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.

$$2a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + (a+b)^3$$

per d divisibile. Quia ergo a^3 relinquit r, relinquet cubus $(a+b)^3$ residuum $-r$, hincque cubus hic $(d-a-b)^3$, vel $(2d-a-b)^3$ dabit residuum $+r$.

387. Statim ergo ac duo habentur cubi a^3 et b^3, idem residuum r relinquentes, dabitur quoque tertius $(d-a-b)^3$, vel $(2d-a-b)^3$ idem residuum relinquens, cujus radix minor quam d ab utraque praecedentium a et b erit diversa. Neque enim esse potest $d-a-b=a$, neque $2d-a-b=a$; foret enim $b=d-2a$, vel $b=2d-2a$, ideoque b^3 relinqueret residuum $-8a^3$, vel $-8r$. Quia vero per hypothesin relinquit r, haecque duo residua r et $-8r$ aequivalentia esse nequeunt, ob differentiam $=9r$ non divisibilem per d, praeter casum $d=3$, qui per se est perspicuus, sequitur duo residua aequalia semper tertium assumere.

379. Si ergo duo cubi a^3 et b^3 idem praebeant residuum r, dabitur eo ipso tertius c^3 idem residuum exhibens, cujus radix ita est comparata, ut summa omnium $a+b+c$ sit vel $=d$, vel $=2d$, ob $c=d-a-b$, vel $c=2d-a-b$, quia singulae sunt minores quam d. Sicque ex duobus semper facile reperitur tertius.

380. Hinc autem colligere licet, infra cubum d^3 plures tribus cubis a^3, b^3, c^3 nunquam dari, qui idem residuum relinquant; si enim daretur quartus ab iis diversus e^3, etiam hi:

$$(\lambda d-a-e)^3, \quad (\lambda d-b-e)^3, \quad (\lambda d-c-e)^3,$$

idem praeberent residuum, forentque a praecedentibus diversi. Nam si esset $\lambda d-a-e=b$, foret $a+b+e$ divisibile per d, ideoque $e=c$, contra hypothesin; non solum ergo quatuor, sed adeo septem haberemus cubos idem residuum dantes.

381. Hinc autem, binis combinandis, denuo plures elici possent cubi ipso d^3 minores, idem residuum relinquentes, ita ut tandem omnes cubi essent prodituri. Cum autem concesso uno residuo r, aliud detur diversum $-r$, manifestum est non plures tribus dari cubos ipso d^3 minores, qui idem residuum exhibeant.

382. In serie ergo residuorum 1, α, β, γ, etc., quorum multitudo est $=d-1=2p$, vel omnia sunt inaequalia, vel terna inter se aequalia; quod posterius fieri nequit, nisi $2p$ sit numerus per 3 divisibilis. Quare si p non divisibile sit per 3, certum est omnia residua inter se fore inaequalia, ideoque omnes numeros ipso d minores in residuis occurrere.

383. Cum omnes numeri primi, exceptis 2 et 3, in alterutra harum formularum $6q+1$ et $6q-1$ contineantur, si divisor primus sit $6q-1$, in residuis omnes numeri ipso minores occurrunt, neque ulla dantur non-residua. Sin autem divisor sit $6q+1$, fieri potest, ut multitudo residuorum diversorum sit tantum $2q$, sicque $4q$ dentur non-residua.

384. Vidimus autem praeterea hunc ultimum casum locum habere, si divisor sit talis formae $aa+ab+bb$, unde patet, ut supra jam animadvertimus, talem formam alios divisores primos non admittere, nisi formae $6q+1$. At quadruplum illius $4aa+4ab+4bb=(2a+b)^2+3b^2$ redit ad hanc formam $aa+3bb$, cujus divisores primi illa insigni proprietate gaudent.

385. Quaerendi ergo ii sunt divisores quadratorum, qui pro residuo relinquunt -3, vel $-3bb$, qui supra observati sunt (341) in his duabus formulis $12q+1$ et $12q+7$, ad hanc unam $6q+1$

redeuntibus, contineri, unde vicissim concludere licet omnes numeros primos hujus formae $6q \pm 1$ illa proprietate praeditos esse; verum plena hujus rei demonstratio adhuc desideratur.

386. Hoc autem concesso, consequimur hanc propositionem: Quoties divisor primus fuerit formae $6q \pm 1$, toties residua cuborum ab 1 ad $216q^3$ non omnia inter se sunt inaequalia, sed ob terna aequalia, multitudo residuorum inaequalium tantum est $2q$, eruntque reliqui numeri divisore minores, quorum multitudo est $4q$, non-residua. Quoties vero divisor primus non est formae $6q \pm 1$, toties omnia residua inter se sunt inaequalia, neque ulla dantur non-residua.

387. Tantum ergo divisores primos formae $6q \pm 1$ perpendi opus est, pro quibus multitudo non-residuorum duplo major est quam multitudo residuorum. Casus autem simpliciores evolvamus:

pro divisore:	7						13										19					
residua:	1,	6					1,	8,	5,	12							1,	8,	7,	11,	12,	18
non-residua:	2,	3					2,	4,	3,	6							2,	3,	4,	5,	6,	9
	5,	4					11,	9,	10,	7							17,	16,	15,	14,	13,	10

pro divisore:	31																					
residua:	1,	8,	27,	2,	16,	15,	29,	4,	23,	30												
non-residua:	3,	5,	6,	7,	9,	10,	11,	12,	13,	14												
	28,	26,	25,	24,	22,	21,	20,	19,	18,	17												

pro divisore:	37																					
residua:	1,	8,	27,	14,	31,	10,	6,	23,	29,	11,	26,	36										
non-residua:	2,	3,	4,	5,	7,	9,	12,	13,	15,	16,	17,	18										
	35,	34,	33,	32,	30,	28,	25,	24,	22,	21,	20,	19										

pro divisore:	43																					
residua:	1,	8,	27,	21,	39,	11,	4,	32,	22,	16,	35,	2,	41,	42								
non-residua	3,	5,	6,	7,	9,	10,	12,	13,	14,	15,	17,	18,	19,	20								
	40,	38,	37,	36,	34,	33,	31,	30,	29,	28,	26,	25,	24,	23.								

388. Pro quovis ergo divisore primo formae $6q \pm 1$ in residuis occurrunt omnes cubi eo minores, deinde eorum complementa $6q$, $6q-7$, $6q-26$, $6q-63$, etc. Porro etiam producta ex binis. Tum vero etiam, si ibi sit quodpiam productum mn cum altero factore m, ibidem quoque alter factor n reperietur.

389. Si enim a^3 relinquat mn, et b^3 relinquat m, posito divisore $6q \pm 1 = d$, fieri potest $a = fb - gd$, ideoque f^3b^3 relinquet mn, at nb^3 etiam relinquit mn, sicque $f^3b^3 - nb^3$, ac propterea quoque $f^3 - n$ divisibile erit per d, seu f^3 relinquet n.

390. Si divisore primo existente $d = 6q \pm 1$, inter residua cuborum occurrat numerus α, tum $\alpha^{2q} - 1$ erit per d divisibile. Unde residua, quae ex divisione progressionis geometricae $1, \alpha, \alpha^2, \alpha^3, \alpha^4 \ldots \alpha^{2q}$ per eundem divisorem oriuntur, convenient cum residuis cuborum.

391. Vicissim autem ostendi debet si $a^{2q} - 1$ divisibile sit per divisorem primum $6q \pm 1$, numerum a certo inter residua cuborum occurrere, quod quidem si $2q$ non sit divisibile per 3, facile

patet. Si enim sit $2q = 3k \pm 1$, cum $a^{2q} = a^{3k \pm 1}$ inter residua cuborum occurrat, utpote unitati aequivalens, ibidem vero sit a^{3k}, ibidem reperiatur a necesse est.

392. Superest ergo, ut ostendatur, si sit $2q = 3k$ et $a^{3k} - 1$ dividi queat per $6q + 1 = 9k + 1$, tum a fore inter residua cuborum (*); a^{3k} ibi quidem certe reperitur utpote cubus, sed inde demonstratio peti debet, quod residuum a^{3k} unitati aequivaleat.

393. Verum cum residua potestatum $1, a, a^2, a^3$, etc. diversa, sint numero $2q$, pariter atque in residuis cuborum, et ambo ordines incipiant ab unitate et communes habeant terminos a^3, a^6, a^9, etc., tum vero reliquae proprietates ipsis sint communes, ordo potestatum nullos terminos ab altero diversos continere potest.

394. Si autem ad non-residua cuborum, per numerum primum $6q + 1$ divisorum, attendamus, id quidem certum est, si mn sit residuum, at m non-residuum, fore quoque n non-residuum. Non vero vicissim omnia producta ex binis non-residuis praebent residuum: at omnia producta ex residuo quocunque in non-residuum sunt non-residua.

395. Primo enim quadrata singulorum non-residuorum quoque inter non-residua continentur; scilicet si A sit non-residuum, quoque A^2 erit non-residuum, hoc vero non-residuum A^2 per non-residuum A multiplicatum certo dat residuum, quia est cubus.

396. Si enim A^2 esset residuum, foret $A^{4q} - 1$ divisibile per $6q + 1$; at cum $A^{6q} - 1$ certe sit divisibile, foret etiam $A^{6q} - A^{4q}$, hoc est $A^{2q} - 1$ divisibile, ideoque A esset residuum cuborum, contra hypothesin. Quare si AA sit residuum, etiam A erit residuum, et contra si A sit non-residuum, erit quoque AA non-residuum.

397. Si ergo divisore primo existente $= 6q + 1$, residua cuborum sint $1, \alpha, \beta, \gamma, \delta$, etc. atque unicum habeatur non-residuum A, primo omnes hi numeri $A, A\alpha, A\beta, A\gamma$, etc. deinde etiam isti $A^2, A^2\alpha, A^2\beta, A^2\gamma$, etc. erunt non-residua, qui numeri cum omnes a se invicem sint diversi, manifestum est, quod jam demonstravimus, multitudinem non-residuorum duplo esse majorem quam residuorum.

398. Hinc etiam patet, si divisor primus sit $6q + 1$, tantum $2q$ residua diversa locum habere posse; si enim omnes numeri inter residua occurrent, in genere $a^{2q} - 1$ esset per $6q + 1$ divisibile, quicquid esset $a < 6q + 1$, quod cum sit absurdum, ideoque unum saltem datur non-residuum, eo ipso $4q$ non-residua sequuntur.

399. Cum igitur ex unico non-residuo A obtineantur duo ordines non-residuorum, prior $A, A\alpha, A\beta, A\gamma$, etc. et posterior $A^2, A^2\alpha, A^2\beta, A^2\gamma$, etc. uterque tot continens terminos, quot ordo residuorum, producta ex binis ordinis alterutrius in altero ordine reperiuntur, et producta ex binis utriusque ordinis fiunt residua.

400. Si adhuc dubitemus, an hoc modo omnia non-residua ex uno obtineantur? sit B non-residuum in neutro ordine contentum, et non-residua erunt tam $B, B\alpha, B\beta, B\gamma$, etc. quam

(*) *Script. ad marg.* Si enim a esset non-residuum, reliqua non-residua omnia, quae sunt $a, a\alpha, a\beta, a\gamma, a\delta$, et $a^2, a^2\alpha, a^2\beta, a^2\gamma$, etc. eadem proprietate gauderent, ut eorum potestates exponentis $2q$, unitate minutae, essent divisibiles per $6q + 1$; ergo omnes numeri hanc haberent proprietatem, quod esset absurdum.

B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, etc. utrobique totidem numero, quot dantur residua, et omnes hi numeri a praecedentibus erunt diversi. Praeterea vero vel AB, vel AB^2 non erit residuum; altero certe existente residuo, altero non-residuo. (*)

401. Si AB non est residuum, binos ordines non-residuorum ita repraesentare poterimus:

Ordo prior: A, $A\alpha$, $A\beta$, $A\gamma$, etc. B, $B\alpha$, $B\beta$, $B\gamma$, etc.

Ordo posterior: A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, etc. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, etc.

et quivis numerus ordinis prioris A, per quemlibet posterioris multiplicatus, praebet residuum, et quidem per quemlibet diversum; unde plura residua prodirent, quam revera sunt, quod esset absurdum.

402. Cum ergo ex divisore primo $6q + 1$ tantum $2q$ residua existant, dato quovis cubo a^3, dabitur alius b^3, minor quam $(6q+1)^3$, quorum differentia per $6q+1$ erit divisibilis, ideoque $aa + ab + bb$ per eum quoque erit divisibilis. Omnis ergo numerus primus $6q+1$ est divisor talis numeri $aa + 3bb$, vel talis $aa + 3$, vel $3aa + 1$.

403. Speciminis loco sit divisor 373, et tam residua cuborum, quam non-residua utriusque ordinis ita se habebunt:

Residua	Non-residua	
$\pm$	Ordinis I. $\pm$	Ordinis II. $\pm$
1, 7, 8, 12, 13, 17	2, 3, 5, 14, 16, 21	4, 6, 9, 10, 11, 15
18, 19, 20, 22, 23	24, 26, 34, 35, 36	25, 28, 29, 32, 37
27, 30, 31, 33, 41	38, 39, 40, 44, 46	42, 43, 48, 52, 63
45, 49, 50, 55, 56	47, 51, 53, 54, 57	68, 70, 71, 72, 73
58, 64, 67, 74, 75	59, 60, 61, 62, 65	76, 77, 78, 79, 80
84, 86, 87, 91, 96	66, 69, 81, 82, 83	88, 92, 94, 102, 103
97, 104, 109, 111, 113	85, 89, 90, 93, 95	105, 106, 108, 114, 117
119, 125, 126, 129, 133	98, 99, 100, 101, 107	118, 120, 122, 124, 127
136, 137, 139, 140, 142	110, 112, 115, 116, 121	130, 131, 132, 138, 141
144, 145, 146, 152, 154	123, 128, 134, 135, 147	143, 149, 153, 159, 162
156, 157, 158, 160, 161	148, 150, 151, 155, 165	164, 166, 170, 171, 173
163, 167, 169, 176, 184	168, 172, 174, 179, 181	175, 177, 178, 180, 183
185.	182.	186.
numero $2.62 = 124$.	numero $= 124$.	numero $= 124$.

404. Cum igitur divisore primo existente $6q + 1$, multitudo non-residuorum duplo major sit quam multitudo residuorum, etiam pauciores erunt divisores, pro quibus datus numerus inter residua contineatur. Ita datus numerus a erit residuum, si divisor fuerit factor talis formae $x^3 \pm ay^3$, vel etiam talis $x^3 \pm aay^3$; si enim sit $x^3 \pm ay^3 = dn$, cubus x^3 per d divisus residuum dat ay^3, sicque etiam a erit in residuis.

(*) *Script. ad marg.* Demonstrari debet, ambo simul non esse posse non-residua. Si AB est non-residuum, vel in ordine A, vel B, vel A^2, vel B^2 continetur. At singula sunt absurda, ergo esset AB residuum.

405. Quaeri ergo debent numerorum $x^3 \pm ay^3$ divisores primi, et pro nostro quidem instituto ii tantum, qui simul sunt formae $6q+1$. Hoc modo posito $a=2$, binarius inter residua reperietur, quoties divisor formae $6q+1$ fuerit numerus hujus seriei:

31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997, 1021, 1051, 1069, 1093, etc.

406. Si ergo sit $6n+1$ talis numerus, tam 2 quam 2^2 erit residuum; tum $2^{2n}-1$ per eum erit divisibilis, ideoque vel 2^n-1, vel 2^n+1. At si $6n+1$ fuerit vel formae $8m+1$, vel $8m+7$, hoc est vel $n=4m$, vel $n=4m+1$, tum etiam $2^{3n}-1$ per $6n+1$ est divisibile; unde patet his casibus, quibus n vel $4m$, vel $4m+1$, fore 2^n-1 per $6n+1$ divisibile; casibus autem, quibus n est vel $4m+2$, vel $4m+3$, non 2^n-1, sed 2^n+1 per $6n+1$ divisibile erit.

407. Ita superiores numeros huc transferendo

per	divisibile est	per	divisibile est
31	$2^{10}-1$ et 2^5-1	499	$2^{166}-1$ et $3^{83}+1$
43	$2^{14}-1$ « 2^7+1	601	$2^{200}-1$ « $2^{100}-1$
109	$2^{36}-1$ « $2^{18}+1$	643	$2^{214}-1$ « $2^{107}+1$
127	$2^{42}-1$ « $2^{21}-1$	691	$2^{230}-1$ « $2^{115}+1$
157	$2^{52}-1$ « $2^{26}+1$	727	$2^{242}-1$ « $2^{121}-1$
223	$2^{74}-1$ « $2^{37}-1$	733	$2^{244}-1$ « $2^{122}-1$
229	$2^{76}-1$ « $2^{38}+1$	739	$2^{246}-1$ « $2^{123}+1$
277	$2^{92}-1$ « $2^{46}+1$	811	$2^{270}-1$ « $2^{135}+1$
283	$2^{94}-1$ « $2^{47}+1$	919	$2^{306}-1$ « $2^{153}-1$
307	$2^{102}-1$ « $2^{51}+1$	997	$2^{332}-1$ « $2^{166}+1$
397	$2^{132}-1$ « $2^{66}+1$	1021	$2^{340}-1$ « $2^{170}+1$
433	$2^{144}-1$ « $2^{72}-1$	1051	$2^{350}-1$ « $2^{175}+1$
439	$2^{146}-1$ « $2^{73}-1$	1069	$2^{356}-1$ « $2^{178}+1$
457	$2^{152}-1$ « $2^{76}-1$	1093	$2^{364}-1$ « $2^{182}+1$

408. Si hos divisores, quibus binarius pro residuo convenit, attentius perpendamus, observabimus eos omnes resultare ex hac forma $27pp+qq$, quoties ea fuerit numerus primus; verum hanc observationem demonstratione confirmare nondum licet.

409. Si eos divisores primos formae $6q+1$ quaeramus, quibus inter residua 3 conveniat, eos reperiemus:

61, 67, 73, 103, 193, 307, 367, 439, 577, 1021, etc.

qui, si conjecturae locum relinquamus, in forma $3pp+qq$ continentur, si fuerit vel $p=9n$, vel $p \pm q = 9n$.

410. Ii autem divisores primi formae $6q+1$, qui in residuis cuborum habent 5, reperiuntur ex forma $x^3 \pm 5y^3$, cujus divisores esse debent 13, 67, 127, 181, 199, 241, 487, 739, etc., quos in forma $3pp+qq$ sub his conditionibus contineri observamus: 1) si $p=15n$, 2) si $p=3m$ et $q=5n$, 3) si $p \pm q = 15n$ et 4) si $p \pm 2q = 15n$.

411. Si inter residua occurrere debeat 6, divisores reperiuntur

7, 37, 139, 163, 181, 241, 307, 337, 349, 379, 631, 727, 751, 997, etc.

qui in forma $3pp + qq$ contineri deprehenduntur, si fuerit vel $p = 9n$, vel $2p \pm q = 9n$. Harum autem observationum veritas tantum conjecturae innititur, neque inductione ulterius commode progredi licet. (*)

Caput XII.

De residuis, ex divisione biquadratorum per numeros primos ortis.

412. Si divisor primus sit d, quod residuum a biquadrato a^4 relinquitur, idem non solum a biquadratis $(d + a)^4$, $(2d + a)^4$, etc., sed etiam a $(d - a)^4$ relinquitur, unde si $d = 2p + 1$, plura quam p residua diversa resultare nequeunt.

413. Si residua sint 1, α, β, γ, δ, etc., quorum multitudo major esse nequit quam p, in iis occurrent omnia biquadrata, ad minimam scilicet formam reducta, quae insuper hac gaudebunt proprietate, ut producta ex binis in iisdem reperiantur.

414. Haec ergo residua nascuntur ex biquadratis 1, 16, 81, 256, $\ldots p^4$, quae utrum pro dato divisore primo $2p + 1$ omnia inter se futura sint diversa, nec ne? diligentius inquiri convenit.

415. Ac primo quidem patet, si unum bis occurrat, scilicet ex biquadratis a^4 et b^4, tum ob $b^4 - a^4$ per $d = 2p + 1$ divisibile, fieri poterit $b = md \pm na$, unde et $n^4a^4 - a^4$ erit divisibile, sicque etiam $n^4 - 1$. Tum ergo quoque c^4 et n^4c^4 paria producent residua, singulaque residua bis occurrent.

416. Si ergo d sit divisor formulae $b^4 - a^4$, sumtis a et b minoribus quam $\frac{1}{2}d$, ideoque formulae $b^2 + a^2$, quia neque $b - a$, neque $b + a$ per eum divisibile esse potest, tum singula residua bis occurrent. Contra vero, si non sit factor talis formae $b^2 + a^2$, omnia residua erunt diversa.

417. At per § 279 omnes divisores primi formae $bb + aa$ in forma $4q + 1$ continentur, quare si divisor propositus fuerit formae $4q - 1$, ex divisione biquadratorum certe $2q - 1$ diversa residua emergunt, totidemque habebuntur non-residua, neque plura. Quos casus primum evolvamus.

418. Sit ergo divisor primus $4q - 1$, et residua diversa ex biquadratis oriunda 1, α, β, γ, δ, etc., quorum numerus erit $2q - 1$, non-residua autem sint A, B, C, D, etc. totidem numero. Ac primo patet, si A fuerit non-residuum, etiam $A\alpha$, $A\beta$, $A\gamma$ fore non-residua. Si enim Aa^4 esset residuum, ex biquadrato b^4 ortum, foret $b^4 - Aa^4$ per d divisibile. At est $b = ma \pm nd$, unde et $m^4a^4 - Aa^4$, ideoque $m^4 - A$ esset divisibile per d, et m^4 relinqueret A, contra hypothesin.

419. Haec proprietas adeo ad omnes divisores extenditur, ita ut semper productum ex residuo in non-residuum sit non-residuum. At productum ex duobus non-residuis, AB, si quidem divisor primus sit $4q - 1$, certe est residuum; si enim esset non-residuum, conveniret cum termino Aa^4 ita ut $Aa^4 - AB$, ac propterea $a^4 - B$ per d esset divisibile, contra hypothesin.

(*) *Script. ad marg.* Ut 7 sit residuum divisorque $3pp + qq$, debet esse vel $p = 3m$ et $q = 7n$, vel $p \pm q = 21n$, vel $4p \pm q = 7n$, vel $p = 21m$, vel $p \pm 2q = 7n$. — Ut 10 sit residuum, pro divisore $3pp + qq$ debet esse vel $p = 5n$, vel $q = 5n$.