si divisor sit formae $8p+5$, quare $2^{4p}-1$ est divisibile per $8p+1$, at $2^{4p+2}-1$ non est divisibile per $8p+5$, quare cum $2^{8p+4}-1$ sit divisibile, necesse est sit $2^{4p+2}+1$ per $8p+5$ divisibile.

461. Hinc cum forma $4q+1$ ad $8p+1$ redeat, si q sit numerus par, hoc casu $2^{2q}-1$, seu 4^q-1 per $4q+1$ est divisibile, ideoque numerus 4, ejusque etiam negativum -4 inter residua biquadratorum reperiri debet. At si q sit numerus impar, quo casu $4q+1$ ad $8p+5$ redit, erit $2^{2q}+1$, seu 4^q+1, vel quod eodem redit $(-4)^q-1$ per $4q+1$ divisibile; ita ut etiam hoc casu -4 inter residua biquadratorum occurrere debeat.

462. Pro divisore ergo primo $4q+1$, sive q sit numerus par, sive impar, in residuis biquadratorum semper reperitur -4, unde cum ob 1 etiam $-4q$ adsit, quoque q adesse debet, sicque altera observatio per alteram confirmatur.

Caput XIII.

De residuis, ex divisione surdesolidorum per numeros primos ortis.

463. Si divisor sit d, et a^5 relinquat α, tum $(d-a)^5$ relinquet $-\alpha$, sicque omnia residua nascentur ex his potestatibus 1, 2^5, 3^5, $4^5 \ldots (d-1)^5$, quae si omnia fuerint diversa, eorum numerus est $= d-1$.

464. Sint 1, α, β, γ, etc. omnia residua diversa, et in iis occurrent producta ex binis; quin etiam si quod productum mn ibi adsit cum altero factore m, etiam alter n aderit. Nam si mn nascatur ex a^5, et m ex b^5, ex nb^5 nascetur etiam mn, eritque a^5-nb^5 divisibile per d. At fieri potest $a = fb \pm gd$, ideoquo a^5 idem relinquit residuum, quod f^5b^5, sic cum $f^5b^5-nb^5$, ac propterea f^5-n divisibile sit per d, in residuis erit n.

465. Si in residuis est a, ibi erunt quoque a^2, a^3, a^4, sed a^5 quidem semper inest. Hinc vicissim, si in residuis sit a^2, ibidem quoque erit $a^5 = a^5 : a^2$; et ob a^4 quoque residuum, erit etiam a residuum. Ergo quaecunque potestas a^n (dum n non fuerit multiplum quinarii) fuerit residuum, ejus omnes potestates a, a^2, a^3, etc. erunt simul residua.

466. Sit m multitudo residuorum 1, α, β, γ, δ, etc. pro divisore primo $2q+1$, et si omnes numeri divisore minores in residuis occurrant, erit $m = 2q$, ac tales quidem casus dari mox patebit.

467. Si fuerit $m < 2q$, dabitur numerus non-residuum, cujusmodi sit A, hincque primo non-residua erunt A, $A\alpha$, $A\beta$, etc. numero m; tum vero quia A^2, A^3, A^4 sunt non-residua, ex quoque m nova obtinentur, ita ut unum non-residuum A involvat quatuor classes non-residuorum

I. A, $A\alpha$, $A\beta$, $A\gamma$, etc. III. A^3, $A^3\alpha$, $A^3\beta$, $A^3\gamma$, etc.

II. A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$, etc. IV. A^4, $A^4\alpha$, $A^4\beta$, $A^4\gamma$, etc.

468. Statim ergo atque unum non-residuum habetur, simul oriuntur $4m$ non-residua, quae si fuerint omnia, necesse est ut sit $m+4m = 2q$, ideoque $5m = 2q$ et $m = \frac{2q}{5}$, nisi ergo q multiplum quinarii, non-residua adesse nequeunt.

469. At si praeter quatuor classes novum daretur non-residuum B, ex eo denuo quatuor classes orirentur:

V. B, $B\alpha$, $B\beta$, $B\gamma$, etc. VII. B^3, $B^3\alpha$, $B^3\beta$, $B^3\gamma$, etc.

VI. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$, etc. VIII. B^4, $B^4\alpha$, $B^4\beta$, $B^4\gamma$, etc.

Jam sive AB dicatur esse residuum, sive non-residuum, absurdum sequitur; unde omnia non-residua, si quidem dantur, a quatuor prioribus classibus exhauriri necesse est.

470. Certum ergo est, quoties in divisore primo $2q+1$ numerus q non fuerit multiplum quinarii, toties omnes numeros in residuis occurrere, eorumque multitudinem esse $= 2q$. Neque ergo dantur duo numeri a et b, minores quam $2q+1$, ut $a^5 - b^5$ esset per $2q+1$ divisibile; hincque etiam $a^4 + a^3b + aabb + ab^3 + b^4$ per nullum numerum primum $2q+1$ dividi potest, in quo q non sit multiplum quinarii.

471. Omnes ergo divisores primi numerorum hujus formae $a^4 + a^3b + a^2b^2 + ab^3 + b^4$, seu hujus $a^5 - b^5$, excluso divisore $a-b$, in hac formula $10p+1$ continentur, iique numeri nullo modo dividi poterunt per ullum numerum in aliqua harum formularum $10p+3$, $10p+7$ et $10p+9$ contentum.

472. At si divisor primus sit $10p+1$, non omnes numeri in ordine residuorum occurrent, si enim omnes occurrerent, foret $x^{2p} - 1$ semper divisibile per $10p+1$, quicquid fuerit x, seu differentiae omnium harum potestatum 1, 2^{2p}, 3^{2p}, 4^{2p} .... $(2p+1)^{2p}$ per $10p+1$ essent divisibiles, cujus absurditas jam supra est ostensa.

473. Quare si divisor primus sit $10p+1$, numerus residuorum diversorum tantum est $= 2p$, et $8p$ habebuntur non-residua, unde semper quini dabuntur numeri ipso $10p+1$ minores, a, b, c, d, e, quorum potestates quintae paria producunt residua.

474. Scilicet proposito numero quocunque a, quatuor semper assignari possunt alii b, c, d, e, singuli divisore $10p+1$ minores, ut per eum divisibiles sint

hi numeri	ac propterea isti quoque
$b^5 - a^5$	$b^4 + ab^3 + a^2b^2 + a^3b + a^4$
$c^5 - a^5$	$c^4 + ac^3 + a^2c^2 + a^3c + a^4$
$d^5 - a^5$	$d^4 + ad^3 + a^2d^2 + a^3d + a^4$
$e^5 - a^5$	$e^4 + ae^3 + a^2e^2 + a^3e + a^4$.

Haec eadem demonstratio ad praecedentes potestates accommodari potest.

475. Differentiae ergo etiam harum primae, a tribus sequentibus, per eumdem divisorem dividi poterunt; hae autem differentiae, cum sint divisibiles per $b-c$, $b-d$, $b-e$, abeunt in has

$$b^3 + b^2c + bc^2 + c^3 + ab^2 + abc + ac^2 + a^2b + a^2c + a^3,$$
$$b^3 + b^2d + bd^2 + d^3 + ab^2 + abd + ad^2 + a^2b + a^2d + a^3,$$
$$b^3 + b^2e + be^2 + e^3 + ab^2 + abe + ae^2 + a^2b + a^2e + a^3,$$

476. Porro vero harum differentias, sigillatim per $c-d$ et $c-e$ divisas, etiam per $10p+1$ divisibiles esse oportet, quae sunt:

*

$$c^2 + cd + d^2 + bc + bd + b^2 + ac + ad + ab + a^2,$$
$$c^2 + ce + e^2 + bc + be + b^2 + ac + ae + ab + a^2,$$

harumque denuo differentia, quae per $d - e$ divisa est,

$$e + d + c + b + a.$$

477. Hinc apparet quinos numeros a, b, c, d, e, quorum potestates quintae, per numerum primum $10p + 1$ divisae, paria relinquunt residua, ita esse comparatos, ut eorum summa

$$a + b + c + d + e$$

etiam per eundem sit divisibilis. Cum autem singuli minores sint quam $10p + 1$, eorum summa est vel $10p + 1$, vel $2(10p + 1)$, vel $3(10p + 1)$, vel $4(10p + 1)$.

478. Cum numeros negativos etiam ut residua spectare liceat, haec summa $a + b + c + d + e$ ut nihilo aequalis considerari potest, unde datis quatuor a, b, c, d, quintus sponte datur, scilicet $e = -a - b - c - d$, qui cum sit unicus, patet plures quam quinque non dari.

479. En ergo novam demonstrationem, quod numerus residuorum diversorum pro quocunque divisore primo $2q + 1$ sit vel $= 2q$, vel $= \frac{2q}{5}$, et quod prius quidem semper eveniat, si q non sit multiplum quinarii, posterius semper, si fuerit $q = 5p$. Priori casu omnes numeri divisore minores sunt residua, posteriori tantum quinta eorum pars.

480. Posito igitur divisore primo $10p + 1$, multitudo residuorum diversorum est $= 2p$, inter quae cujusvis residui negativum quoque occurrit, ex quo eorum multitudo est par. Tum vero idem residuum quinque potestatibus diversis, quarum radices sint divisore minores, convenit, quas notasse juvabit.

481. Tales divisores cum sint 11, 31, 41, 61, 71, 101, etc. consideremus primo divisorem $10p + 1 = 11$, quo fit $p = 1$:

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 3^5, 4^5, 5^5, 9^5	2	4	8	5
10	2^5, 6^5, 7^5, 8^5, 10^5	9	7	3	6.

482. Sit divisor $10p + 1 = 31$ et $p = 3$, habebimus

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 2^5, 4^5, 8^5, 16^5	2	4	8	16
5	7^5, 14^5, 19^5, 25^5, 28^5	10	20	9	18
26	3^5, 6^5, 12^5, 17^5, 24^5	21	11	22	13
6	11^5, 13^5, 21^5, 22^5, 26^5	12	24	17	3
25	5^5, 9^5, 10^5, 18^5, 20^5	19	7	14	28
30	15^5, 23^5, 27^5, 29^5, 30^5	29	27	23	15

483. Sit divisor primus $10p + 1 = 41$, ideoque $p = 4$, erunt

Residua	ex potestatibus	Classes non-residuorum I.	II.	III.	IV.
1	1^5, 10^5, 16^5, 18^5, 37^5	2	4	8	16
40	4^5, 23^5, 25^5, 31^5, 40^5	39	37	33	25
3	11^5, 12^5, 28^5, 34^5, 38^5	6	12	24	7
38	3^5, 7^5, 13^5, 29^5, 30^5	35	29	17	34
9	5^5, 8^5, 9^5, 21^5, 39^5	18	36	31	21
32	2^5, 20^5, 32^5, 33^5, 36^5	23	5	10	20
14	15^5, 22^5, 24^5, 27^5, 35^5	28	15	30	19
27	6^5, 14^5, 17^5, 19^5, 26^5	13	26	11	22

484. Sit divisor primus $10p + 1 = 61$ et $p = 6$, erunt

Residua	ex potestatibus	Classes non-residuorum I.	II.	III.	IV.
1	1^5, 9^5, 20^5, 34^5, 58^5	2	4	8	16
60	3^5, 27^5, 41^5, 52^5, 60^5	59	57	53	45
13	12^5, 25^5, 42^5, 47^5, 57^5	26	52	43	25
48	4^5, 14^5, 19^5, 36^5, 49^5	35	9	18	36
14	5^5, 39^5, 45^5, 46^5, 48^5	28	56	51	41
47	13^5, 15^5, 16^5, 22^5, 56^5	33	5	10	20
11	8^5, 11^5, 28^5, 37^5, 38^5	22	44	27	54
50	23^5, 24^5, 33^5, 50^5, 53^5	39	17	34	7
21	10^5, 17^5, 29^5, 31^5, 35^5	42	23	46	31
40	26^5, 30^5, 32^5, 44^5, 51^5	19	38	15	30
29	6^5, 21^5, 43^5, 54^5, 59^5	58	55	49	37
32	2^5, 7^5, 18^5, 40^5, 55^5	3	6	12	24

485. Proposito ergo quocunque divisore primo formae $10p+1$, dabitur numerus a, ut $a^5 - 1$ per eum sit divisibilis, quam proprietatem quoque habebunt numeri a^2, a^3, a^4, quorum potestates quintae etiam unitatem relinquunt. Sequentes termini a^5, a^6, etc. ab his non sunt diversi, cum sit $a^5 = n(10p+1)+1$, sicque a^5 ipsi 1, a^6 ipsi a, a^7 ipsi a^2 etc. aequivaleat.

486. Cum quinque numeri, quorum potestates quintae per $10p+1$ divisae unitatem relinquunt, ita repraesentari queant 1, a, a^2, a^3, a^4, si b^5 det residuum α, quinque habebuntur numeri b, ab, a^2b, a^3b, a^4b, quorum potestates quintae, per $10p+1$ divisae, idem relinquunt residuum α.

487. Quia idem ad altiores potestates extendi potest, proposito quocunque numero primo $mn+1$, semper dabitur numerus a, ut $a^m - 1$ per eum sit divisibile; ejusque potestates omnes eadem praeditae erunt proprietate. Erit autem a minor quam divisor $mn+1$, talesque numeri diversi tot, quot m continet unitates, exhiberi possunt.

488. Proposito porro divisore primo $mn+1$, si per eum potestates 1^m, 2^m, 3^m, 4^m, etc. dividantur, usque ad $(mn)^m$, plura residua diversa non relinquentur, quam n, ideoque dabuntur $(m-1)n$ numeri divisore minores, qui non sunt residua.

489. Si post unitatem a sit minimus numerus, cujus potestas a^m, per $mn+1$ divisa, unitatem relinquat, cujusmodi numerus semper datur et quidem unicus; tum si potestas b^m relinquat α, omnium horum numerorum b, ab, a^2b, $a^3b \ldots a^{m-1}b$, quorum multitudo est $=m$, potestates exponentis m idem residuum α relinquent.

490. Si $m=2$, minima potestas a^2, quae per numerum primum $2n+1$ divisa, relinquit unitatem, est ut sequitur

$2n+1$	n	a^2
3	1	2^2
5	2	4^2
7	3	6^2
11	5	10^2

et ita porro; hoc ergo casu semper est $a=2n$.

491. Si $m=3$, potestates a^3, quae per $3n+1$ divisae, unitatem relinquunt, sunt

$3n+1$	n	potestates	$3n+1$	n	potestates
7	2	1^3, 2^3, 4^3	61	20	1^3, 13^3, 47^3
13	4	1^3, 3^3, 9^3	67	22	1^3, 29^3, 37^3
19	6	1^3, 7^3, 11^3	73	24	1^3, 8^3, 64^3
31	10	1^3, 5^3, 25^3	79	26	1^3, 23^3, 55^3
37	12	1^3, 10^3, 26^3	97	32	1^3, 35^3, 61^3
43	14	1^3, 6^3, 36^3	103	34	1^3, 46^3, 56^3.

492. Sit $m=4$ et potestates a^4, quae per $4n+1$ divisae, relinquunt unitatem, sunt

$4n+1$	n	potestates	$4n+1$	n	potestates
5	1	1^4, 2^4, 4^4, 3^4	53	13	1^4, 23^4, 52^4, 30^4
13	3	1^4, 5^4, 12^4, 8^4	61	15	1^4, 11^4, 60^4, 50^4
17	4	1^4, 4^4, 16^4, 13^4	73	18	1^4, 27^4, 72^4, 46^4
29	7	1^4, 12^4, 28^4, 17^4	89	22	1^4, 34^4, 88^4, 55^4
37	9	1^4, 6^4, 36^4, 31^4	97	24	1^4, 22^4, 96^4, 75^4
41	10	1^4, 9^4, 40^4, 32^4	101	25	1^4, 10^4, 100^4, 91^4

493. Si $m=5$, potestates a^5, quae per $5n+1$ divisae, relinquunt 1, sunt, ut ante jam vidimus,

$5n+1$	n	potestates
11	2	1^5, 3^5, 9^5, 5^5, 4^5
31	6	1^5, 2^5, 4^5, 8^5, 16^5
41	8	1^5, 10^5, 18^5, 16^5, 37^5
61	12	1^5, 9^5, 20^5, 58^5, 34^5
71	14	1^5, 5^5, 25^5, 54^5, 57^5
101	20	1^5, 36^5, 84^5, 95^5, 87^5.

494. Sit $m = 6$, et senae potestates a^6, quae per $6n + 1$ divisae, unitatem relinquunt, sunt

$6n+1$	n	potestates
7	1	1^6, 2^6, 4^6, 6^6, 5^6, 3^6
13	2	1^6, 3^6, 9^6, 12^6, 10^6, 4^6
19	3	1^6, 7^6, 11^6, 18^6, 12^6, 8^6

hic scilicet eaedem potestates, quae pro casu $m = 3$ prodeunt, quibus totidem, ex radicibus negativis ortae, sunt adjiciendae.

495. Sit $m = 7$, et potestates a^7, quae per $7n + 1$ divisae, unitatem relinquunt, sunt

$7n+1$	n	potestates
29	4	1^7, 7^7, 20^7, 24^7, 23^7, 16^7, 25^7
43	6	1^7, 4^7, 16^7, 21^7, 41^7, 35^7, 11^7
71	10	1^7, 20^7, 45^7, 48^7, 37^7, 30^7, 32^7
113	16	1^7, 16^7, 30^7, 28^7, 109^7, 49^7, 106^7.

496. Jam observavimus, uno horum numerorum cognito, reliquos ex ejus potestatibus oriri. Verum methodus talem numerum investigandi haec promptissima videtur: Proposito divisore primo $mn + 1$, quaerantur duae potestates a^m et b^m idem residuum praebentes; tum quaeratur x, ut sit $x = \frac{b + p(mn+1)}{a}$, et x^m unitatem relinquet. Semper autem p ita capi potest, ut x fiat numerus integer.

497. Si divisore existente $mn + 1$, potestates exponentis m unitatem relinquentes sint

$$1^m,\ \alpha^m,\ \beta^m,\ \gamma^m,\ \delta^m,\ \text{etc. numero } m,$$

tum 1, α, β, γ, δ, etc. erunt residua ex progressione geometrica 1, α, α^2, α^3, α^4, etc. orta; erunt ergo etiam ex serie potestatum 1^n, 2^n, 3^n, 4^n, 5^n, 6^n, etc. nata.

498. En ergo methodum facillimam unum saltem numerum α inveniendi, ut $\alpha^m - 1$ per $mn + 1$ fiat divisibile, scilicet pro α semper sumi potest 2^n, seu residuum ex hac potestate binarii ortum, quin etiam valores idonei ex 3^n, 5^n, etc. peti possunt; cognito autem uno, reliqui facile innotescunt.

499. Si divisore primo existente $mn + 1$, in residuis potestatum 1, 2^n, 3^n, 4^n, etc. occurrat numerus N, ibi quoque occurret numerus Na^n; dabiturque numerus x, ut $x^n - Na^n$ per $mn + 1$ fiat divisibile, eritque etiam $N^m - 1$ per $mn + 1$ divisibile.

500. Vicissim autem, si $N^m - 1$ per $mn + 1$ est divisibile, erit N residuum potestatis cujusdam x^n; si enim esset non-residuum, omnia reliqua non-residua pari essent praedita proprietate, ideoque omnes numeri; forentque omnes hi numeri $1^m - 1$, $2^m - 1$, $3^m - 1$, etc. divisibiles per $mn + 1$, quod autem fieri nequit.

501. Posito divisore primo $mn + 1$, sint potestatum 1^m, 2^m, 3^m, 4^m, etc. residua 1, A, B, C, D, etc., potestatum vero 1^n, 2^n, 3^n, 4^n, etc. residua 1, α, β, γ, δ, etc., ac potestates omnes

$$1^m,\ \alpha^m,\ \beta^m,\ \gamma^m,\ \delta^m,\ \text{etc.}$$

residuum relinquent 1; hae vero potestates 1^n, A^n, B^n, C^n, etc. residuum relinquent 1, ideoque hae formae $\alpha^m - A^n$ erunt divisibiles per $mn + 1$.

Pagina intercalata.

Tentamen demonstrationis, quod si divisor primus sit $8q+7$, *in residuis reperiatur* 2. Ponamus esse in residuis 2, et cum ibidem sit $(2q+m)^2$, erit quoque $8qq+8mq+2mm$, hincque

$$8mq+2mm-7q \text{ et } 2mm-7m-7q \text{ et } 2mm-7m+q+7,$$

quod si nunquam fiat non-residuum, patebit propositum. At non-residua repraesentari possunt per quadrata negativa, quorum dupla etiam erunt residua per hypothesin; sit ergo

$$2mm-7m+q+7 = -2aa+8bq+7b, \text{ fietque}$$

$$q = \frac{2aa+2mm-7m+7-7b}{8b-1} \text{ et } 8q+7 = \frac{(4a)^2+(4m-7)^2}{8b-1},$$

foretque $8q+7$ divisor ipsius $(4a)^2+(4m-7)^2$, quod cum fieri nequit, sequitur ex residuo 2 nullum deduci absurdum, cujusmodi necessario resultare deberet, si 2 non esset residuum. (*)

Theorema. Si divisor $12q+11$, erit 3 residuum.

Ponamus 3 esse residuum, ac si nullum absurdum inde sequatur, pro vero erit habendum. Erit ergo -3 non-residuum, et omnia non-residua $-3aa$. At residuum est $(2q+m)^2$ et $12qq+12mq+3mm$, hincque $3mm-11q-11m$, item $3mm+q-11m+11$, quod nunquam potest esse non-residuum $-3aa$: ponatur enim

$$3mm-11m+11+q = -3aa+12bq+11b, \text{ erit}$$

$$q = \frac{3aa+3mm-11m+11-11b}{12b-1}, \text{ unde fit } 12q+11 = \frac{(6a)^2+(6m-11)^2}{12b-1},$$

quod cum sit absurdum, $3mm-11m+11+q$ nunquam inter non-residua continebitur.

Vel ita pro divisore $8q+7$.

Si 2 esset non-residuum, in genere $2mm-7m-7q \pm \alpha(8q+7)$ esset non-residuum; in genere autem residuum est $(4q+n)^2 = 16qq+8nq+nn = 8nq+nn-14q = nn-14q-7n = nn+2q-7n+14 \pm \beta(8q+7)$, omnes ergo numeri continerentur in alterutra harum formularum:

$$2mm-7m-7q \pm \alpha(8q+7)$$
$$nn-7n-14q \pm \beta(8q+7).$$

Si unicus assignari posset numerus, hic non contentus, demonstratio esset perfecta; vel si idem numerus in utraque contineretur, quod fit si, posito $m=f+g$, $n=f+2g$, fuerit $ff-2gg+7g+7q$ divisibile per $8q+7$.

(*) *Script. ad marg.* Si $2mm-7m+q+7$ ponatur $=-aa$, fit

$$8q+7 = \frac{2(2a)^2+(4m-7)^2}{8b-1},$$

nunc demonstrandum restat $2xx+yy$ nunquam divisibile esse per $8q+7$.

Nota altera, ut videtur, huc pertinens. $8xx-(2y+1)^2$ alios divisores primos non habet, nisi formae $8n-1$ et $8n+1$

$\frac{8xx-1}{7}$ int si $x = 7a \pm 1$, $\frac{8xx-1}{23}$ int. si $x = 23a \pm 7$, $\frac{8xx-1}{31}$ int. si $x = 31a \pm 2$

$\frac{8xx-1}{47}$ " " $x = 47a \pm 10$, $\frac{8xx-1}{17}$ " " $x = 17a \pm 7$, $\frac{8xx-1}{41}$ " " $x = 41a \pm 6$.