles.

261. Sit $6p+1$ numerus primus, et cum forma $a^{6p} - 1$ per eum sit divisibilis, nisi a ejus sit multiplum, dabuntur casus, quibus etiam $a^{3p} - 1$ per eum dividi poterit, scilicet sumto $a = c^3 \pm \lambda\,(6p+1)$. Tum vero etiam dantur casus, quibus formula $a^{2p} - 1$ non erit divisibilis per istum numerum primum $6p+1$, uti ex demonstratione modo allata patet.

262. Cum ante ostenderimus formulam $a^{3p} - 1$ fore per $6p+1$ divisibilem, si fuerit

$$a = cc \pm \lambda\,(6p+1),$$

nunc colligere licet, si numerus a simul in hac forma $cc \pm \lambda\,(6p+1)$ et in hac $c^3 \pm \lambda\,(6p+1)$ contineatur, tum etiam formulam $a^p - 1$ per $6p+1$ fore divisibilem, id quod quoque continget si fuerit $a = c^6 \pm \lambda\,(6p+1)$.

263. Si sit $4p+1$ numerus primus, ut $a^{4p} - 1$ per eum sit divisibile, tum adeo $a^{2p} - 1$ per eum dividi poterit, si fuerit $a = c^4 \pm \lambda\,(4p+1)$. Dantur vero etiam casus, quibus formula $a^{2p} - 1$ divisionem non admittet: iis ergo vel $a^p + 1$, vel $a^{2p} + 1$ certe per $4p+1$ erit divisibile.