Caput IX.

De divisoribus numerorum formae $a^n \pm b^n$.

264. Posito $2p+1$ numero primo, dum a et b ejus non sint multipla, tam haec formula $a^{2p}-1$ quam ista $b^{2p}-1$ per eum erit divisibilis; ideoque etiam earum differentia $a^{2p}-b^{2p}$ semper per numerum primum $2p+1$ divisionem admittet.

265. Ponamus jam numerum a^n-b^n divisibilem esse per numerum primum $2p+1$, et ut exploremus, quomodo hoc fieri possit, ponamus φ esse maximum communem divisorem numerorum n et $2p$, ita ut posito $n=\alpha\varphi$ et $2p=\beta\varphi$, numeri α et β futuri sint primi inter se.

266. Cum autem α et β sint numeri primi inter se, fieri potest $\mu\alpha=\nu\beta+1$. Quare cum $a^{\alpha\varphi}-b^{\alpha\varphi}$ per $2p+1$ sit divisibilis, etiam $a^{\mu\alpha\varphi}-b^{\mu\alpha\varphi}$, hoc est $a^{(\nu\beta+1)\varphi}-b^{(\nu\beta+1)\varphi}$ erit divisibilis, tum vero ob $a^{\beta\varphi}-b^{\beta\varphi}$, quoque hic numerus $a^{\nu\beta\varphi}-b^{\nu\beta\varphi}$, nec non idem per a^φ multiplicatus, scilicet $a^{(\nu\beta+1)\varphi}-a^\varphi b^{\nu\beta\varphi}$.

267. Auferatur haec posterior forma a praecedente, et differentia $a^\varphi b^{\nu\beta\varphi}-b^{(\nu\beta+1)\varphi}=b^{\nu\beta\varphi}(a^\varphi-b^\varphi)$ divisibilis erit per numerum primum $2p+1$. At $b^{\nu\beta\varphi}$ per eum non est divisibilis, ergo alter factor $a^\varphi-b^\varphi$ divisibilis sit necesse est.

268. Quare si numerus a^n-b^n divisibilis sit per numerum primum $2p+1$, fueritque φ maximus communis divisor numerorum n et $2p$, etiam hic numerus $a^\varphi-b^\varphi$ per $2p+1$ divisibilis erit, et nisi posterior divisionem admittat, ne prior quidem admittet.

269. Quodsi ergo n et $2p$ fuerint numeri inter se primi, seu unitas maximus eorum communis divisor, nisi $a-b$ sit divisibile per $2p+1$, etiam a^n-b^n per hunc numerum primum divisionem non admittet.

270. Divisores ergo primos numeri a^n-b^n investigaturi, praeter divisores ipsius $a-b$, qui sponte se offerunt, reliquos quaerere debemus inter eos numeros primos $2p+1$, in quibus $2p$ ad n non est primus, sed compositus.

271. Unde si n sit numerus primus, omnes divisores numeri a^n-b^n praeter eos, quos $a-b$ continet, tantum inter numeros primos hujus formae $\lambda n+1$ quaerere debemus, siquidem a et b sint numeri primi inter se, quam conditionem adjici debere manifestum est.

272. Pro variis ergo valoribus ipsius n divisores primi formae a^n-b^n praeter $a-b$ quaeri debent, ut sequitur: (*)

formae	divisores quaeri debent inter hos numeros primos:
a^2-b^2	$2\lambda+1$ ... 3, 5, 7, 11, 13, 17, 19, nullis exclusis
a^3-b^3	$3\lambda+1$ ... 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, etc.
a^5-b^5	$5\lambda+1$ ... 11, 31, 41, 61, 71, 101, etc.
a^7-b^7	$7\lambda+1$ ... 29, 43, 71, 113, 127, etc.
$a^{11}-b^{11}$	$11\lambda+1$ ... 23, 67, 89, 199, 331, etc.

etc.

(*) *Script. ad marg.* 1. Ad divisores formae a^n-b^n etiam accedere potest ipse numerus n. 2. Ex a^3-b^3 sequitur numerum $aa+ab+bb$ alios divisores habere non posse nisi $3\lambda+1$; ergo $3\lambda-1$ certe non sunt divisores.

273. Si n non sit numerus primus, sed productum duorum primorum, puta $n = \alpha\beta$, divisores primi formae $a^{\alpha\beta} - b^{\alpha\beta}$ praeter $a - b$ continentur in forma $2p + 1$, existente $2p$ ad $\alpha\beta$ non primo, unde, prout vel α, vel β, vel adeo $\alpha\beta$ fuerit maximus communis divisor, forma divisorum primorum erit vel $\lambda\alpha + 1$, vel $\lambda\beta + 1$, vel $\lambda\alpha\beta + 1$, in quarum prima λ non debet continere β, in secunda autem non α, in tertia vero non limitatur.

274. At divisores formae $\lambda\alpha + 1$ simul dividunt $a^\alpha - b^\alpha$, et divisores formae $\lambda\beta + 1$ simul hanc $a^\beta - b^\beta$, siquidem in priore λ sit numerus primus ad β, in posteriori autem ad α.

275. Quare si formulae $a^{\alpha\beta} - b^{\alpha\beta}$ ii tantum divisores desiderentur, qui non simul dividant vel $a^\alpha - b^\alpha$, vel $a^\beta - b^\beta$, ii quaeri debent inter numeros primos formae $\lambda\alpha\beta + 1$; sin autem tantum divisores formae $a^\alpha - b^\alpha$ excludere velimus, reliquos inter numeros primos $\lambda\beta + 1$ quaerere debemus.

276. Sit $\alpha = 2$ et $\beta = 2$, atque omnes divisores primi hujus numeri $a^4 - b^4$, qui non simul dividant $a^2 - b^2$, continebuntur in forma $4\lambda + 1$; hique ergo divisores erunt numeri $a^2 + b^2$; unde patet numeros formae $a^2 + b^2$ alios divisores primos non admittere, nisi qui sint formae $4\lambda + 1$.

277. Sit $\alpha = 3$ et $\beta = 2$, atque omnes divisores primi numerorum $a^6 - b^6$, qui non simul dividant $a^3 - b^3$, continentur in forma $2\lambda + 1$; qui autem insuper quoque non $a^2 - b^2$ dividant, in hac $6\lambda + 1$; hi ergo erunt divisores formae $a^2 - ab + b^2$, neque tales numeri alios divisores agnoscunt.

278. Ex his in genere colligimus, si definiendi sint divisores numeri $a^{2m} - b^{2m}$, qui non simul sint divisores numeri $a^m - b^m$; hoc est, si desiderentur divisores numeri $a^m + b^m$, eos inter numeros primos hujus formae $2\lambda m + 1$ quaeri oportere. Hinc autem excluditur divisor $a + b$, si m sit numerus impar.

279. Ita pro variis valoribus ipsius m faciamus hanc tabulam:

Numerorum formae	divisores quaeri debent inter numeros primos formae
$a^2 + b^2$	$4\lambda + 1$ qui sunt 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97
$a^3 + b^3$	$6\lambda + 1$ 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$a^4 + b^4$	$8\lambda + 1$ 17, 41, 73, 89, 97, 113, 137, 193
$a^5 + b^5$	$10\lambda + 1$ 11, 31, 41, 61, 71, 101, 131, 151, 181
$a^6 + b^6$	$12\lambda + 1$ 13, 37, 61, 73, 97, 109, 157, 181, 193
$a^7 + b^7$	$14\lambda + 1$ 29, 43, 71, 113, 127, 197, 211, 239
$a^8 + b^8$	$16\lambda + 1$ 17, 97, 113, 193, 241, 257, 337

etc.

hic casus, ubi exponens est potestas binarii, prae reliquis sunt notandi, quia in reliquis generatim divisores assignari possunt. Tales ergo numeri $a^{2^n} + b^{2^n}$ alios divisores primos non habent, nisi qui in forma $2^{n+1}\lambda + 1$ contineantur.

280. At $a^n - b^n$ dividi poterit per numerum primum $mn + 1$, si numeri a et b ita fuerint comparati, ut $ax^m - by^m$ fiat divisibile per $mn + 1$; dum scilicet pro x et y numeri assignari queant, quibus ista conditio adimpleatur, tum certe $a^n - b^n$ per $mn + 1$ erit divisibile.

281. Si enim $ax^m - by^m$ sit divisibile per $mn+1$, tum etiam $a^n x^{mn} - b^n y^{mn}$ erit divisibile. At semper divisibilis est haec forma $x^{mn} - y^{mn}$, ideoque etiam ista $a^n x^{mn} - a^n y^{mn}$, quamobrem etiam differentia $a^n y^{mn} - b^n y^{mn}$, ac proinde $a^n - b^n$ per numerum primum $mn+1$ divisibile erit.

282. Si ergo pro a et b ejusmodi numeri assumantur, ut $a^n - b^n$ non sit divisibilis per numerum quempiam primum $mn+1$, tum nulli numeri pro x et y assignari poterunt, ut $ax^m - by^m$ per eundem numerum primum $mn+1$ divisionem admittat, nisi quidem uterque numerus x et y sit ejusdem multiplum, statuuntur autem x et y primi inter se.

283. Sic cum $2^2 - 1$ tantum per 3 sit divisibile, fueritque $2m+1$ numerus primus, tum nisi sit $m = 1$, nullus numerus in hac forma contentus $2x^m - y^m$ per illum numerum primum $2m+1$ dividi poterit:

ita posito	nullus numerus	divisibilis erit per
$m = 2$	$2x^2 - y^2$	5
$m = 3$	$2x^3 - y^3$	7
$m = 5$	$2x^5 - y^5$	11
$m = 6$	$2x^6 - y^6$	13
	etc.	

Caput X.

De residuis ex divisione quadratorum per numeros primos ortis.

284. Quod residuum relinquitur, si quadratum a^2 per numerum quemvis d dividatur, idem quoque relinquitur, si haec infinita quadrata $(nd \pm a)^2$ per eundem numerum d dividantur.

285. Quare si residua examinare velimus, quae divisione numerorum quadratorum per datum numerum d relinquuntur, sufficiet quadrata considerasse, quorum radices sint ipso hoc divisore d minores, ideoque haec

$$1,\ 4,\ 9,\ 16 \ldots . (d-4)^2,\ (d-3)^2,\ (d-2)^2,\ (d-1)^2,$$

quorum numerus est $d-1$.

286. At quadrata extrema 1 et $(d-1)^2$, et quaevis bina, ab extremis aeque remota, paria dant residua; unde si $d-1$ sit numerus par, plura residua diversa resultare nequeunt, quam $\frac{1}{2}(d-1)$, et si $d-1$ est numerus impar, ob unum in medio positum, quam $\frac{1}{2}d$.

287. Sit jam d numerus primus, et quia binarii judicium in promtu est, ponatur $d = 2p+1$, cum nunc omnia residua ex his quadratis resultent $1, 4, 9, \ldots (p-2)^2, (p-1)^2, p^2$, eorum numerus major esse nequit quam p, unde manifestum est non omnes numeros ipso $d = 2p+1$ minores, quorum multitudo est $2p$, inter residua occurrere, sed ad minimum eorum semissem excludi.

288. Primum autem dico, omnia residua ex his quadratis $1, 4, 9 \ldots p^2$ oriunda inter se esse inaequalia; si enim duo quadrata ipso p^2 non majora, puta m^2 et n^2, idem darent residuum, eorum differentia $m^2 - n^2$, ideoque vel $m-n$, vel $m+n$ per divisorem primum $d = 2p+1$ esset divisibilis, quod, cum, ob $m < \frac{1}{2}d$ et $n < \frac{1}{2}d$, sit $m+n$ minus quam d, fieri nequit.

*