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, ... 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 $q=5n$.

420. Hoc ergo casu, quo divisor est $= 4q - 1$, residua biquadratorum eadem praedita sunt proprietate, atque residua quadratorum, quin etiam cum iis plane convenirent pro eodem divisore. Omnia enim residua biquadratorum in residuis quadratorum continentur, et cum multitudine sint paria, prorsus eadem sint necesse est, unde hic de residuis et non residuis eadem valent, quae supra exposuimus.

421. Sit jam divisor primus $4q + 1$, et residua 1, α, β, γ, δ, etc. omnia hanc habent proprietatem, ut $\alpha^q - 1$ divisibile sit per $4q + 1$. Haec quidem residua etiam continebuntur in residuis quadratorum pro eodem divisore $4q + 1$; at vicissim, non omnia residua quadratorum simul sunt residua biquadratorum, quod ita ostenditur.

422. Quodvis residuum quadratorum per x^2 potest repraesentari, quod si esset residuum biquadratorum, foret $x^{2q} - 1$ divisibile per $4q + 1$, denotante x numerum quemcunque minorem divisore; nempe $1^{2q} - 1$, $2^{2q} - 1$, $3^{2q} - 1$, $4^{2q} - 1, \ldots (2q)^{2q} - 1$ dividi possent per $4q + 1$, quod cum fieri nequeat, non omnia quadrata in residuis biquadratorum occurrunt.

423. Si x^2 in residuis biquadratorum non occurrat, ibidem non occurrent quoque αx^2, βx^2, γx^2, δx^2, etc., quae cum sint residua quadratorum, patet in residuis quadratorum, quorum multitudo est $2q$, tot ad minimum esse non-residua biquadratorum, quot fuerint residua biquadratorum; unde patet multitudinem residuorum biquadratorum vel esse $= q$, vel adhuc minorem, quod posterius autem fieri nequit.

424. Quo haec facilius evolvere liceat, divisores simpliciores formae $4q + 1$ examinemus, et tam residua quam non-residua biquadratorum consideremus:

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

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

425. Ex his exemplis videmus numerum residuorum esse $= q$, quem jam demonstravimus majorem esse non posse. Non-residuorum numerus triplo est major, quae in ternas classes distinximus, cum cujusvis classis numeri peculiaribus proprietatibus gaudeant.

426. Has tres classes commodissime ita constituere licet: cum dentur quadrata in residuis non occurrentia, sit xx tale quadratum; et certum est neque x, neque x^3 in residuis reperire posse. Si ergo residua sint 1, α, β, γ, δ, ε, etc. ternae non-residuorum classes erunt:

I. x, αx, βx, γx, δx, etc.

II. x^2, αx^2, βx^2, γx^2, δx^2, etc.

III. x^3, αx^3, βx^3, γx^3, δx^3, etc.

427. Quaevis classis tot continet terminos quot sunt residua, et omnes termini harum classium sunt a se invicem diversi. Ejusdem quidem classis termini manifesto sunt diversi; diversitas autem terminorum in diversis classibus ita ostendetur.

428. Si αx aequivaleret ipsi βx^2, foret $\beta x^2 - \alpha x$, ideoque $\beta x - \alpha$ per $4q+1$ divisibile, unde cum α sit residuum, βx quoque esset residuum ipsi aequivalens, quod esset absurdum. Simili modo si αx, vel αx^2 conveniret cum βx^3, foret vel $\alpha - \beta x^2$, vel $\alpha - \beta x$ divisibile per $4q+1$, ideoque βx^2, vel βx in residua transiret, contra hypothesin.

429. Hinc si numerus residuorum sit $= n$, numerus non-residuorum erit $3n$, vel saltem non erit minor quam $3n$. Ac si in tribus memoratis classibus omnia non-residua contineantur, necesse est sit multitudo tam residuorum quam non-residuorum junctim sumta $= 4q$, ideoque $n = q$.

430. His classibus ita ut fecimus dispositis, manifestum est producta ex binis non-residuis tam primae quam tertiae classis in classe secunda contineri; deinde vero producta vel ex binis terminis secundae classis, vel ex termino primae in terminum tertiae in ordinem residuorum transgredi. Productum autem ex termino primae in terminum secundae classis reperitur in tertia classi, at productum ex secunda classe in tertiam reperitur in prima.

431. Hinc intelligitur neque in prima, neque in tertia classe numerum quadratum locum habere posse, quoniam is in se ipsum ductus foret residuum. Sola ergo secunda classis continet quadrata, et quoniam residua etiam ut quadrata spectari possunt, multitudo omnium quadratorum est $= 2n$.

432. Si secunda classis cum residuis omnia quadrata complectatur, quae ut residua diversa respectu divisoris $4q+1$ spectari possunt, quorumque numerus est $= 2q$, ut in residuis quadratorum vidimus, ob $2n = 2q$, ideoque $4n = 4q$, omnes numeri ipso divisore minores habentur, neque ulla dabuntur non-residua in nostris tribus classibus non contenta, eritque $n = q$.

433. Si ergo quis dubitet, an in nostris tribus non-residuorum classibus omnes occurrant numeri, qui non sint residua, hoc dubium tolletur, si ostendamus nullum dari quadratum non-residuum, quod non in secunda classe contineatur. Si enim yy esset tale quadratum, inde statim tres novae classes non-residuorum emergerent, foretque jam numerus non-residuorum $= 6n$, ac si nunc non-residua essent completa, foret $7n = 4q$.

434. Verum quod tale quadratum yy, tres novas classes non-residuorum post se trahens, non detur, ita ostenditur: Sint tres classes ex tali quadrato oriundae et prioribus adjiciendae

IV. y, αy, βy, γy, etc. V. y^2, αy^2, βy^2, γy^2, etc. VI. y^3, αy^3, βy^3, γy^3, etc.,

quarum singulae n terminos continebunt, ac duos casus examinari oportet, alterum quo xy esset residuum, alterum quo esset non-residuum.

435. Sit xy residuum, atque omnes termini classis quartae per x multiplicati, scilicet xy, αxy, βxy, γxy, etc. numero n, erunt residua. Verum etiam omnes termini classis tertiae per x multiplicati, scilicet x^4, αx^4, βx^4, γx^4, etc. sunt residua totidem numero, atque ab illis diversa; nam si αxy et βx^4 convenirent, foret $\alpha y - \beta x^3$ divisibile per divisorem, et αy caderet in classem tertiam, contra hypothesin. Prodirent ergo $2n$ residua diversa; quod cum sit absurdum, fieri nequit ut xy sit residuum.

436. Remoto ergo casu, quo xy est residuum, ponamus xy esse non-residuum, et cum in sex classibus omnia non-residua comprehendantur, in una earum xy occurrere deberet; sive autem ponamus xy ipsi αx, sive αx^2, sive αx^3, sive αy, sive αy^2, sive αy^3 aequivalere, sequeretur absurdum, dum y vel esset residuum, vel in classem I, vel II non-residuorum caderet, vel etiam x esset residuum, vel in classem IV, vel V caderet.

437. Cum igitur sex classes non-residuorum admitti nequeant, vel tantum tres sunt constituendae, quod volumus, vel plures quam sex. Quod posterius eveniret, si nondum omnia quadrata non-residua in classe II et V occurrerent. Sit ergo zz non-residuum in neutra harum classium contentum, et ex eo resultabunt tres novae classes, singulae n terminis constantes:

VII. z, αz, βz, etc. VIII. z^2, αz^2, βz^2, etc. IX. z^3, αz^3, βz^3, etc.

438. Nunc vero, ut § 435 ostendetur, neque xy, neque xz, neque yz esse posse residuum, quia inde plura residua, quam revera sunt, sequerentur. Deinde si xy in quapiam sex primorum classium contineretur, eadem incommoda orirentur, quae ante; ex quo xy in quapiam trium postremarum classium esse deberet. Videamus ergo, num xy ipsi αz aequivalere posset.

439. At si xy ipsi αz aequivaleret, xz, quia certe est non-residuum, vel ipsi βy, vel βy^2, vel βy^3 aequivaleret; quare cum $xy - \alpha z$ et $xz - \beta y^\nu$, denotante ν vel 1, vel 2, vel 3, essent divisibilia per $4q + 1$, foret $z(xy - \alpha z) - y(xz - \beta y^\nu)$, hoc est $\beta y^{\nu+1} - \alpha z^2$ quoque divisibile, sicque αz^2 aequivaleret ipsi $\beta y^{\nu+1}$, ideoque in alia classe contineretur, quod aeque esset absurdum.

440. Sic igitur demonstratum est, si divisor primus fuerit $4q + 1$, residua diversa biquadratorum fore numero $= q$, neque plura, neque pauciora, non-residua autem tribus classibus comprehendi, quarum quaelibet constet q terminis.

441. Quare cum residua diversa ex biquadratis $1, 2^4, 3^4, 4^4, \ldots 16q^4$, quorum multitudo est $= 2q$, oriantur, bina debent esse aequalia. Hinc si a sit numerus quicunque minor quam $2q$, dabitur semper alius b, et quidem unicus pariter non major quam $2q$, ut b^4 et a^4 aequalia relinquant residua, seu ut $b^4 - a^4$ per $4q + 1$ sit divisibile.

442. Cum autem tam $b - a$ quam $b + a$ minus sit quam $4q + 1$, erit $bb + aa$ per $4q + 1$ divisibile. Hinc proposito numero primo $4q + 1$, semper summa duorum quadratorum $aa + bb$ per eum divisibilis exhiberi potest, ita ut neutra radix superet $2q$, et quidem alterum quadratum pro lubitu assumi potest.

443. Supra autem jam ostendimus summam duorum quadratorum $aa + bb$ inter se primorum, praeter binarium alios divisores primos non admittere, nisi formae $4n + 1$. Unde concludi posse videtur, omnes numeros primos formae $4q + 1$ ipsos esse summas duorum quadratorum, certe autem vel $2(4q + 1)$, vel $5(4q + 1)$, vel $13(4q + 1)$ etc. erit summa duorum quadratorum.

444. Etsi jam evictum est, plura duobus biquadratis, quorum radices $2q$ non excedant, non dari, idem residuum relinquentes, tamen hoc etiam seorsim demonstrari potest. Sint enim tres numeri a, b, c, non excedentes $2q$, ut tam $aa + bb$, quam $aa + cc$ et $bb + cc$ per $4q + 1$ essent divisibilia, atque etiam differentiae $aa - cc$, $aa - bb$, $bb - cc$ forent divisibiles. At cum neque $a - c$, neque $a + c$ per $4q + 1$ dividi possit, productum quoque $aa - cc$ dividi non poterit.

445. Nova ergo ratione demonstravimus, si divisor primus sit $4q+1$, multitudinem residuorum diversorum ex biquadratis oriundorum esse $=q$, neque minorem esse posse; unde non-residuorum multitudo erit $3q$, in ternas classes supra memoratas distinguenda.

446. Residua ergo biquadratorum, quae sint 1, α, β, γ, δ, etc. ex divisore primo $4q+1$ oriunda, hanc habent proprietatem, ut α^q-1, β^q-1, γ^q-1, etc. per eum numerum primum $4q+1$ divisionem admittant. Utrum autem omnia residua huic proprietati refragentur, nec ne? videndum est.

447. Sit xx non-residuum, et x atque x^3 pariter erunt non-residua. Jam si $(xx)^q-1$, seu $x^{2q}-1$ esset divisibile per $4q+1$, omnes termini αx^2, βx^2, γx^2, etc. eadem proprietate gauderent, qua cum per se gaudeant ipsa residua, omnia quadrata ab 1 usque ad $4qq$ eadem proprietate essent praedita.

448. Omnibus ergo numeris ab 1 usque ad $2q$ ista conveniret proprietas, ut eorum potestates exponentis $2q$, per $4q+1$ divisae, unitatem relinquerent; sicque omnes differentiae inter binos terminos hujus seriei 1, 2^{2q}, 3^{2q}, $4^{2q}\ldots(2q)^{2q}$ per $4q+1$ essent divisibiles, quod autem absurdum esse jam supra ostensum est.

449. Hisce conficitur id, quod erat propositum, scilicet si quadratum xx fuerit non-residuum, tum $x^{2q}-1$ certe non esse divisibile per $4q+1$. Multo minus autem, cum x et x^3 etiam sint non-residua, hae formulae x^q-1, vel $x^{3q}-1$ divisibiles erunt per $4q+1$, unde patet si a^q-1 divisionem admittat per $4q+1$, tum numerum a necessario inter biquadratorum residua reperiri.

450. Quando ergo potestas a^q, per numerum primum $4q+1$ divisa, unitatem relinquit, tum omnia residua, ex serie potestatum 1, a, a^2, a^3, a^4, etc. orta, in nostris residuis biquadratorum continebuntur. Et vicissim, si a non sit residuum biquadratorum, formula a^q-1 certe non erit divisibilis per $4q+1$.

451. Si q sit numerus impar, inter residua non occurret numerus -1, vel $4q$, quia $(-1)^q-1$ certe per $4q+1$ dividi nequit. Hoc ergo casu, si residua sint 1, α, β, γ, δ, etc., eorum negativa -1, $-\alpha$, $-\beta$, $-\gamma$, etc., seu $4q$, $4q+1-\alpha$, $4q+1-\beta$, $4q+1-\gamma$, etc. certe inter non-residua reperientur.

452. Hinc sequitur, si q sit numerus impar, non dari duo biquadrata a^4 et b^4, quorum summa a^4+b^4 esset per numerum $4q+1$ divisibilis. Si enim residuum ipsi a^4 conveniens esset α, alterius b^4 esset $-\alpha$, quod autem fieri non posse modo ostendimus.

453. Contra autem, si q sit numerus par, inter residua biquadratorum certe occurrit -1, si enim esset non-residuum, non esset $(-1)^q-1$ per $4q+1$ divisibile. Cum igitur sit divisibile, patet propositum, scilicet inter residua biquadratorum simul singulorum negativa, seu complementa contineri.

454. Si ergo q sit numerus par et $4q+1$ numerus primus, seu si $8q+1$ sit numerus primus, proposito quocunque biquadrato a^4, aliud dabitur b^4, ita ut eorum summa a^4+b^4 sit per $8q+1$ divisibilis. Ita dato numero a, semper inveniri potest numerus x, ut biquadratorum summa a^4+x^4 divisibilis sit per 17, vel 41, vel 73, vel 89, vel 97, etc.

455. Contra autem, nulla dabitur duorum biquadratorum summa, quae esset divisibilis per ullum numerum primum hujus seriei 5, 13, 29, 37, 53, 61, 101, etc.; multo vero minus per ullum numerum primum formae $4q-1$, quia ne summa duorum quidem quadratorum per talem numerum est divisibilis.

456. Summa ergo duorum biquadratorum inter se primorum, praeter binarium, alios divisores habere nequit, nisi qui contineantur in forma $8q+1$, ita est:

$1+2^4=17$	$2^4+3^4=97$	$4^4+5^4=881$	$7^4+8^4=73.89$
$1+3^4=2.41$	$2^4+5^4=641$	$4^4+7^4=2657$	$7^4+9^4=2.4481$
$1+4^4=257$	$2^4+7^4=2417$	$4^4+9^4=17.401$	$7^4+10^4=12401$
$1+5^4=2.313$	$2^4+9^4=6577$	$5^4+6^4=17.113$	$8^4+9^4=10657$
$1+6^4=1297$	$3^4+4^4=337$	$5^4+7^4=2.17.89$	$9^4+10^4=16511.$
$1+7^4=2.1201$	$3^4+5^4=2.353$	$5^4+8^4=4721$	
$1+8^4=17.241$	$3^4+7^4=2.17.73$	$5^4+9^4=2.3593$	
$1+9^4=2.17.193$	$3^4+8^4=4177$	$6^4+7^4=3697$	
$1+10^4=73.137$	$3^4+10^4=2.17.593$		

457. Si jam quaeratur, quibus divisoribus binarius in residuis reperiatur, id quidem in casibus evolutis § 424 nusquam evenit. At ubi 2 occurrit, ibi etiam 2α occurrit; ideoque divisor $4q+1$ factor esse debet talis numeri a^4-2b^4, seu $2b^4-a^4$; unde concluduntur hi divisores:

73, 89, 113, 233, 281, 353, 593, 617, 937, 1249, 1889, 2273, 2393, 4177,
4721, 4801, 6529, etc.,

qui numeri in forma $64pp+qq$ contenti videntur. (*)

458. Numeri autem in formula $64pp+qq$ contenti sunt:

73, 89, 113, 233, 257, 281, 337, 353, 577, 593, 601, 617, 881, 937, 1033, 1049,
1097, 1153, 1193, 1201, 1249, etc.,

ubi cum omnes praecedentes occurrant, et reliqui quaesito satisfaciant, nihil est, quod de veritate conjecturae dubitemus, et cum omnes hi numeri sint formae $8n+1$, in residuis tam -2 quam $+2$ reperietur.

459. Omnes divisores primos formae $4q+1$ usque ad 101 examinando, inter residua semper occurrit numerus q, ita ut esset q^q-1 divisibile per $4q+1$, quod si generatim esset verum, simul inter residua forent numeri q, q^2, q^3, $16q$, $81q$, $256q$, $16qq$, $81qq$, hincque -4, $q-20$, -64, $-4q$.

460. Haec observatio per supra § 389 allatam confirmatur, ubi animadvertimus numerum 2 inter residua quadratorum esse, si divisor primus sit formae $8p+1$, esse autem non-residuum,

(*) *Script. ad marg.* Ut 3 sit residuum, divisor esse debet $pp+qq$, ut sit vel $p=12m$, vel $p=3(2m+1)$ et $q=4n+2$. Ut 5 sit residuum, divisor fit $=100pp+qq$.

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 $1, \alpha, \beta, \gamma$, 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 $a^3=a^5:a^2$; 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 $1, \alpha, \beta, \gamma, \delta$, 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: