Caput XIV.

De residuis, ex divisione quadratorum per numeros compositos ortis.

502. Sint 1, α, β, γ, δ, etc. residua, quae ex divisione quadratorum per numerum primum $2p+1$ oriuntur, quorum numerus est $=p$; ac videamus primo, quaenam residua oriantur, si divisio fiat per duplum $2(2p+1)$, atque hic quidem excludamus quadrata paria; tantum enim ea quadrata, quae ad divisorem sunt prima, consideremus.

503. Multitudo autem quadratorum, quorum radices sunt divisore minores, est $=2p$, et quoniam quadrata aa et $(4p+2-a)^2$ idem relinquunt residuum, multitudo residuorum diversorum major esse nequit quam p; erit ergo vel $=p$, vel minor quam p.

504. Minor scilicet esset, si darentur duo quadrata aa et bb, ut non esset $b=4p+2-a$, quae idem relinquerent residuum. Foret autem tum $bb-aa=(b-a)(b+a)$ divisibile per $2(2p+1)$, et alter factor per 2, alter per $2p+1$ divisibilis esse deberet. At uno existente pari, alter quoque erit par, ideoque per totum divisorem divisibilis, unde foret $b=2(2p+1)-a$.

505. Multitudo ergo residuorum diversorum, quae quidem ex quadratis ad divisorem primis oriuntur, erit $=p$, totidem numero, quot ex divisore primo $2p+1$ nascuntur. Ac si residua, ex divisore $2(2p+1)$ orta, sint 1, A, B, C, D, etc., eorum numerus est $=p$, et ibidem occurrent producta ex binis.

506. Dantur autem $2p$ numeri ad hunc divisorem primi eoque minores, unde cum eorum tantum semissis residua constituat, alter semissis dabit ordinem non-residuorum, quae si sint $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc., eorum numerus erit $=p$, et producta ex horum binis iterum fient residua.

507. Contemplemur quaedam exempla, in iisque tam residua, quae ex divisore primo $2p+1$, quam ex ejus duplo $2(2p+1)$ nascuntur, simulque apponamus non-residua ad divisorem prima:

divisor	3	6	5	10	7	14
residua	1	1	1, 4,	1, 9	1, 2, 4	1, 9, 11
non-residua	2	5	2, 3,	3, 7	3, 5, 6	3, 5, 13

divisor	11	22
residua	1, 3, 9, 5, 4	1, 9, 3, 5, 15
non-residua	2, 6, 7, 8, 10	7, 13, 17, 19, 21

divisor	13	26
residua	1, 3, 4, 9, 10, 12	1, 3, 9, 17, 23, 25
non-residua	2, 5, 6, 7, 8, 11	5, 7, 11, 15, 19, 21

divisor	17	34
residua	1, 2, 4, 8, 9, 13, 15, 16	1, 9, 13, 15, 19, 21, 25, 33
non-residua	3, 5, 6, 7, 10, 11, 12, 14	3, 5, 7, 11, 23, 27, 29, 31

508. Repraesentemus rem in genere:

divisor	$2p+1$	$2(2p+1)$
residua	1, α, β, γ, δ, etc.	1, A, B, C, D, etc.
non-residua	a, b, c, d, e, etc.	$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, etc.

et primo observamus omnia residua divisoris $2(2p+1)$, vel ipsa, vel numero $2p+1$ minuta constituere residua divisoris $2p+1$.

509. Scilicet vel A, vel $A-(2p+1)$ in residuis $1, \alpha, \beta, \gamma$, etc. occurrit. Cum enim detur quadratum impar aa, ut sit $aa-A$ per $2(2p+1)$ divisibile, erit quoque per $2p+1$ divisibile, unde A etiam inter residua divisoris $2p+1$ reperiatur necesse est, vel $A-(2p+1)$, si fuerit $A>2p+1$.

510. Numeri porro impares seriei $1, \alpha, \beta, \gamma$, etc. in serie $1, A, B, C, D$, etc. occurrunt, pares autem ibi non reperiuntur, at vero iidem aucti numero $2p+1$. Sit enim α numerus impar, et cum $aa-\alpha$ sit divisibile per $2p+1$, erit $aa-\alpha=n(2p+1)$. Jam a vel est par, vel impar. Si impar, erit $aa-\alpha$ par, ac propterea etiam n par, sicque $aa-\alpha$ divisibile erit per $2(2p+1)$.

511. At si a sit par, erit $2p+1-a$ impar, atque etiam $(2p+1-a)^2-\alpha=n(2p+1)$, ubi n fiet par, ita ut haec formula quoque per $2(2p+1)$ sit divisibilis; unde si α sit numerus impar, certe inter residua $1, A, B, C$, etc. continebitur.

512. At si α sit numerus par, ejus loco inter residua divisoris $2p+1$ considerari potest $\alpha+2p+1$, qui cum sit impar, ob rationes allatas etiam inter residua divisoris $2(2p+1)$ reperiri debet.

513. Datis ergo residuis $1, \alpha, \beta, \gamma$, etc., ex divisore primo $2p+1$ ortis, ex iis statim concinnari potest series residuorum $1, A, B, C$, etc. ex duplo divisore ortorum $2(2p+1)$, illorum scilicet, quae sunt imparia, ipsa ponendo, paria autem numero $2p+1$ augendo.

514. Simili modo ex serie non-residuorum a, b, c, d, etc. divisori $2p+1$ respondentium formabitur series non-residuorum divisori $2(2p+1)$ respondentium, dum imparia ipsa sumuntur, paria vero numero $2p+1$ augentur.

De divisore $4(2p+1)=d$.

515. Multitudo numerorum hoc divisore minorum ad eumque primorum est $2.1.2p=4p$, et non solum quadrata aa et $(d-a)^2$ idem relinquunt residuum, sed dantur praeterea duo alia bb et $(d-b)^2$. Fieri enim potest $bb-aa=(b-a)(b+a)=4n(2p+1)$, sumendo $b-a=2n$ et $b+a=2(2p+1)$, unde fit $b=2(2p+1)-a$, sicque quaternorum quadratorum, idem residuum relinquentium, radices sunt: a, $2(2p+1)-a$, $2(2p+1)+a$, $4(2p+1)-a$.

516. Plura autem quam quatuor dari non possunt, unde hoc casu numerus residuorum tantum est p, uti pro divisore primo $2p+1$; at numerus non-residuorum est $3p$, ut ex subjunctis exemplis videre licet:

divisor	3	12	5	20	7	28
residua	1	1	1, 4	1, 9	1, 2, 4	1, 9, 25
non-residua	2	5 7 11	2, 3	3, 7 11, 19 13, 17	3, 5, 6	3, 27, 19 5, 17, 13 11, 15, 23

divisor	11	44
residua	1, 3, 9, 5, 4	1, 9, 25, 5, 37
non-residua	2, 6, 7, 8, 10	3, 27, 31, 15, 23 7, 19, 43, 35, 39 13, 29, 17, 21, 41
divisor	13	52
residua	1, 3, 4, 9, 10, 12	1, 9, 25, 49, 29, 17
non-residua	2, 5, 6, 7, 8, 11	3, 27, 23, 43, 35, 51 5, 45, 21, 37, 41, 33 7, 11, 19, 31, 47, 15.

517. Sint pro divisore $2p+1$ residua $1, \alpha, \beta, \gamma, \delta$, etc. et pro divisore $4(2p+1)$ residua $1, A, B, C, D$, etc. multitudine aequalia; ac primo patet ex his residuis illa reperiri, scilicet ex serie $1, A, B, C, D$, etc., quae sunt minora quam $2p+1$, ipsa in serie $1, \alpha, \beta, \gamma, \delta$, etc. continentur; quae vero sunt majora, minui debent numero $2p+1$, vel ejus duplo, vel ejus triplo.

518. Deinde observo inter residua $1, A, B, C, D$, etc. nullum numerum hujus formae $4q-1$ contineri. Cum enim quadratum aa, demto numero $4q-1$, nequeat esse divisibile per 4, fieri non potest, ut sit $aa-(4q-1)$ multiplum ipsius $4(2p+1)$, unde numeri 3, 7, 11, 15, 19, 23 semper sunt inter non-residua.

519. Si in serie $1, \alpha, \beta, \gamma, \delta$, etc. occurrat numerus impar formae $4q+1$, idem quoque in serie $1, A, B, C, D$, etc. occurret; nam si $aa-(4q+1)$ sit divisibile per $2p+1$, quoque divisibile erit $(2p+1 \pm a)^2-(4q+1)$; et quia numerorum a et $2p+1 \pm a$ alter certe est par, alter impar, sumatur a impar, et $aa-(4q+1)$ per 4 erit divisibile, unde etiam per $4(2p+1)$, ita ut pro hoc divisore $4q+1$ futurum sit residuum.

520. At si numerus impar $4q-1$ sit residuum divisoris $2p+1$, non erit residuum divisoris $4(2p+1)$, uti jam vidimus; tum vero $2(2p+1)+4q-1$, quia redit ad formam $4r+1$, certe inter residua divisoris $4(2p+1)$ continebitur.

521. Si numerus par $2q$ sit residuum divisoris $2p+1$, tum vel

$$2q+2p+1, \quad \text{vel} \quad 2q+3(2p+1)$$

erit residuum divisoris $4(2p+1)$, prout vel hic, vel ille numerus fuerit formae $4r+1$, alter enim formae $4r-1$ semper excluditur.

522. Scilicet si sit $p=2m$, et $4m+1$ numerus primus, si $4q$ sit residuum divisoris $4m+1$, tum $4q+4m+1$ erit residuum divisoris $4(4m+1)$; at si $4q+2$ residuum divisoris $4m+1$, tum $4q+2+3(4m+1)$ erit residuum divisoris $4(4m+1)$.

523. Sit $p=2m-1$ et $4m-1$ numerus primus: Si $4q$ sit residuum divisoris $4m-1$, tum $4q+3(4m-1)$ erit residuum divisoris $4(4m-1)$. At si $4q+2$ sit residuum divisoris $4m-1$, tum $4q+2+4m-1=4q+4m+1$ erit residuum divisoris $4(4m-1)$.

*

524. Ope harum regularum ex singulis residuis divisoris primi $2p+1$ totidem residua divis $4(2p+1)$ reperiuntur; unumquodque enim vel ipsum, vel auctum numero $2p+1$, vel $2(2p+$ vel $3(2p+1)$, ut prodeat numerus formae $4q+1$, erit residuum divisoris $4(2p+1)$.

525. Ex quovis autem residuo divisoris $2p+1$ unum quoque non-residuum pro divis $4(2p+1)$ elicitur, formae $4q-1$; tum vero ex quovis non-residuo divisoris $2p+1$ bina n residua pro divisore $4(2p+1)$ prodeunt; si enim illud sit par, addendo $2p+1$ et $2(2p+1)$, sit impar, addendo 0 et $2(2p+1)$ duo non-residua obtinentur.

De divisore $8(2p+1)=d$.

526. Hic semper octo dantur numeri minores quam d, quorum quadrata per d divisa relinqu idem residuum, scilicet uno numero existente a, reliqui septem sunt

$$2(2p+1)\pm a,\quad 4(2p+1)\pm a,\quad 6(2p+1)\pm a,\quad 8(2p+1)-a$$

neque plures exhiberi possunt.

527. Quare cum multitudo numerorum, ipso d minorum ad eumque primorum sit $=4.1.2p=8$ horumque octoni idem praebeant residuum, manifestum est numerum residuorum diversorum fc $=p$, non-residuorum vero $=7p$.

528. Deinde patet inter residua occurrere non posse ullum numerum formae $4q-1$, v alterutrius hujus $8q-1$, $8q-5$; neque vero etiam inter residua esse potest numerus form $8q+5$, propterea quod forma $xx-(8q+5)$ nunquam per 8 neque ergo per $8(2p+1)$ divi potest, quia est $xx=8n+1$ ob x imparem.

529. Alia igitur residua non locum habent, nisi quae sint formae $8n+1$, et quia divis est $16p+8$, pro n sumi possunt omnes numeri ab 0 usque ad $2p$. At ex forma $8n+1$ excludit vel $2p+1$, vel $3(2p+1)$, vel $5(2p+1)$, vel $7(2p+1)$, quae scilicet est formae $8n+1$, i ut tantum $2p$ hujusmodi numeri relinquantur, quorum autem semissis solum residua constituit.

530. Ex his autem numeris formae $8n+1$, quorum multitudo est $2p$, si unicus conste qui sit non-residuum, eo per singula residua multiplicando obtinentur reliqua non-residua numer p, praeterea vero reliqui numeri impares sive formae $8n+3$, sive $8n+5$, sive $8n+7$ suppedi tant adhuc $6p$ residua.

531. Divisor ergo $8(2p+1)$ totidem praebet residua, quot divisor $2p+1$, quae si sir $1, \alpha, \beta, \gamma, \delta$, etc. ex singulis residua divisoris $8(2p+1)$ elicientur, addendo ejusmodi multiplur ipsius $2p+1$, ut aggregatum fiat formae $8n+1$, veluti ex hoc exemplo videre licet:

Pro divisore 13, residua	1,	3,	4,	9,	10,	12
adde	0,	6.13,	13,	0,	3.13,	13
pro divisore 104, residua	1,	81,	17,	9,	49,	25.

532. Si pro divisore $8(2p+1)$ fuerit residuum A, erit A^p-1 divisibile per $8(2p+1)$ ac si hoc evenerit, erit A vicissim residuum quadratorum. Scilicet si A^p-1 sit divisibile pe $8(2p+1)$, semper assignari potest quadratum xx, ut sit $xx-A$ divisibile per $8(2p+1)$.

De divisore $3(2p+1)=d$.

533. Multitudo numerorum hoc divisore minorum et ad eum primorum est $=2.2p=4p$, inter quos duo ad minimum sunt, quorum quadrata idem residuum relinquunt, scilicet a^2 et $(d-a)^2$, unde numerus diversorum residuorum major quam $2p$ esse nequit.

534. Praeterea vero cum a per 3 non sit divisibile, vel $2p+1-2a$, vel $2(2p+1)-2a$ per 3 erit divisibile, sit quotus $=m$, et quadratum numeri $3m+a$ idem relinquet residuum, ergo vel $2p+1-a$, vel $2(2p+1)-a$, indeque praeterea vel $2(2p+1)+a$, vel $2p+1+a$ idem quoque residuum relinquet.

535. Hoc modo cum semper quaterna quadrata idem dent residuum, numerus residuorum diversorum erit tantum $=p$, ideoque idem ac pro divisore $2p+1$. In residuis autem nequit esse ullus numerus formae $3n-1$, cum nullum quadratum, tali numero minutum, per 3, neque ergo per $3(2p+1)$ dividi queat.

536. Omnia ergo residua divisoris $3(2p+1)$ erunt numeri formae $3n+1$, et si residua divisoris $2p+1$ sint $1, \alpha, \beta, \gamma$, etc. quodlibet vel ipsum, vel numero $2p+1$, vel $2(2p+1)$ auctum, quo prodeat numerus formae $3n+1$, erit residuum divisoris $3(2p+1)$.

Pro divisore $(2p+1)(2q+1)=d$.

537. Sint pro divisore $2p+1$ residua $1, \alpha, \beta, \gamma, \delta$, etc. numero $=p$, et pro divisore $2q+1$ residua $1, \pi, \varrho, \sigma, \tau$, etc. numero $=q$, ac numeri utrique ordini communes erunt residua divisoris $d=(2p+1)(2q+1)$.

538. At ad priorem ordinem pertinere censendus est numerus $m(2p+1)+\alpha$, ubi m ita potest definiri, ut fiat aequalis vel $n(2q+1)+1$, vel $n(2q+1)+\pi$, etc., sicque ex quovis residuo divisoris $2p+1$ producuntur q residua divisoris $2q+1$, sicque omnino pq residua diversa pro divisore $(2p+1)(2q+1)$ obtinentur.

539. Sit hujusmodi divisor compositus $5.7=35$, et cum sint residua pro divisore 5 haec duo 1, 4, et pro 7 haec tria 1, 2, 4; ergo pro divisore 35 residua erunt $7n+1$, $7n+2$, $7n+4$, quae scilicet vel in forma $5m+1$, vel $5m+4$ continentur. Erunt ergo haec residua numero sex: 1, 29; 9, 16; 4, 11.

540. Cum pro divisore $(2p+1)(2q+1)$ tantum dentur pq residua diversa, quaterna quadrata idem praebebunt residuum, quorum unum si sit $=aa$, reliquorum trium radices erunt:

$$(2p+1)(2q+1)-a, \quad m(2p+1)-a, \quad n(2p+1)+a,$$

sumendis numeris m et n ita, ut $m(2p+1)-2a$ et $n(2p+1)+2a$ dividi queant per $2q+1$, quod ob $2p+1$ et $2q+1$ primos inter se, semper fieri potest, ut m et n sint minores quam $2q+1$.

Caput XV.

De divisoribus numerorum formae $xx+yy$.

541. Hinc primo excludo casus, quibus numeri x et y habent communem divisorem; si enim maximus communis divisor esset $=\varphi$ et $x=p\varphi$ et $y=q\varphi$, ut p et q forent primi inter se, haberetur $xx+yy=(pp+qq)\varphi\varphi$, et inventio divisorum reduceretur ad formam $pp+qq$.