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.

*

289. Cum igitur omnia residua, ex divisione quadratorum $1, 4, 9 \ldots p^2$ per numerum primum $d = 2p + 1$ orta, sint inaequalia, ea ita repraesentemus:

radices	1	2	3	4	5	6	$\ldots\ldots p$
quadrata	1	4	9	16	25	36	$\ldots\ldots p^2$
residua	1	α	β	γ	δ	ε	$\ldots\ldots \pi$

et multitudo horum residuorum erit $= p$.

290. Cum jam multitudo omnium numerorum ipso divisore $2p + 1$ minorum, qui simul ad eum sunt primi, sit $= 2p$, patet horum numerorum semissem ex ordine residuorum excludi, quos ideo *non-residua* appellemus. Erit ergo multitudo non-residuorum pariter $= p$, quae litteris germanicis $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. indicemus.

291. Si ergo pro quovis divisore primo $2p + 1$ haec non-residua invenerimus, affirmare poterimus, nullum dari numerum quadratum xx, ita ut $xx - \mathfrak{A}$ esset per $2p + 1$ divisibile, denotante $\mathfrak{A}$ non-residuum quodcunque. Ac tales formulae $xx - \mathfrak{A}$ per $2p + 1$ individuae tot semper exhiberi possunt, quot p continet unitates.

292. Pro quovis ergo divisore primo $2p+1$ numeri ipso minores distinguuntur in duas classes, quarum altera residua, altera vero non-residua complectitur, et utraque totidem continet numeros, ita ut quasi cuivis residuo suum respondeat non-residuum. Indolem ergo harum duarum classium accuratius scrutari conveniet.

293. Si in ordine residuorum occurrant duo numeri m et n, in eodem quoque occurret eorum productum mn, seu residuum ei aequivalens. Oriatur enim residuum m ex quadrato a^2 et n ex b^2, atque ex producto a^2b^2, quod pariter est quadratum, orietur residuum mn.

294. Si ergo inter residua sit numerus quicunque m, ibidem quoque reperientur omnes ejus potestates m^2, m^3, m^4, etc., vel residua iis aequivalentia. Tum vero si praeterea adsit numerus n, in eodem residuorum ordine quoque aderunt numeri mn, m^2n, mn^2 et in genere $m^\mu n^\nu$.

295. Ordo ergo residuorum $1, \alpha, \beta, \gamma \ldots \pi$, pro quovis divisore primo $2p + 1$, hanc insignem habet proprietatem, ut in eodem quoque producta ex binis pluribusve terminis quibuscunque occurrant, siquidem secundum indolem residuorum ad minimos valores revocentur.

296. Hoc eo magis est notatu dignum, quod ordo residuorum determinato terminorum numero constat, quorum scilicet numerus tantum sit $= p$, exclusis totidem numeris non-residuis. Hoc tamen non obstante, quomodocunque residua per multiplicationem inter se combinentur, tamen perpetuo numeri in eodem ordine jam contenti occurrunt.

297. Sit m numerus quicunque in ordine residuorum occurrens, divisore primo existente $2p+1$, ac supra vidimus, si termini progressionis geometricae $1, m, m^2, m^3, m^4$, etc. per $2p + 1$ dividantur, inter residua quoque omnia producta ex binis contineri; sicque in residuis harum potestatum nulli occurrent numeri, qui non simul in residuis quadratorum reperiantur.

298. Cum igitur multitudo residuorum, ex potestatibus oriundorum, superare nequeat multitudinem ex quadratis ortorum, quae est $= p$, manifestum est vel potestatem m^p, vel adhuc inferiorem residuum

praebere $=1$. Quod quidem jam ostendimus, nam si m ex quadrato aa oriatur, erit $m = aa - k(2p+1)$; et $m^p - 1$ manifesto per numerum primum $2p+1$ est divisibile.

299. Sed ad residua quadratorum revertentes notemus, si ibi occurrant numeri m et mn, tum etiam necessario ibidem numerum n reperiri debere. Si enim residuum m oriatur ex quadrato aa, et mn ex quadrato bb, ex naa quoque residuum mn nascetur, unde $bb - naa$ per $2p+1$ erit divisibile, existentibus a et b ad $2p+1$ primis.

300. At si $bb - naa$ divisibile est per $2p+1$, etiam $(b + k(2p+1))^2 - naa$ erit divisibile. Semper autem k ita assumere licet, ut fiat $b + k(2p+1) = ac$, seu ut $k(2p+1)$ per a divisum relinquat b. Dabitur ergo numerus c, ut sit $aacc - naa$, hoc est $cc - n$ per $2p+1$ divisibile, quare quadratum cc dabit residuum n.

301. Si in ordine residuorum sit numerus α, non-residuorum vero numerus $\mathfrak{A}$, productum $\alpha\mathfrak{A}$ in ordine non-residuorum certe reperietur. Si enim in ordine residuorum esset, ibidem quoque foret $\mathfrak{A}$, contra hypothesin.

302. Si in ordine residuorum occurrat productum mn, ejusque alter factor m in ordine non-residuorum, alter quoque n certo in eodem ordine non-residuorum reperietur; si enim hic n esset in residuis, eodem quoque m pertineret.

303. Si duo non-residua $\mathfrak{A}$ et $\mathfrak{B}$ in se ducantur, productum incidet in ordinem residuorum. Nam cum in ordine residuorum omnia quadrata occurrant, primo evidens est omnia quadrata $\mathfrak{A}^2$, $\mathfrak{B}^2$, $\mathfrak{C}^2$, etc. ibi esse; quod vero etiam producta binorum $\mathfrak{A}\mathfrak{B}$ ibidem reperiantur, ulteriori indiget probatione jam instituenda.

304. Cognitis residuis 1, α, β, γ, etc., quorum numerus est $= p$, divisore primo existente $2p+1$, non-residua quidem eo ipso dantur, cum sint reliqui numeri minores quam $2p+1$, quorum numerus itidem est $= p$. At dato uno non-residuo $\mathfrak{A}$, reliqua omnia ex ipsis residuis ita determinantur, ut sint $\mathfrak{A}$, $\alpha\mathfrak{A}$, $\beta\mathfrak{A}$, $\gamma\mathfrak{A}$, etc., reductione scilicet ad minimos terminos facta. Sunt enim hi numeri inaequales inter se, et eorum multitudo $= p$.

305. Duo igitur quaecunque non-residua $\mathfrak{D}$ et $\mathfrak{E}$ spectari possunt tanquam hujusmodi producta $\delta\mathfrak{A}$ et $\varepsilon\mathfrak{A}$, existentibus δ et ε residuis, $\mathfrak{A}$ vero non-residuo; unde productum duorum quorumvis non-residuorum erit $\mathfrak{D}\mathfrak{E} = \delta\varepsilon\mathfrak{A}\mathfrak{A}$, ubi $\delta\varepsilon$ utpote productum duorum residuorum in ordine residuorum reperitur.

306. Tum vero in ordine residuorum occurrit etiam $\mathfrak{A}\mathfrak{A}$, quia in eo omnia plane quadrata, seu residua aequivalentia reperiuntur. Quare cum tam $\delta\varepsilon$ quam $\mathfrak{A}\mathfrak{A}$ sit residuum, eorum productum quoque $\mathfrak{D}\mathfrak{E}$ residuum sit necesse est, sicque productum duorum quorumvis non-residuorum certe in ordine residuorum continetur.

307. Combinatio ergo duorum numerorum pro indole residuorum et non-residuorum ita se habet:

1. Productum ex duobus residuis est residuum.
2. Productum ex residuo et non-residuo est non-residuum.
3. Productum ex duobus non-residuis est residuum.

308. Non mediocriter haec illustrabuntur, si residua et non-residua ex divisione quadratorum per numeros primos contemplemur:

divisor	3					5					7							11				
residua	1					1,	4				1,	4,	2					1,	4,	9,	5,	3
non-residua	2					2,	3				3,	5,	6					2,	6,	7,	8,	10
divisor	13													17								
residua	1,	4,	9,	3,	12,	10					1,	4,	9,	16,	8,	2,	15,	13				
non-residua	2,	5,	6,	7,	8,	11					3,	5,	6,	7,	10,	11,	12,	14				
divisor	19										23											
residua	1,	4,	9,	16,	6,	17,	11,	7,	5		1,	4,	9,	16,	2,	13,	3,	18,	11,	8,	6	
non-residua	2,	3,	8,	10,	12,	13,	14,	15,	18		5,	7,	10,	12,	14,	15,	17,	19,	20,	21,	22	
divisor	29																					
residua	1,	4,	9,	16,	25,	7,	20,	6,	23,	13,	5,	28,	24,	22								
non-residua	2,	3,	8,	10,	11,	12,	14,	15,	17,	18,	19,	21,	26,	27 (*).								

309. *Complementum* residui vocemus numerum, qui cum residuo faciat divisorem; ita si divisore existente $= d$, sit quodpiam residuum $= r$, ejus complementum erit $d - r$.

310. Si cujuspiam residui complementum occurrat in ordine residuorum, etiam omnium residuorum complementa ibidem occurrent. Nam si in ordine residuorum $1, \alpha, \beta, \gamma, \delta$, etc. occurrat $d - \alpha$, divisore existente d, hoc residuum $d - \alpha$ etiam per $-\alpha = -1.\alpha$ repraesentari potest, quare cum tam α quam productum $-1.\alpha$ sit residuum, etiam -1 erit residuum, ideoque etiam $-\beta, -\gamma, -\delta$, etc. quibus aequivalent complementa reliquorum residuorum.

311. In serie ergo residuorum vel nullius, vel omnium complementa occurrent. Ex superioribus exemplis patet, si divisor sit vel 3, vel 7, vel 11, vel 19, vel 23, nullius residui complementum in residuis reperiri, sed ea esse non-residua. Sin autem divisor sit 5, vel 13, vel 17, vel 29, in ordine residuorum quoque singulorum complementa inveniri.

312. Si divisor sit $2p + 1$ primus, atque in residuis quoque singulorum complementa occurrant, quoniam bina ita inter se cohaerent, ut alterum alterius sit complementum, neque idem sui ipsius complementum esse potest, ob $2p + 1$ semissem non admittentem, numerus residuorum necessario erit par.

313. Cum igitur numerus residuorum sit $= p$, nisi p sit numerus par, fieri nequit, ut residuorum complementa sint etiam residua. Quare si p sit numerus impar, certum est nullius residui complementum in ordine residuorum contineri, ideoque omnium residuorum complementa ordinem non-residuorum constituent.

314. Sit igitur p numerus impar $= 2q - 1$, ut divisor primus sit $4q - 1$, atque omnium residuorum complementa erunt non-residua. Ita si quodpiam residuum sit α, ejus complementum

(*) *Script. ad marg.* Divisor: 59. Residua: 1, -2, 3, 4, 5, -6, 7, -8, 9, -10, -11, 12, -13, -14, 15, 16, 17, -18, 19, 20, 21, 22, -23, -24, 25, 26, 27, 28, 29. Ergo *si* $4n - 1$ est primus, vel $xx + myy$, vel talis forma $xx - myy$ per eum est divisibilis.

$4q - 1 - \alpha$ erit non-residuum, seu nullum datur quadratum, quod per $4q - 1$ divisum, relinquat $4q - 1 - \alpha$.

315. Cum igitur α quodcunque quadratum denotare possit, puta nn, nullum datur quadratum, quod numero $4q - 1 - nn$ minutum, per $4q - 1$ dividi queat. Hinc $mm - (4q - 1 - nn)$, seu $mm + nn$ nunquam per numerum primum formae $4q - 1$ divisibile existet, nisi forte uterque numerus m et n seorsim per eum sit divisibilis.

316. Demonstratum ergo est summam duorum quadratorum inter se primorum dividi non posse per ullum numerum primum hujus formae $4q - 1$. Quodsi ergo talis binorum quadratorum summa habeat divisores primos, ii certo erunt hujus formae $4q + 1$, remoto scilicet binario, qui etiam quandoque divisor esse potest, ambobus quadratis sumtis imparibus.

317. Quando residuorum complementa inter residua deprehenduntur, complementa non-residuorum etiam erunt non-residua; ac si unius residui complementum fuerit non-residuum, omnium residuorum complementa erunt non-residua, atque complementa omnium non-residuorum vicissim erunt residua.

318. Si divisore existente $2p + 1$, sit p numerus par, his solis casibus evenire potest, ut residuorum complementa quoque sint residua; quod autem semper sint residua, hinc nondum est evictum. Ad hoc autem comparari debent haec residua cum residuis ex serie potestatum ortis, ab eodem divisore $2p + 1$, si series potestatum ita fuerit comparata, ut multitudo residuorum aequalis sit multitudini non-residuorum.

319. Sit $1, a, a^2, a^3$, etc. hujusmodi series potestatum, quae p residua diversa praebeat, divisore existente primo $= 2p + 1$, ita ut omnia residua futura sint $1, a, a^2, a^3, \ldots . a^{p-1}$, ipsas scilicet potestates tanquam residuis aequivalentes adhibendo. Non-residua autem sint totidem numero, ita expressa: $A, Aa, Aa^2, Aa^3, \ldots . Aa^{p-1}$.

320. Hic jam residua, pariter ac residua quadratorum, ita sunt comparata, ut 1) ab unitate incipiant, 2) producta binorum residuorum quoque sint residua, 3) producta ex residuo et non-residuo inter non-residua occurrant, unde concludere licet producta ex binis non-residuis iterum in ordinem residuorum transire.

321. Si $a^p - 1$ divisibile sit per $2p + 1$, tum a certe est residuum quadratorum. Si enim esset non-residuum, omnia reliqua residua, quae sunt $a\alpha$, $a\beta$, $a\gamma$, etc. eandem haberent proprietatem, ideoque omnes numeri x ita essent comparati, ut $x^p - 1$ per $2p + 1$ dividi posset, quod est absurdum (*).

322. Cum enim in residuis quadratorum res ita se habeat, ubi numerus non-residuorum aequalis est numero residuorum, si in residuis potestatum secus eveniret, et producta ex binis non-residuis iterum darent non-residuum, multitudo non-residuorum superaret multitudinem residuorum, contra hypothesin.

323. Hoc autem firmius ita ostendi potest: Cum A quodvis non-residuum denotare possit, ac tum aliud quodvis non-residuum ita repraesentari possit, ut sit Aa^n, productum binorum non-

(*) Hic paragraphus in autographo margini adscriptus est.

residuorum erit AAa^n, quod si esset non-residuum, aequivaleret tali formae Aa^m, vel tali Aa^{m+vp}, ita ut m majus sit quam n, ideoque differentia $Aa^m - AAa^n$ foret per $2p+1$ divisibilis.

324. Cum autem neque A neque a^n per $2p+1$ dividi queat, foret $a^{m-n} - A$ per $2p+1$ divisibile, seu potestas a^{m-n} per $2p+1$ divisa relinqueret residuum A. Cum autem A non sit residuum, sequitur hanc hypothesin esse absurdam, ideoque productum duorum non-residuorum non in forma Aa^m, quae omnia non-residua complectitur, contineri, ideoque necessario inter residua occurrere debere.

325. Quare si a sit ejusmodi numerus, ut a^p sit minima potestas, quae per numerum primum $2p+1$ divisa, unitatem relinquat, ideoque ex divisione terminorum progressionis geometricae $1, a, a^2, a^3, a^4 \ldots a^{p-1}$ tot residua diversa oriantur, quot p continet unitates, totidemque dentur non-residua, certum est omnia producta binorum non-residuorum in ordine residuorum contineri.

326. Cum autem omnes numeri divisore $2p+1$ minores vel in residuis, vel in non-residuis contineantur, singulorum quadrata in ordine residuorum certo occurrent, quod cum etiam eveniat in residuis ex quadratis ortis, sequitur ambos ordines residuorum, tam ex quadratis quam ex superiori progressione geometrica ortos, plane inter se congruere.

327. Quodsi ergo pro divisore primo $2p+1$ sint residua ex quadratis orta $1, \alpha, \beta, \gamma, \delta$, etc., tum vero $\mathfrak{A}$ fuerit quodvis non-residuum, hic numerus $\mathfrak{A}$ etiam inter non-residua reperietur, quae progressioni geometricae $1, a, a^2, a^3, \ldots . a^{p-1}$ respondent, si quidem a^p fuerit minima potestas unitatem pro residuo praebens.

328. Jam supra vidimus, si a fuerit residuum ex quadratis ortum, fore $a^p - 1$ certo per $2p+1$ divisibile; nunc autem patet, si a fuerit non-residuum respectu quadratorum, tum a^p non esse minimam potestatem ipsius a, quae per $2p+1$ divisa, unitatem relinquat. Ergo vel unitatem non relinquet, vel dabitur adhuc minor $a^{\frac{p}{\nu}}$, quae unitatem relinquet.

329. Si sit a ejusmodi numerus, ut potestas ejus a^p, per numerum primum $2p+1$ divisa, relinquat unitatem, tum a certe inter residua quadratorum continetur. Hoc evidens est, si a^p sit minima potestas istius indolis. Sin autem non sit minima, id eo magis verum esse videtur. Nam si detur minor, ex residuis illis, numero p, quaedam transeunt in ordinem non-residuorum. Si enim $a^{\frac{1}{2}p}$ sit minima, tum a adeo inter residua biquadratorum, sin $a^{\frac{1}{3}p}$, inter residua potestatum sextarum etc., ergo semper inter residua quadratorum continebitur.

330. Si ergo a fuerit non-residuum ratione quadratorum, tum $a^p - 1$ certe non est divisibile per $2p+1$, unde si a sit complementum cujuspiam residui, puta $a = d - \alpha$, ponendo $d = 2p+1$, tum $(d-\alpha)^p - 1$ non est divisibile per $2p+1$, at $\alpha^p - 1$ certe est divisibile, ob α residuum, unde differentia $(d-\alpha)^p - \alpha^p$ etiam non erit divisibilis.

331. At haec differentia esset divisibilis, si p esset numerus par, quare nisi p sit numerus impar, illa conditio, qua $(d-\alpha)^p - 1$ indivisibile per $2p+1$ assumsimus, hoc est qua $d - \alpha$ est non-residuum, subsistere nequit.

332. At si p sit numerus par, complementum cujuspiam residui α, puta $d - \alpha$, certe est residuum, propterea quod $(d-\alpha)^p - 1$ per $2p+1$ est divisibile; si enim esset non-residuum, haec divisibilitas locum habere non posset.

333. Si ergo sit $p = 2q$, numerusque primus divisor propositus $= 4q + 1$, tum inter residua quadratorum, etiam singulorum complementa deprehendentur, hoc est, si residua fuerint $1, \alpha, \beta, \gamma$, etc. etiam residua erunt $-1, -\alpha, -\beta, -\gamma$, etc.

334. Pro quovis ergo quadratorum, ex hac progressione $1, 4, 9, 16 \ldots 4qq$ assumto, dabitur aliud, quod ad illud additum producit summam per $4q + 1$ divisibilem, seu cum multitudo horum quadratorum sit $= 2q$, et quodlibet habet quasi suum conjugatum, dabuntur q paria duorum quadratorum diversa, quorum summa sit per $4q + 1$ divisibilis. (*)

335. Et quia singula quadrata non superant $4qq$, binorum summa certe minor est quam $8qq$, unde si talis summa per $4q + 1$ dividatur, quotus certe erit minor quam $2q$. Hic autem quotus nisi sit $= 2$, etiam erit vel numerus primus formae $4n + 1$, vel talium aliquod productum (316).

336. Quoties ergo divisor primus est formae $4q + 1$, toties inter residua quadratorum occurrit $4q$, ideoque etiam q, tanquam complementum unitatis, cui aequivalet -1: parique modo ibidem etiam occurrunt omnia reliqua quadrata negativa -4; -9, -16, etc., ita ut residua constituantur complexa, tam quadratorum ipsorum, quam eorundem negative sumtorum, una cum productis ex binis quibusque, quorum tamen omnium numerorum, si per divisorem $4q + 1$ ad minimam formam perducantur, multitudo erit $= 2q$, ita ut totidem excludantur.

337. Contra autem, si divisor primus sit formae $4q - 1$, tum -1 et omnia quadrata negativa inter non residua referuntur (**). Si enim -1 esset residuum, foret $(-1)^{2q-1} - 1$ divisibile per $4q - 1$, quod autem fieri nequit. Praecedente autem casu, si -1 esset non-residuum, divisore existente $4q + 1$, tum $(-1)^{2q} - 1$ non esset divisibile per $4q + 1$, quod perinde est falsum.

338. Sola autem quadrata semper in ordine residuorum reperiuntur, reliqui vero numeri, pro ratione divisoris, mox inter residua, mox inter non-residua cadunt, quemadmodum modo vidimus -1 esse residuum, si divisor sit $4q + 1$; at -1 esse non-residuum, si divisor sit $4q - 1$.

339. Pro ceteris numeris non-quadratis simile discrimen observatur: Scilicet numerus $+2$ inter residua reperitur, quoties divisor primus est vel hujus $8q + 1$, vel hujus formae $8q - 1$, seu $8q + 7$. Reliquis casibus, quibus divisor est vel $8q + 3$, vel $8q + 5$, numerus $+2$ inter non-residua locum occupat. (***)

340. At numerus -2 inter residua occurrit casibus, quibus divisor primus est vel $8q + 1$, vel $8q + 3$; idem vero numerus -2 inter non-residua cadit casibus, quibus divisor primus est vel $8q + 5$, vel $8q + 7$.

341. Numerus porro $+3$ est residuum, si divisor primus sit vel $12q + 1$, vel $12q + 11$; at idem erit non-residuum, si divisor sit vel $12q + 5$, vel $12q + 7$. Verum numerus -3 est residuum, si divisor primus sit vel $12q + 1$, vel $12q + 7$: at -3 erit non-residuum, si divisor sit $12q + 5$, vel $12q + 11$.

Scripturae ad marginem:

(*) Semper duo exhiberi possunt quadrata, quorum summa divisibilis sit per numerum primum $4q + 1$, et quidem alterum quadratum ad lubitum assumi potest.

(**) Non ergo datur summa duorum quadratorum per talem numerum primum $4q - 1$ divisibilis.

(***) Hoc autem non, ut praecedens, demonstratione muniri potest.

342. Numerus $+4$ semper ad residua refertur, et de -4 idem est judicium ac de -1. Numerus autem 5 reperitur inter residua, si divisor sit vel $20q+1$, vel $20q+9$, vel $20q+11$, vel $20q+19$; at -5 inter residua deprehenditur, si divisor sit vel $20q+1$, vel $20q+3$, vel $20q+7$, vel $20q+9$.

343. Colligamus haec, ut uni conspectui exponantur:

Inter residua erit numerus	si divisor primus fuerit
$+1$	$4q+(1,\ 3)$
-1	$4q+1$
$+2$	$8q+(1,\ 7)$ (*)
-2	$8q+(1,\ 3)$
$+3$	$12q+(1,\ 11)$
-3	$12q+(1,\ 7)$
$+5$	$20q+(1,\ 9,\ 11,\ 19)$
-5	$20q+(1,\ 3,\ 7,\ 9)$
$+6$	$24q+(1,\ 5,\ 19,\ 23)$
-6	$24q+(1,\ 5,\ 7,\ 11)$
$+7$	$28q+(1,\ 3,\ 9,\ 19,\ 25,\ 27)$
-7	$28q+(1,\ 9,\ 11,\ 15,\ 23,\ 25)$
$+10$	$40q+(1,\ 3,\ 9,\ 13,\ 27,\ 31,\ 37,\ 39)$
-10	$40q+(1,\ 7,\ 9,\ 11,\ 13,\ 19,\ 23,\ 37)$
$+11$	$44q+(1,\ 9,\ 25,\ 5,\ 7,\ 37,\ 39,\ 19,\ 35,\ 43)$
-11	$44q+(1,\ 9,\ 25,\ 5,\ 37,\ 3,\ 15,\ 23,\ 27,\ 31)$
$+12$	$48q+(1,\ 11,\ 13,\ 23,\ 25,\ 35,\ 37,\ 47)$
-12	$48q+(1,\ 13,\ 25,\ 37,\ 7,\ 19,\ 31,\ 43)$
$+14$	$56q+(1,\ 5,\ 9,\ 13,\ 25,\ 45,\ 11,\ 31,\ 43,\ 47,\ 51,\ 55)$
-14	$56q+(1,\ 5,\ 9,\ 13,\ 25,\ 45,\ 3,\ 15,\ 19,\ 23,\ 27,\ 39)$
$+15$	$60q+(1,\ 7,\ 11,\ 17,\ 43,\ 49,\ 53,\ 59)$
-15	$60q+(1,\ 17,\ 49,\ 53,\ 19,\ 23,\ 31,\ 47)$ (**)
	etc.

344. Haec autem hactenus tantum inductione nituntur, atque ad demonstrationem investigandam juvabit sequentia observasse. Primo, numerus quicunque $\pm n$ inter residua reperietur, si divisor primus fuerit formae $4nq+1$, vel adeo $4nq+ii$, denotante i numerum imparem quemcunque.

Scripturae ad marginem;

(*) $xx-2yy$ alios divisores primos non admittit, nisi formae $8q+(1,7)$.

(**) 1) Si $xx=mn+r$, tum quadratum xx tam per m quam n divisum, idem relinquet residuum r. Ergo si residuum r convenit divisori m, conveniet etiam divisori n.

2) Si

divisor	inter non-resid.	residuum
$4n-1$	-1	
$8n-1$	-2	$+2$
$8n-3$	± 2	
$12n-1$	-3	$+3$
$12n-7$	± 3	
$8n\pm 3$	$+2$	

Hoc demonstrari potest; at si divisor $8n+1$, inter residua est $+2$, quod autem hinc non demonstratur.

Deinde etiam numerus positivus $+n$ erit residuum, si divisor primus fuerit formae $4nq-1$, vel generalius $4nq-ii$; pro his autem divisoribus numerus negativus $-n$ inter non-residua reperietur.

345. Si numerus positivus n sit residuum pro divisore d, erit etiam residuum pro divisore primo quocunque formae $4nq \pm d$, vel adeo $4nq \pm dii$; at si numerus negativus $-n$ sit residuum pro divisore d, erit is quidem residuum pro divisore $4nq+d$, at non-residuum pro divisore $4nq-d$.

346. Si numerus positivus n fuerit residuum pro divisore d, deinde etiam pro divisore e, erit etiam residuum pro divisore primo quocunque formae $4nq \pm de$. At si numerus negativus $-n$ fuerit residuum pro divisoribus d et e, erit quoque residuum pro divisore quocunque primo formae $4nq+de$; pro divisoribus autem $4nq-de$ inter non-residua referetur.

347. Si numerus positivus n fuerit non-residuum pro divisoribus d et e, certe erit residuum pro divisoribus primis omnibus formae $4nq \pm de$; at si numerus negativus $-n$ sit non-residuum pro divisoribus d et e, is erit residuum pro omnibus divisoribus primis formae $4nq+de$; pro divisoribus autem formae $4nq-de$ erit non-residuum.

348. Quicunque numerus $\pm n$ proponatur, erit is semper residuum, si divisor primus fuerit in aliqua talium formarum $4nq+A$, $4nq+B$, $4nq+C$, etc. contentus, quarum numerus aequatur semissi multitudinis numerorum ad $4n$ primorum eoque minorum. Sin autem divisor in reliquis formis contineatur, erit is non-residuum.

349. Hic autem excipi debent casus, quibus numerus n est quadratus, quippe qui semper inter residua occurrit, quicunque divisores accipiantur. Ac si n sit quadratum negativum, eadem ratio valet ac pro -1.

350. Primum igitur demonstrari debet, si divisor primus sit $4nq+ii$, existente i numero impari, inter residua quadratorum semper occurrere tam numeros n et q, quam eorum negativa $-n$ et $-q$. Sit $i=2m+1$, et quia divisor $4nq+4mm+4m+1$ est formae $4p+1$, inter residua continetur quadratum negativum $-4mm-4m-1$, ideoque numerus $4nq$, et ob 4 residuum, etiam numerus nq, itemque $-nq$, quare vel ambo numeri n et q simul inter residua, vel ambo simul inter non-residua occurrere deberent, unde dum alteruter fuerit inter residua, et alter ibidem reperiatur necesse est.

351. Si n non esset residuum, nullum daretur quadratum xx, ut $xx-n$ divisibile esset per $4nq+4mm+4m+1$. Si ergo demonstrari posset dari hujusmodi quadratum, evicta esset veritas propositionis. Vel si n esset non-residuum, haec expressio $n^{2nq+2mm+2m}-1$ non esset divisibilis per numerum primum, quare si contrarium demonstrari posset, haberemus quod intendimus. (*)

352. Deinde si divisor primus sit $4nq-4mm-4m-1$, inter residua quadratorum occurrere numerum n, inter non-residua vero numerum $-n$, demonstrari oportet. Pari autem jure inter

(*) *Script. ad marg.* Si n esset non-residuum, foret quoque non-residuum nzz, ideoque etiam
$$\pm nzz \mp y(4nq+4mm+4m+1),$$
quae expressio, si uno saltem casu esset quadratum, propositum constaret. Quod ob signa ambigua semper uno saltem casu evenire debere videtur; idque eo magis, cum etiam n et q sint permutabiles, quin etiam verum est, etsi divisor non sit primus. Dubium, si $n=3$, $q=5$, $2m+1=5$, $\pm 3zz \pm 85y$, vel $\pm 5zz \pm 85y$ quadratum effici nequit. Ergo demonstratio ita est adornanda, ut divisor statuatur primus.

residua erit numerus q, et inter non-residua $-q$. Cum autem inter residua certo sit $(2m+1)^2$, ibidem erit $4nq$, ideoque etiam nq.

353. Concessis ergo his propositionibus, etsi demonstratio nondum patet, posito i numero impari et $4nq \pm ii$ primo, pro divisore primo $4nq+ii$, cum residua sint n et $-n$, item naa et $-naa$, semper ejusmodi quadratum xx dabitur, ut sit $xx-naa$ divisibile per $4nq+ii$, deinde etiam ejusmodi quadratum yy, ut sit $yy+naa$ divisibile per $4nq+ii$

354. At divisore primo existente $4nq-ii$, ob residuum naa, semper datur quadratum xx, ut sit $xx-naa$ divisibile per $4nq-ii$; nullum autem existit quadratum yy, ut $yy+naa$ fiat per $4nq-ii$ divisibile, quia hoc casu $-naa$ est non-residuum.

355. Cum $4nq+ii$ sit numerus formae $4p+1$, semper dabitur summa duorum quadratorum $ff+gg$ per eum divisibilis, quorum alterum ff pro lubitu assumi potest. Quare si $xx-naa$ divisibile sit per $4nq+ii$, inveniri potest quadratum yy, ut fiat $xx+yy$ per $4nq+ii$ divisibile, ac tum erit etiam $yy+naa$ per eundem divisibile.

356. Cum $4nq-ii$ sit formae $4p-1$, nulla datur summa quadratorum per $4nq-ii$ divisibilis; quare si $xx-naa$ fuerit per $4nq-ii$ divisibile, fieri nequit ut $yy+naa$ per eundem divisibile existat; foret enim quoque summa $xx+yy$ divisibilis, quod est absurdum.

357. Sumto divisore primo $d=4nq+ii$, quia datur forma $xx+naa$ per eum divisibilis, dabitur etiam forma $yy+qaa$ per eum divisibilis, unde etiam $qxx-nyy$. Dabitur vero etiam forma $yy-qaa$ divisibilis, ac propterea quoque talis forma $qxx+nyy$.

358. Si divisor primus sit $d=4nq-ii$, quia dantur tales formulae $xx-naa$, item $yy-qaa$, per eum divisibiles, etiam haec forma $qxx-nyy$ per d erit divisibilis. Cum autem talis forma $yy+qaa$ non per d sit divisibilis, nulla quoque hujusmodi forma $qxx+nyy$ per d erit divisibilis.

359. Verum etiamsi haec propositiones demonstrari possent, reliquae, quas supra observavimus, nondum essent evictae. Ex 345 si detur quadratum, per d divisum reliquens residuum positivum n, dabitur quoque reliquens naa; tum autem existente $4nq \pm d$ numero primo, dabitur quoque quadratum xx, quod per $4nq \pm d$ divisum relinquat idem residuum, seu $xx-naa$ divisibile erit per $4nq+d$.

360. Scilicet si fuerit $bb-naa$ per d divisibile, semper talis numerus $xx-naa$ dabitur divisibilis per numerum primum $4nq \pm d$. Quin etiam denotante i numerum imparem, ejusmodi forma $xx-naa$ exhiberi potest, quae sit divisibilis per numerum primum $4nq \pm dii$.

361. Si detur quadratum bb, quod per d divisum relinquat residuum negativum $-n$, vel $-naa$, dabitur etiam quadratum xx, quod per numerum primum $4nq+dii$ divisum relinquet $-n$, vel $-naa$. Scilicet si d sit divisor formae $bb+ncc$, dabitur x, ut sit $xx+naa$ divisibile per numerum primum $4nq+dii$.

362. Verum si d divisor formae hujusmodi $bb+ncc$, nulla dabitur hujusmodi forma $xx+naa$, quae sit divisibilis per talem numerum primum $4nq-dii$. Veluti si sit $n=3$, sumatur $d=7$, quia $2^2+3.1=7$, atque certum est hujus formae $xx+3aa$ numeros nullos admittere divisores talis formae $12q-7ii$, cujusmodi sunt: 5, 17, 29, 41, 53, 65, 77, 89, 101, 9, 21, 33, 45.

363. Ex § 346 sequitur, si d et e fuerint divisores cujuspiam numeri hujus formae $aa - nbb$, tum semper dari quadratum xx, ut $xx - ncc$ sit divisibile per numerum primum $4nq \pm deii$, quod quidem ex praecedente deduci posset, demonstrando si $aa - nbb$ habeat divisorem d, aliaque similis forma $ff - ngg$ divisorem e, dari etiam $hh - nkk$ divisibilem per productum de. Hoc patebit, si residua quadratorum, per numeros compositos divisorum, perpendemus.

364. Denique notatu dignum est, quod numerus n, ac propterea etiam naa inter residua quadratorum occurrere nequeat, nisi divisor primus sit hujus formae $4nq + \alpha$, ubi α non omnes numeros ad $4n$ primos eoque minores significat, sed eorum tantum semissem, altera semisse penitus exclusa. Sicque omnes divisores primi formae $xx - naa$ talem habent formam $4nq + \alpha$, denotante α aliquot numeros, totidemque exclusis.

365. Similis est ratio numerorum formae $xx + naa$, cujus divisores primi adstringuntur ita ad formam $4nq + \alpha$, ut totidem numeri excludantur ab α, quot admittuntur. Utroque autem casu omnia quadrata imparia ii pro α valent, et si α valeat, etiam αii valebit.

366. Ut demonstrationes has desideratas tentemus, consideremus divisorem primum $4p + 1$, et cum duorum quadratorum summa $aa + bb$ exhiberi queat per eum divisibilis, ita ut alterum pro lubitu assumi possit, auferatur $(4p + 1)\,bb$, eritque $aa - 4pbb$ per $4p + 1$ divisibile, seu dabitur quadratum aa, quod per $4p + 1$ divisum relinquit $4pbb$, dabitur ergo quoque relinquens p, seu dabitur forma $aa - pbb$ per $4p + 1$ divisibilis.

367. Cum etiam detur forma $aa - bb$ per $4p + 1$ divisibilis, addendo $(4p + 1)\,bb$, dabitur etiam talis forma $aa + pbb$ per $4p + 1$ divisibilis, quae quidem jam inde patent, quod si quadrata per numerum primum $4p + 1$ dividantur, in residuis tam $+p$ quam $-p$ reperiantur.

368. Sit autem divisor primus $4ffp + ii$, denotante i numerum imparem, et quia tam forma $aa + bb$ quam $aa - bb$ per eum divisibilis exhiberi potest, hincque $iiaa + iibb$ et $iiaa - iibb$; inde auferendo, hinc vero addendo $(4ffp + ii)\,bb$, habebuntur formulae $iiaa - 4ffpbb$ et $iiaa + 4ffpbb$ per $4ffp + ii$ divisibiles, seu inter residua quadratorum erunt $\pm 4ffpbb$, ideoque etiam $\pm p$. Dabuntur ergo numeri tam hujus $xx + pyy$, quam hujus $xx - pyy$ formae per $4ffp + ii$ divisibiles. (*)

369. Si ergo concessis superioribus observationibus, divisor primus in quapiam harum formularum contineatur: $4rq + 1$, $4rq + \alpha$, $4rq + \beta$, $4rq + \gamma$, $4rq + \delta$, etc., ubi numeri $1, \alpha, \beta, \gamma, \delta$, etc. sunt primi ad $4r$ eoque minores, quorum tamen tantum semissis hic occurrit, tum inter residua quadratorum certe occurrit numerus r; similique modo pro residuo $-r$ tales formulae divisorum habentur, quae cum illis conveniunt, si divisor sit formae $4p + 1$, ab iis autem discrepant, si divisoris forma fuerit $4p - 1$.

(*) *Script. ad marg.* Prius manifestum; nam $\frac{xx + pyy}{4ffp + ii} =$ int. si $x = i$, $y = 2f$;

ut $xx - 2yy$ divis. sit per 41, $x = 7, 10, 13, 14, 17$
$y = 2, 3, 8, 4, 1$

ut $xx - 2yy$ divis. sit per 17,

$x =$	12, 5	11, 6	10, 7	16, 1	17, 4
$y =$	2	1	4	3	5

370. Observari etiam meretur, ex formis $4rq + 4m + 1$ semissem excludi tam pro residuo $+r$, quam $-r$, quorum divisores pro hac forma sunt communes. At ex forma $4rq + 4m - 1$ semissis valet pro residuo $+r$, alter pro residuo $-r$, et qui divisores pro altero residuo valent, pro altero excluduntur.

Caput XI.

De residuis, ex divisione cuborum per numeros primos natis.

371. Divisore primo existente $d = 2p + 1$, quod residuum relinquit cubus a^3, idem relinquent etiam hi cubi $(a + d)^3$, $(a + 2d)^3$, etc. et generaliter $(a + nd)^3$, ex quo sufficiet eos tantum cubos considerasse, quorum radices sunt ipso d minores, qui sunt:

$$1,\ 8,\ 27,\ 64,\ldots(d-4)^3,\quad (d-3)^3,\quad (d-2)^3,\quad (d-1)^3.$$

372. Sit r residuum, quod horum cuborum quicunque, a^3, relinquit, et manifestum est cubum $(d-a)^3$ relicturum residuum $-r$, seu $d - r$. Quare si inter residua cuborum occurrat numerus quicunque r, ibidem quoque occurret ejus negativum $-r$, seu $d - r$, quod illius complementum vocatur.

373. Sint 1, α, β, γ, δ, etc. residua ex divisione cuborum per numerum primum $d = 2p + 1$ orta, quorum si omnia a se invicem fuerint diversa, numerus erit $= d - 1$; ideoque omnes numeri ipso d minores ibi occurrent. Sin autem qui numeri bis vel pluries occurrant, inde quidem numeri excludentur inter non-residua referendi. (*)

374. Investigaturi, an fieri possit, ut idem numerus r inter residua bis occurrat? ponamus ex cubis a^3 et b^3, quorum radices a et b sint ipso divisore d minores et inaequales, idem residuum r resultare, atque eorum differentia $b^3 - a^3 = (b - a)(aa + ab + bb)$ per d erit divisibilis. Cum autem, ob d primum, ad eum factor $b - a$ sit primus, necesse est alterum factorem $aa + ab + bb$ esse divisibilem per d.

375. At si cubus b^3 idem praebeat residuum ac cubus a^3, cuivis alii cubo c^3 respondebit cubus e^3, idem quoque atque ille residuum relinquens. Si enim cubi a^3 et b^3 idem residuum praebeant, etiam hi a^3x^3 et b^3x^3 ad minimos valores reducendo, seu $(ax - md)^3$ et $(bx - nd)^3$ idem producent residuum. Quia vero a et d sunt numeri inter se primi, semper x et m ita accipere licet, ut $ax - md$ dato numero c aequetur, hincque erit $e = bx - nd$, diversus ab c et ipso d minor; si enim esset $e = c$, foret $ax - md = bx - nd$, hincque $(a - b)x$ divisibile per d, at nec $a - b$ nec x est divisibile.

376. Statim ergo atque unum residuum bis occurrit, omnia bis occurrent; ideoque multitudo diversorum residuorum ad semissem deprimitur. Hoc autem evenire nequit, nisi divisor d sit divisor talis formae $aa + ab + bb$, existentibus a et b ipso d minoribus. Sin autem non fuerit divisor talis formae, omnia residua erunt diversa eorumque multitudo $= d - 1 = 2p$.

377. Praebeant cubi a^3 et b^3 idem residuum r, ita ut $a^2 + ab + b^2$ sit divisibile per d, eritque etiam $3a^3 + 3a^2b + 3ab^2$ per d divisibile, auferatur $a^3 - b^3$, ut habeatur

(*) In his residuis occurrunt omnes cubi ipso d^3 minores, ad minimos valores reducti, tum etiam producta ex binis, ternis, etc.