DEMONSTRATIO THEOREMATIS FERMATIANI OMNEM NVMERVM PRIMVM FORMAE $4n+1$ ESSE SVMMAM DVORVM QVADRATORVM.

AVCTORE *LEONARDO EVLERO*

§. 1.

Cum nuper eos essem contemplatus numeros, qui ex additione duorum quadratorum oriuntur, plures demonstraui proprietates, quibus tales numeri sunt praediti: neque tamen meas meditationes eo vsque perducere licuit, vt huius theorematis, quod Fermatius olim Geometris demonstrandum proposuit, veritatem solide ostendere potuissem. Tentamen tamen demonstrationis tum exposui, vnde certitudo huius theorematis multo luculentius elucet, etiamsi criteriis rigidae demonstrationis destituatur: neque dubitaui, quin iisdem vestigiis insistendo tandem demonstratio desiderata facilius obtineri possit; quod quidem ex eo tempore mihi ipsi vsu venit, ita, vt tentamen illud, si alia quaedam levis consideratio accedat, in rigidam demonstrationem abeat. Nihil quidem noui in hac re me praestitisse gloriari possum, cum ipse Fermatius iam demonstrationem huius theorematis elicuisse se profiteatur; verum, quod eam nusquam publici iuris fecit, eius iactura perinde ac plurimorum aliorum egregiorum huius viri inuentorum efficit, vt, quae nunc demum de his deperditis rebus quasi recuperamus, ea non immerito pro nouis inuentis habeantur. Cum enim nemo vnquam

tam felicifer in arcana numerorum penetrauerit, quam Fermatius, omnis opera in hac ſcientia vlterius excolenda fruſtra impendi videtur, niſi ante, quae ab hoc excellenti Viro iam fuerunt inueſtigata, quaſi de nouo in lucem protrahantur. Etſi enim poſt eum plures Viri docti in hoc ſtudiorum genere vires ſuas exercuerunt, nihil tamen plerumque ſunt conſecuti, quod cum ingenio huius Viri comparari poſſet.

§. 2. Vt autem demonſtrationem theorematis, quod hic conſidero, inſtituam, duas propoſitiones in ſubſidium vocari oportet, quarum demonſtrationem iam alibi dedi. Altera eſt, quod omnes numeri, qui ſunt diuiſores ſummae duorum quadratorum inter ſe primorum, ipſi ſint ſummae duorum quadratorum; ſic ſi a et b ſint numeri inter ſe primi, atque numeri ex iis formati $aa + bb$ diuiſor ſit d, erit quoque d ſumma duorum quadratorum: huius theorematis demonſtrationem dedi in ſcripto ante memorato, quo numeros, qui ſunt duorum quadratorum ſummae, ſum contemplatus. Altera propoſitio, qua demonſtratio ſequens indiget, ita ſe habet: ſi p ſit numerus primus, atque a et b numeri quicunque per p non diuiſibiles, erit ſemper $a^{p-1} - b^{p-1}$ per numerum primum p diuiſibilis: demonſtrationem huius rei iam dudum in Comment. Acad. Petrop. Tom. VIII dedi.

§. 3. Quodſi iam $4n + 1$ ſit numerus primus, per eum omnes numeri in hac forma $a^{4n} - b^{4n}$ contenti erunt diuiſibiles, ſiquidem neuter numerorum a et b ſeorſim per $4n + 1$ fierit diuiſibilis. Quare ſi a et b ſint numeri minores, quam $4n + 1$, (cyphra tamen

tamen excepta), numerus inde formatus $a^{4n} - b^{4n}$ sine vlla limitatione per numerum primum propositum $4n + 1$ erit diuisibilis. Cum autem $a^{4n} + b^{4n}$ sit productum horum factorum $a^{2n} + b^{2n}$ et $a^{2n} - b^{2n}$, necesse est, vt alteruter horum factorum sit per $4n + 1$ diuisibilis; fieri enim nequit, vt vel neuter, vel vterque simul diuisorem habeat $4n + 1$. Quodsi iam demonstrari posset, dari casus, quibus forma $a^{2n} + b^{2n}$ sit diuisibilis per $4n + 1$, quoniam $a^{2n} + b^{2n}$, ob exponentem $2n$ parem, est summa duorum quadratorum, quorum neutrum seorsim per $4n + 1$ diuisibile existit, inde sequeretur, hunc numerum $4n + 1$ esse summam duorum quadratorum.

§. 4. Verum summa $a^{2n} + b^{2n}$ toties erit per $4n + 1$ diuisibilis, quoties differentia $a^{2n} - b^{2n}$ per eundem numerum non est diuisibilis. Quare qui negauerit, numerum primum $4n + 1$ esse summam duorum quadratorum, is negare cogitur, vllum numerum huius formae $a^{2n} + b^{2n}$ per $4n + 1$ esse diuisibilem: eundem propterea affirmare oportet, omnes numeros in hac forma $a^{2n} - b^{2n}$ contentos per $4n + 1$ esse diuisibiles; siquidem neque a, neque b per $4n + 1$ sit diuisibile. Quamobrem mihi hic demonstrandum est, non omnes numeros in forma $a^{2n} - b^{2n}$ contentos per $4n + 1$ esse diuisibiles; hoc enim si praestitero, certum erit, dari casus, seu numeros pro a et b substituendos, quibus forma $a^{2n} - b^{2n}$ non sit per $4n + 1$ diuisibilis; illis ergo casibus altera forma $a^{2n} + b^{2n}$ necessario per $4n + 1$ erit diuisibilis: vnde cum a^{2n} et b^{2n} sint numeri quadrati, conficietur id, quod proponitur,

ſcilicet numerum $4n+1$ eſſe ſummam duorum quadratorum.

§. 5. Vt igitur demonſtrem, non omnes numeros in hac forma $a^{2n}-b^{2n}$ contentos, ſeu non omnes differentias inter binas poteſtates dignitatis $2n$ eſſe per $4n+1$ diuiſibiles, conſiderabo ſeriem harum poteſtatum ab vnitate vsque ad eam, quae a radice $4n$ formatur.

$$1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n},\ 6^{2n}\ldots\ldots\ldots\ (4n)^{2n}$$

ac iam dico, non omnes differentias inter binos terminos huius ſeriei eſſe per $4n+1$ diuiſibiles. Si enim ſingulae differentiae primae

$$2^{2n}-1;\ 3^{2n}-2^{2n};\ 4^{2n}-3^{2n};\ 5^{2n}-4^{2n};\ \ldots\ (4n)^{2n}-(4n-1)^{2n}$$

per $4n+1$ eſſent diuiſibiles, etiam differentiae huius progreſſionis, quae ſunt differentiae ſecundae illius ſeriei per $4n+1$ eſſent diuiſibiles: atque ob eandem rationem differentiae tertiae, quartae, quintae etc. omnes forent per $4n+1$ diuiſibiles; ac denique etiam differentiae ordinis $2n$, quae ſunt, vt conſtat, omnes inter ſe aequales. Differentiae autem ordinis $2n$ ſunt $= 1.2.3.4\ldots\ldots 2n$, quae ergo per numerum primum $4n+1$ non ſunt diuiſibiles, ex quo viciſſim ſequitur, ne omnes quidem differentias primas per $4n+1$ eſſe diuiſibiles.

§. 6. Quo vis huius demonſtrationis melius perſpiciatur, notandum eſt, differentiam ordinis $2n$ produci ex $2n+1$ terminis ſeriei propoſitae, qui ſi ab initio capiantur, omnes ita ſunt comparati, vt binorum quorumuis differentiae per $4n+1$ diuiſibiles eſſe debeant, ſi theorematis veritas negetur. Sin autem

plures

plures termini ad hanc differentiam vltimam constituendam concurrerent, iique vltra terminum $(4n)^{2n}$ progrederentur, quoniam differentiae a termino sequente $(4n+1)^{2n}$ ortae ad enunciata theorematis non pertinent, demonstratio nullam vim retineret. Hinc autem, quod differentia vltima, quam sumus contemplati, tantum ab $2n+1$ terminis pendet, conclusio, quam inde deduximus, omnino est legitima; indeque sequitur, dari differentias primas, veluti $a^{2n}-(a-1)^{2n}$, quae non sint per $4n+1$ diuisibiles, atque ita quidem, vt a non sit maior, quam $2n+1$. Hinc autem porro recte infertur, summam $a^{2n}+(a-1)^{2n}$, ideoque summam duorum quadratorum per $4n+1$ necessario esse diuisibilem: ideoque numerum primum $4n+1$ summam esse duorum quadratorum.

§. 7. Quoniam differentia ordinis $2n$ ab $2n+1$ terminis seriei potestatum pendet, totidem tantum ab initio captos consideremus

$1; 2^{2n}; 3^{2n}; 4^{2n}; 5^{2n}; 6^{2n} \ldots (2n)^{2n}; (2n+1)^{2n}$

vnde differentiae primae erunt: $2^{2n}-1$; $3^{2n}-2^{2n}$; $4^{2n}-3^{2n}$; $5^{2n}-4^{2n}$; $\ldots\ldots (2n+1)^{2n}-(2n)^{2n}$

cuius progressionis terminorum numerus est $= 2n$. Ex demonstratione itaque praecedente patet, non omnes terminos huius progressionis differentiarum esse per numerum primum $4n+1$ diuisibiles; neque tamen hinc intelligimus, quot et quinam sint illi termini, per $4n+1$ non diuisibiles. Ad demonstrationem enim sufficit, si vel vnicus terminus, quisquis ille sit, per $4n+1$ non sit diuisibilis. Quodsi autem casus speciales euoluamus, quibus $4n+1$ est numerus primus,

primus, ex differentiis istis, quarum numerus est $= 2n$, reperiemus, semper semissem esse per $4n+1$ diuisibilem, alterum vero semissem non diuisibilem: quae obseruatio etsi ad vim demonstrationis non spectat, tamen ad eam illustrandam non parum confert, quare aliquot casus speciales ad examen reuocasse iuuabit.

§. 8. Minimus numerus primus formae $4n+1$ est $= 5$, qui oritur, si $n = 1$; vnde duae habebuntur differentiae 2^2-1 et 3^2-2^2, quarum prior non est diuisibilis per 5, altera vero est diuisibilis. Pro reliquis casibus vtamur signo d ad eas differentias indicandas, quae sunt diuisibiles, at signo o eas notemus, quae non sunt diuisibiles, quae signa differentiis pro quouis casu, subscribamus

$4n+1$	Differentiae
13	2^6-1; 3^6-2^6; 4^6-3^6; 5^6-4^6; 6^6-5^6; 7^6-6^6;
	o o d o d d
17	2^8-1; 3^8-2^8; 4^8-3^8; 5^8-4^8; 6^8-5^8; 7^8-6^8; 8^8-7^8; 9^8-8^8
	d o o o d d o d
29	$2^{14}-1$; $3^{14}-2^{14}$; $4^{14}-3^{14}$; $5^{14}-4^{14}$; $6^{14}-5^{14}$; $7^{14}-6^{14}$; $8^{14}-7^{14}$; $9^{14}-8^{14}$;
	o d o d d d o o
	$10^{14}-9^{14}$; $11^{14}-10^{14}$; $12^{14}-11^{14}$; $13^{14}-12^{14}$; $14^{14}-13^{14}$; $15^{14}-14^{14}$
	o d d o o d

Hinc patet, terminos diuisibiles et non diuisibiles nulla certa lege contineri, etiamsi vtrique sint multitudine pares: tamen per se est perspicuum, vltimum terminum $(2n+1)^{2n}-2n^{2n}$ semper per $4n+1$ esse diuisibilem, quia factorem habet $(2n+1)^2-4nn = 4n+1$; at de reliquis nihil certi statui potest.

§. 9.

§. 9. Porro quoque ad vim demonstrationis penitius perspiciendam notari oportet, demonstrationem tum solum locum habere, si numerus $4n+1$ sit primus; prorsus vti natura theorematis postulat. Nam si $4n+1$ non esset numerus primus, neque de eo affirmari posset, quod sit summa duorum quadratorum, neque forma $a^{4n}-b^{4n}$ per eum esset necessario diuisibilis. Quin etiam vltima conclusio foret falsa, qua pronunciauimus, differentias illas ordinis $2n$, quae sunt $= 1.2.3.4.\ldots\ldots 2n$, non esse per $4n+1$ diuisibiles. Si enim $4n+1$ non esset numerus primus, sed factores haberet, qui essent minores, quam $2n$, tum vtique productum $1.2.3.4.\ldots\ldots 2n$ hos factores contineret, foretque idcirco per $4n+1$ diuisibile. At si $4n+1$ est numerus primus, tum demum affirmare licet, productum $1.2.3.4.\ldots\ldots 2n$ plane non esse per $4n+1$ diuisibile: quia hoc productum per nullos alios numeros diuidi potest, nisi qui tanquam factores in illud ingrediuntur.

§. 10. Cum denique demonstratio tradita hoc nitatur fundamento, quod seriei potestatum $1, 2^{2n}, 3^{2n}, 4^{2n}$, etc. differentiae ordinis $2n$ sint constantes, omnesque $= 1.2.3.4.\ldots\ldots 2n$, hoc vberius explicandum videtur, etsi passim in libris analyticorum solide expositum reperitur. Primum igitur notandum est, si seriei cuiuscunque terminus generalis, seu is qui exponenti indefinito x respondet, sit $= Ax^m + Bx^{m-1} + Cx^{m-2} + Dx^{m-3} + Ex^{m-4} +$ etc. hanc seriem ad gradum m referri, quia m est exponens maximae potestatis ipsius x. Deinde si hic terminus generalis a sequente $A(x+1)^m + B(x+1)^{m-1} + C(x+1)^{m-2} +$

etc. ſubtrahatur, prodibit terminus generalis ſeriei differentiarum, in quo exponens ſummae poteſtatis ipſius x erit $= m - 1$, ideoque ſeries differentiarum ad gradum inferiorem $m - 1$ pertinebit. Pari modo ex termino generali ſeriei differentiarum primarum colligetur terminus generalis ſeriei differentiarum ſecundarum, qui igitur denuo ad gradum depreſſiorem $m - 2$ pertinebit.

§. 11. Ita ſi ſeries propoſita ad gradum m referatur, ſeries differentiarum primarum, ad gradum $m - 1$ referetur; ſeries porro differentiarum ſecundarum ad gradum $m - 2$; ſeries differentiarum tertiarum ad gradum $m - 3$; ſeries differentiarum quartarum ad gradum $m - 4$; et in genere ſeries differentiarum ordinis n ad gradum $m - n$ pertinebit. Vnde ſeries differentiarum ordinis m ad gradum $m - m = 0$ perueniet, eiusque ergo terminus generalis, quia ſumma ipſius x poteſtas eſt $= x^0 = 1$, erit quantitas conſtans, ideoque omnes differentiae ordinis m inter ſe erunt aequales. Hinc ſerierum primi gradus, quarum terminus generalis eſt $= Ax + B$, iam differentiae primae ſunt inter ſe aequales: ſerierum autem ſecundi gradus, quae hoc termino generali $Ax^2 + Bx + C$ continentur, differentiae ſecundae ſunt aequales, et ita porro.

§. 12. Quodſi ergo ſeriem quamcunque poteſtatum conſideremus

$1, 2^m, 3^m, 4^m, 5^m, 6^m, 7^m, 8^m$, etc.

cuius terminus generalis eſt $= x^m$, ſeu is, qui indici x reſpondet, ſeries differentiarum ordinis m ex terminis inter ſe aequalibus conſtabit. At ſeriei differentiarum primarum terminus generalis erit $= (x + 1)^m - x^m$; qui a ſequente

ſequente $(x+2)^m-(x+1)^m$ ſubtractus dabit terminum generalem ſeriei differentiarum ſecundarum, qui erit $=(x+2)^m-2(x+1)^m+x^m$. Hinc porro ſeriei differentiarum tertiarum erit terminus generalis $=(x+3)^m-3(x+2)^m+3(x+1)^m-x^m$; ac tandem ſeriei differentiarum ordinis m concluditur terminus generalis $=(x+m)^m-m(x+m-1)^m+\frac{m(m-1)}{1.2}(x+m-2)^m-\frac{m(m-1)(m-2)}{1.2.3}(x+m-3)^m+$ etc. qui cum ſit quantitas conſtans, idem erit quicunque numerus pro x ſubſtituatur, erit ergo

vel $=m^m-m(m-1)^m+\frac{m(m-1)}{1.2}(m-2)^m-\frac{m(m-1)(m-2)}{1.2.3}(m-3)^m$ + etc.

vel $=(m+1)^m-m.m^m+\frac{m(m-1)}{1.2}(m-1)^m-\frac{m(m-1)(m-2)}{1.2.3}(m-2)^m$ + etc.

vbi in forma priori poſuimus $x=0$, in poſteriori $x=1$.

§. 13. Euoluamus iam caſus huius ſeriei ſpeciales et a poteſtatibus minimis ad altiores aſcendamus: ac poſito primo $m=1$, ſeriei 1, 2, 3, 4, 5, 6, etc. terminus generalis differentiarum primarum erit $=1^1-1.0^1=1$; vel $=2^1-1.1^1=1$. Si $m=2$, ſeriei $1; 2^2; 3^2; 4^2; 5^2$; etc. differentiae ſecundae ſunt vel $2^2-2.1^2$, vel $3^2-2.2^2+1.1^2$; at eſt $2^2-2.1^2=2(2^1-1.1^1)$, vnde hae differentiae ſecundae ſunt $=2.1$. Sit $m=3$, et ſeriei $1, 2^3, 3^3, 4^3, 5^3$, etc. differentiae tertiae erunt vel $=3^3-3.2^3+3.1^3$, vel $4^3-3.3^3+3.2^3-1.1^3$; at $3^3-3.2^3+3.1^3=3(3^2-2.2^2+1.1^2)=3.2.1$, quia ex caſu praecedente eſt $3^2-2.2^2+1.1^2=2.1$. Simili modo ſi $m=4$ ſeriei $1, 2^4, 3^4, 4^4, 5^4$,

etc. differentiae quartae erunt vel $4^4 - 4.3^4 + 6.2^4 - 4.1^4$, vel $5^4 - 4.4^4 + 6.3^4 - 4.2^4 + 1.1^4$. At est $4^4 - 4.3^4 + 6.2^4 - 4.1^4 = 4(4^3 - 3.3^3 + 3.2^3 - 1.1^3) = 4.3.2.1$.

§. 14. Quo hic progressus melius perspiciatur, sint seriei $1, 2^m, 3^m, 4^m, 5^m$ etc. differentiae ordinis $m = P$; seriei $1; 2^{m+1}; 3^{m+1}; 4^{m+1}; 5^{m+1}$ etc. differentiae ordinis $m+1 = Q$. erit $P = (m+1)^m - m.m^m + \frac{m(m-1)}{1.2}(m-1)^m - \frac{m(m-1)(m-2)}{1.2.3}(m-2)^m +$ etc. $Q = (m+1)^{m+1} - (m+1)m^{m+1} + \frac{(m+1)m}{1.2}(m-1)^{m+1} - \frac{(m+1)m(m-1)}{1.2.3}(m-1)^{m+1} +$ etc. Vbi P ex forma posteriori, at Q ex forma priori expressimus. Hic primo patet, in vtraque expressione parem esse terminorum numerum, et singulos terminos expressionis P esse ad singulos terminos expressionis Q, vti 1 ad $m+1$. Namque est

$(m+1)^m : (m+1)^{m+1} = 1 : m+1$;

$m.m^m : (m+1)m^{m+1} = 1 : m+1$;

$\frac{m(m-1)}{1.2}(m-1)^m : \frac{(m+1)m}{1.2}(m-1)^{m+1} = 1 : m+1$;

$\frac{m(m-1)(m-2)}{1.2.3}(m-2)^m : \frac{(m+1)m(m-1)}{1.2.3}(m-2)^{m+1} = 1 : m+1$;

etc.

Hanc ob rem erit $P : Q = 1 : m+1$, ideoque $Q = (m+1)P$.

§. 15. Hinc ergo patet fore

seriei	Differentias
$1; 2; 3; 4; 5;$ etc.	primas $= 1$
$1; 2^2; 3^2; 4^2; 5^2;$ etc.	secundas $= 1.2$

$1; 2^3;$

$1; 2^3; 3^3; 4^3; 5^3$; etc. tertias $= 1.2.3$
$1; 2^4; 3^4; 4^4; 5^4$; etc. quartas $= 1.2.3.4$

$1; 2^m; 3^m; 4^m; 5^m$; etc. ordinis $m = 1.2.3 \ldots m$,

ergo

$1; 2^{2n}; 3^{2n}; 4^{2n}\ 5^{2n}$; etc. ordinis $2n = 1.2.3 \ldots 2n$.

Atque ita quoque demonſtrauimus, ſeriei poteſtatum $1; 2^{2n}; 3^{2n}; 4^{2n}; 5^{2n}$ etc. differentias ordinis $2n$ non ſolum eſſe conſtantes, ſed etiam aequari producto $1.2.3 \ldots 2n$, vti in demonſtratione theorematis propoſiti aſſumſimus.

THEOREMA 1.

1. Ex ſerie quadratorum 1, 4, 9, 16, 25, etc. nulli numeri per numerum primum p ſunt diuiſibiles, niſi quorum radices ſunt per eundem numerum p diuiſibiles.

DEMONSTRATIO.

Si enim quiſpiam numerus quadratus aa fuerit per numerum primum p diuiſibilis, quia ex factoribus a et a conſtat, neceſſe eſt, vt alteruter factor per p ſit diuiſibilis, quare numerus quadratus aa per numerum primum p diuiſibilis eſſe nequit, niſi eius radix a ſit diuiſibilis per p.

COROLL. 1.

2. Numeri ergo quadrati per numerum primum p diuiſibiles nascuntur ex radicibus p, $2p$, $3p$, $4p$ etc. ſuntque ergo pp, $4pp$, $9pp$, $16pp$, etc. et reliqui numeri quadrati omnes per numerum primum p non erunt diuiſibiles.

COROLL. 2.

3. Si ergo numeri quadrati, quorum radices in hac progreſſione arithmetica p, $2p$, $3p$, $4p$, etc. non continentur, per numerum primum p diuidantur, in diuiſione ſemper reſiduum remanebit, quod erit minus, quam numerus p.

SCHOLION.

4. Cuiusmodi ſint haec reſidua, quae ex diuiſione ſingulorum quadratorum per numerum primum quemcunque p naſcuntur, in hac diſſertatione diligentius inueſtigare conſtitui. Plurima enim hic inſignia phaenomena occurrent, quorum conſideratione natura numerorum non mediocriter illuſtratur. Tam eximia autem in doctrina numerorum adhuc latent myſteria, in quibus euoluendis opera non fruſtra impendi videtur.

THEOREMA. 2.

5. Si ſeries quadratorum in infinitum continuata in membra diſpeſcatur, quorum ſingula ex p terminis conſtent, hoc modo

$$1, 4, \ldots pp \,|\, (p+1)^2 \ldots 4pp \,|\, (2p+1)^2 \ldots 9pp \,|\, (3p+1)^2 \ldots 16pp \,|\, \text{etc.}$$

tum ſi vniuscuiusque membri termini ſinguli per numerum primum p diuidantur, eadem reſidua eodemque ordine recurrent.

DEMONSTRATIO.

Singulorum enim membrorum termini primi 1, $(p+1)^2$, $(2p+1)^2$, $(3p+1)^2$; etc. ſi per p diuidantur,

dantur, idem dabunt residuum $= 1$. Similique modo termini secundi 4, $(p+2)^2$, $(2p+2)^2$, $(3p+2)^2$ etc. per p diuisi aequalia producent residua $= 4$, si quidem sit $p \succ 4$. Eodemque modo patet, terminos tertios aequalia praebere residua, itemque quartos et quintos etc. Atque in genere, si primi membri terminus quotuscunque sit nn, reliquorum membrorum termini analogi erunt $(p+n)^2$, $(2p+n)^2$, $(3p+n)^2$ etc. qui omnes per p diuisi idem relinquunt residuum, quod terminus nn. In singulis ergo membris eadem redeunt residua eodemque ordine.

COROLL. 1.

6. Si igitur nouerimus residua, quae ex terminis primi membri nascantur, simul habebimus residua, quae ex diuisione omnium reliquorum membrorum per numerum p facta oriuntur.

COROLL. 2.

7. Quia postremus cuiusque membri terminus per numerum p diuisibilis existit, residuum erit $= 0$; quemadmodum primi cuiusque membri termini residuum est $= 1$. Secundorum vero terminorum cuiusque membri residuum erit $= 4$, et tertiorum $= 9$, quartorum $= 16$ etc. si quidem sit $p \succ 4$, et $p \succ 9$, et $p \succ 16$ etc.

COROLL. 3.

8. Quamdiu enim numeri quadrati 1, 4, 9, 16, etc. minores sunt, quam numerus p, illi ipsi residua constituent.

tuent. Ex sequentibus vero quadratis numero p maioribus residua emergent alia ipso numero p minora.

SCHOLION.

9. Ex diuisionis natura constat, residua semper esse minora diuisore p, ac si forte per inaduertentiam residuum relinquatur maius, quam diuisor p, id subtrahendo p, quoties fieri potest, ad numerum ipso p minorem reducetur. Sic residuum $p + a$, et in genere $np + a$, quod forte ex diuisione per p prodierit, aequivalebit residuo a; atque cum de residuis, quae ex diuisione numerorum per p nascuntur, agitur, omnia haec residua a, $p + a$, $2p + a$, et $np + a$ pro aequivalentibus haberi possunt; omnia scilicet redeunt ad minimum a, quae reductio cum sit in promtu, eam tuto negligere poterimus, vel tanquam iam factam assumere. Ita si numeri quadrati 1, 4, 9, 16 25 etc. per numerum p diuidantur, nihil obstabit, quominus dicamus residua inde oriunda esse 1, 4, 9, 16, 25 etc. etiamsi hic numeri occurrant ipso diuisore p maiores. De cetero notandum est, hoc theorema vim suam retinere, siue diuisor p sit numerus primus, siue secus.

COROLL. 4.

10. Cum terminus vltimus pp primi membri nullum praebeat residuum, omnia residua, quae quidem ex tota serie quadratorum oriri possunt, nascentur ex his terminis 1, 4, 9, 16 . . . . $(p-1)^2$; quorum numerus est $= p - 1$.

COROLL.

COROLL. 5.

11. Plura ergo diuersa residua oriri nequeunt, quam $p-1$: quod quidem per se est manifestum. Cum enim omnia residua sint ipso diuisore p minora, omnium autem numerorum ipso p minorum numerus sit $=p-1$, etiam numerus residuorum diuersorum numerus maior esse nequit.

THEOREMA. 3.

12. Si omnes termini seriei quadratorum 1, 4, 9, 16, etc. per numerum quemcunque p diuidantur, ac residua notentur, inter haec residua non omnes numeri minores, quam p, occurrent.

DEMONSTRATIO.

Omnia enim residua, quae quidem ex diuisione omnium quadratorum per numerum p oriuntur, ex his terminis resultant:

$$1, 4, 9, 16 \ldots (p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2,$$

quorum terminorum numerus est $=p-1$: ideoque inde totidem residua proueniunt. Verum haec residua non omnia inter se sunt diuersa; nam terminus vltimus $(p-1)^2 = pp-2p+1$ per p diuisus residuum relinquit $=1$. idem scilicet, quod primus terminus 1. Simili modo terminus penultimus $(p-2)^2 = pp-4p+4$ idem praebet residuum, quod terminus secundus 4; et terminus antepenultimus $(p-3)^2$ idem dat residuum, quod terminus tertius 9. Atque

in genere terminus ordine n, qui est nn, idem dat residuum, quod terminus ordine $p-n$, qui est $(p-n)^2$. Cum igitur omnia residua, quae ex his terminis $1, 4, 9 \ldots\ldots (p-1)^2$ oriuntur, et quorum numerus est $= p-1$, non sint inter se diuersa, in iis non omnes numeri ipso p minores, quorum numerus est $= p-1$, occurrere possunt.

COROLL. 1.

13. Cum igitur bina residua semper sint aequalia, numerus diuersorum residuorum ad semissem $\frac{p-1}{2}$ redigitur, siquidem sit $p-1$ numerus par; at si $p-1$ sit numerus impar, seu p par, tum numerus diuersorum residuorum erit $= \frac{p}{2}$: hoc enim casu dabitur residuum medium, quod sui aequale non habet.

COROLL. 2.

14. Cum igitur omnium numerorum ipso p minorum numerus sit $= p-1$, patet semissem horum numerorum in residuis, locum habere: dabunturque ergo numeri, qui ex diuisione numerorum quadratorum per numerum p nunquam relinquentur, solo excepto casu, quo $p = 2$; quia $p-1 = \frac{p}{2} = 1$.

COROLL. 3.

15. Quicunque ergo praeterea sit numerus p, per quem numeri quadrati diuidantur, ex numeris ipso p minoribus, semper erunt ad minimum $\frac{p-1}{2}$, vel $\frac{p}{2}$ numeri, qui inter residua non reperiuntur. Prior casus valet, si p est numerus impar, posterior si par.

COROLL.

COROLL. 4.

16. Hinc igitur numeri ipso diuisore p minores, quorum multitudo est $= p - 1$, sponte se in duas classes discriminant, quarum altera continet numeros in residuis locum habentes; altera vero eos, qui in classe residuorum non occurrunt. Hos numeros non-residua hic appellabo.

SCHOLION.

17. Quo haec clarius percipiantur, iuuabit nonnulla exempla, in quibus residua et non-residua distinguuntur, inspexisse.

Sit	$p = 3$	$p = 4$	$p = 5$	$p = 6$
	1, 4	1, 4, 9	1, 4, 9, 16	1, 4, 9, 16, 25
residua	1, 1	1, 0, 1	1, 4, 4, 1	1, 4, 3, 4, 1
non-resid.	2	2, 3	2, 3	2, 5

Sit	$p = 7$	$p = 8$
	1, 4, 9, 16, 25, 36	1, 4, 9, 16, 25, 36, 49
Residua	1, 4, 2, 2, 4, 1	1, 4, 1, 0, 1, 4, 1
non-residua	3, 5, 6	2, 3, 5, 6, 7

Sit	$p = 9$	$p = 10$
	1, 4, 9, 16, 25, 36, 49, 64	1, 4, 9, 16, 25, 36, 49, 64, 81
Residua	1, 4, 0, 7, 7, 0, 4, 1	1, 4, 9, 6, 5, 6, 9, 4, 1
non-residua	2, 3, 5, 6, 8	2, 3, 7, 8

Sit	$p = 11$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100
Residua	1, 4, 9, 5, 3, 3, 5, 9, 4, 1
non-residua	2, 6, 7, 8, 10,

Sit	$p = 12$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121
Residua	1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1
non-residua	2, 3, 5, 6, 7, 8, 10, 11

Hinc perſpicitur, numerum non-reſiduorum interdum eſſe, vel $\frac{p-1}{3}$; vel $\frac{p-2}{2}$, prout p fuerit numerus vel par, vel impar; interdum eſſe etiam maiorem, nunquam vero eſſe minorem, omnino vti demonſtratio theorematis poſtulat.

THEOREMA. 4.

18. Vt omnia reſidua, quae ex diuiſione quadratorum per numerum quemcunque p reſultare poſſunt, inueniantur, tantum opus eſt quadrata ab vnitate vsque ad terminum $(\frac{p-1}{2})^2$, vel $(\frac{p}{2})^2$, prout p fuerit vel numerus impar, vel par, per p diuidere.

DEMONSTRATIO.

Ante iam demonſtrauimus, omnia reſidua prouenire ex diuiſione horum terminorum:

$$1, 4, 9, 16, \ldots\ldots (p-1)^2$$

deinde vero vidimus, ſeriem reſiduorum hinc natorum eſſe reciprocam, ſeu ordine retrogrado ſcriptam eandem manere. Quare reſidua omnia, quatenus inter ſe ſunt diuerſa, reperientur, ſi huius ſeriei termini tantum ad medietatem vsque capiantur, vnde ſi p ſit numerus impar, ideoque $p-1$ par, omnes numeri, qui inter reſidua occurrunt, prodibunt ex his terminis:

$$1, 4, 9, 16 \ldots\ldots (\tfrac{p-1}{2})^2$$

Sin autem p ſit numerus par, quia ſuperior progreſſio, habet terminum medium, qui retrogrediendo ſibi ipſe reſpondet, reſidua omnia ex his terminis orientur

$$1, 4, 9, 16 \ldots\ldots (\tfrac{p}{2})^2.$$

COROLL.

COROLL. 1.

19. Si igitur p sit numerus impar, puta $p = 2q+1$, omnia residua ex his tantum quadratis

$$1, 4, 9, 16 \ldots\ldots qq$$

cognoscentur. At si p sit numerus par, puta $p = 2q$, haec quadrata $1, 4, 9, 16 \ldots\ldots qq$ omnia producent residua.

COROLL. 2.

20. Si haec residua omnia inter se fuerint inaequalia, cum eorum numerus sit $= q$, casu priori, quo $p = 2q+1$, et $p-1 = 2q$, numerus non-residuorum erit $= q$. Casu posteriori, quo $= p = 2q$, et $p-1 = 2q-1$, omnium non-residuorum numerus erit $= q-1$.

COROLL. 3.

21. Si a sit numerus quicunque non maior, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$, atque residuum constet, quod ex diuisione quadrati aa per numerum p resultat, omnia quadrata in hac forma generali $(np \pm a)^2$ contenta idem praebebunt residuum. At numeri omnes omnino in forma $np \pm a$ includuntur, ita vt a non excedat vel $\frac{p-1}{2}$, vel $\frac{p}{2}$.

SCHOLION.

22. Quo indolem numerorum, qui sunt residua, facilius explorare liceat, seriem residuorum repraesentemus his litteris 1. α. β. γ. δ. ε. ζ. etc. pro diuisore

p, ita vt numerus horum terminorum sit vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, prout p sit vel numerus impar, vel par. Primo igitur patet, in hac serie 1. α. β. γ. δ. ε. etc. occurrere ordine omnes numeros quadratos 1, 4, 9, 16 etc. qui quidem sint ipso numero p minores: reliquos autem esse residua, quae in diuisione maiorum quadratorum per eundem numerum p relinquuntur. Reliquas proprietates residuorum in sequentibus theorematis indagabimus.

THEOREMA. 5.

23. Si in serie residuorum 1, α, β, γ, δ, etc. occurrat numerus quicunque r, ibidem quoque reperientur omnes potestates ipsius r^2, r^3, r^4, r^5, etc, seu residua, quae ex harum potestatum diuisione per numerum propositum p, nascuntur.

DEMONSTRATIO.

Emergat residuum r ex quadrato aa, ita vt sit $aa = mp + r$; et quadratum $a^4 = (mp + r)^2$ per p diuisum idem dabit residuum, quod oritur ex rr; atque ex quadrato $a^6 = (mp + r)^3$ idem oritur residuum, quod ex r^3; similique modo residua quadratorum a^8, a^{10}, a^{12}, etc. conuenient cum residuis terminorum r^4, r^5, r^6, etc. At residua ex omnibus quadratis quantumuis magnis oriunda iam proueniunt ex quadratis minimis 1, 4, 9, 16 . . . . . $(\frac{p-1}{2})^2$, vel $(\frac{p}{2})^2$, ideoque continentur in serie residuorum 1, α, β, γ, δ, etc. Ergo si in hac serie occurrit numerus r, ibidem quoque occurrent termini r^2, r^3, r^4, r^5, etc. seu residua, quae ex eorum diuisione per diuisorem propositum p relinquuntur.

COROLL.

COROLL. 1.

24. Quae igitur poteſtatum r^2, r^3, r^4, r^5, etc. fuerint minores, quam p, eae ipſae in ſerie reſiduorum $1, \alpha, \beta, \gamma, \delta$, etc. reperientur. At altiores poteſtates ſua reſidua, quae diuiſae per p relinquunt, ibidem introducent.

COROLL. 2.

25. Si ſit $r = 1$, quia omnes eius poteſtates ſunt $= 1$, ex iis nonniſi vnicus terminus 1 in ſerie reſiduorum $1, \alpha, \beta, \gamma, \delta$, etc. naſcitur. Neque ergo ex hoc caſu nouus terminus in ſerie reſiduorum cognoſcitur.

COROLL. 3.

26. Quia in ſerie reſiduorum plures termini non occurrunt, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, plura quoque reſidua diuerſa ex poteſtatibus r^2, r^3, r^4, r^5, etc. etiamſi in infinitum continuentur, prodire non poſſunt. Vnde infinitae harum poteſtatum per p diuiſae aequalia praebebunt reſidua.

COROLL. 4.

27. Praebeant ergo hae poteſtates r^m et r^n idem reſiduum atque earum differentia $r^m - r^n$ per numerum p erit diuiſibilis, ſeu $r^n (r^{m-n} - 1)$. Vnde ſi factor r^n ſit ad p primus, quod euenit ſi reſiduum r fuerit ad p primum, alter factor $r^{m-n} - 1$ per p erit diuiſibilis, ideoque poteſtas r^{m-n} per p diuiſa vnitatem relinquet.

COROLL.

COROLL. 5.

28. Dabitur ergo potestas r^λ, quae per p diuisa vnitatem relinquit, quae vtique in serie residuorum continetur, siquidem r sit numerus ad p primus. Tum autem potestas $r^{\lambda+1}$ dabit residuum r, potestas $r^{\lambda+2}$ residuum r^2, et $r^{\lambda+3}$ residuum r^3 etc. sicque hae potestates altiores eadem residua reproducunt, quae potestates inferiores r, r^2, r^3, etc.

COROLL. 6.

29. Cum igitur plura residua diuersa prouenire nequeant, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, patet, dari numerum λ, non maiorem, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$, ita vt potestas r^λ per p diuisa vnitatem relinquat.

SCHOLION.

30. Hinc ergo intelligitur, quomodo fieri possit, vt etiamsi potestates r^2, r^3, r^4, r^5 etc. in infinitum progrediantur, tamen ex iis residua numero finita oriantur, si per diuisorem p diuidantur. Demonstraui quidem in dissertatione superiori, si r sit numerus ad p primus, dari semper eiusmodi potestatem r^λ, quae per p diuisa vnitatem relinquat, ita vt sit $\lambda \leq p$. Nunc autem videmus, si r iam in serie residuorum ex quadratis natorum contineatur, tum exponentem λ etiam minorem fieri, quam $\frac{p}{2}$.

THEOREMA. 6.

31. Si in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. quae ex diuisione numerorum quadratorum per numerum

rum p oriuntur, occurrant numeri r et s, ibidem quoque occurret horum numerorum productum rs, vel residuum quod ex eius diuisione per numerum p enascitur.

DEMONSTRATIO.

Proueniet residuum r ex quadrato aa, et residuum s ex quadrato bb, erit $aa = mp + r$, et $bb = np + s$; hinc fiet quadratum $aabb = mnpp + msp + nrp + rs$, quod ergo per p diuisum residuum relinquet rs, vel si $rs > p$, idem relinquet residuum, quod oritur ex rs. Quare cum residuum ex quadrato $aabb$ natum in serie residuorum contineatur, ibi quoque rs, seu residuum inde ortum reperietur.

COROLL. 1.

32. In serie ergo residuorum $1, \alpha, \beta, \gamma, \delta$ etc. si occurrant duo numeri r et s, ibidem quoque occurrent nonsolum potestates r, r^2, r^3, r^4 etc. et s, s^2, s^3, s^4, etc. sed etiam producta ex binis terminis quibuscunque rs, r^2s, rs^2, r^3s, r^3s^2, rs^3 etc.

COROLL. 2.

33. Hinc igitur patet, si formula $\frac{1}{(1-r)(r-s)}$ in seriem resoluatur $1 + r + s + rr + rs + ss + r^3 + r^2s + rss + s^3 +$ etc. singulos terminos huius seriei in serie residuorum occurrere, vel etiam residua ex his terminis diuisione per p orta.

COROLL. 3.

34. Etiamsi autem horum terminorum numerus sit infinitus, tamen constat, plura ex iis residua diuersa produci non posse, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, prout p fuerit numerus vel impar, vel par.

SCHOLION.

35. Quo clarius appareat, quomodo ex his terminis numero infinitis, tamen residuorum diuersorum numerus finitus et quidem non maior, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$ oriatur, euoluamus exemplum aliquod, sitque $p = 19$, erit $\frac{p-1}{2} = 9$, vnde

ex his quadratis 1, 4, 9, 16, 25, 36, 49, 64, 81
orientur residua 1, 4, 9, 16, 6, 17, 11, 7, 5

Ex hac serie residuorum contemplemur hos duos numeros 5 et 6, ex quibus formemus primo series potestatum

5, 25, 125, 625, 3125, 15625, 78125, etc.
6, 36, 216, 1296, 7776, 46656, 279936, etc.

Ex illa serie per $p = 19$ diuisa prodeunt residua:

5, 6, 11, 17, 9, 7, 16, 4, 1,

sequens scilicet residuum semper inuenitur, si praecedens per 5 multiplicetur, et productum, si sit > 19, infra 19 deprimatur. Simili modo ex potestatibus numeri 6 haec prodibunt residua:

6, 17, 7, 4, 5, 11, 9, 16, 1.

Porro

Porro si haec singula residua per singula superiora multiplicentur, et producta infra 19 deprimantur, iidem prodeunt numeri; multiplicetur enim inferior series primo per 5, tum per 6, et 11, 17, etc. vt sequitur:

per 5:	11,	9,	16,	1,	6,	17,	7,	4,	5,
per 6:	17,	7,	4,	5,	11,	9,	16,	1,	6,
per 11:	9,	16,	1,	6,	17,	7,	4,	5,	11,
per 17:	7,	4,	5,	11,	9,	16,	1,	6,	17,
per 9:	16,	1,	6,	17,	7,	4,	5,	11,	9,
per 7:	4,	5,	11,	9,	16,	1,	6,	17,	7,
per 16:	1,	6,	17,	7,	4,	5,	11,	9,	16,
per 4:	5	11,	9,	16,	1,	6,	17,	7,	4,

Perspicitur igitur, quomodocunque hi numeri, 1, 4, 9. 16, 6, 17, 11, 7, 5 seriem residuorum constituentes, inter se per multiplicationem combinentur, siquidem diuisione per 19 facta infra 19 deprimantur; eosdem semper numeros recurrere, neque vnquam vllum numerum eorum, qui non sunt residua, nempe 2, 3, 8, 10, 12, 13, 14, 15, 18 prodire.

COROLL. 4.

36. Si ergo sit 1, α, β, γ, δ, etc. series residuorum omnium, quae ex diuisione quadratorum per numerum p resultant, in eadem serie quoque occurrent omnia producta ex binis pluribusue numerorum α, β, γ, δ, etc. Ergo si haec expressio $\frac{1}{(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\text{etc.}}$ in seriem euoluatur, omnes eius termini in serie residuorum occurrent.

THEOREMA. 7.

37. Si in serie residuorum 1, α, β, γ, δ, etc. quae ex diuisione quadratorum per numerum p prodeunt, reperiantur numeri r et rs, qui sint ad p primi, quorum ille huius est factor, tunc in eadem residuorum serie etiam numerus s continebitur.

DEMONSTRATIO.

Proueniat residuum r ex quadrato aa et rs ex bb, erit $aa = mp + r$, et $bb = np + ss$: vnde fit $bb - aas = np - mps$, ficque $bb - aas$ erit per p diuisibile. At cum r et rs sint numeri ad p primi, erunt quoque quadrata aa et bb ad p prima, vnde si haec quadrata aa et bb inter se non sint prima, per communem diuisorem quadratum ad prima reduci poterunt, ita vt $bb - aas$ maneat per p divisibile. Sint ergo b et a numeri inter se primi, atque cum etiam haec forma $(mp \pm b)^2 - aas$ sit per p diuisibilis, semper pro m eiusmodi numerus assignari potest, vt fiat $mp \pm b$ multiplum ipsius a. Sit ergo $mp \pm b = ac$, erit $aacc - aas$ per p diuisibile, quod cum sit $= aa(cc - s)$, alterque factor aa sit ad p primus, necesse est, vt alter factor $cc - s$ per p sit diuisibilis, vnde quadratum cc per p diuisum relinquet s, ex quo numerus s in serie residuorum 1, α, β, γ, δ, etc. reperietur, siquidem ibi numeri r et rs occurrant, iique sint ad p primi.

COROLL.

COROLL. 1.

38. Vt igitur veritas theorematis consistat, necesse est, vt numeri r et rs, seu r et s sint ad diuisorem p primi. Supra enim vidimus, si sit $p = 12$, in residuis reperiri numeros 4 et 0, seu 4 et 12, hinc autem, posito $r = 4$ et $rs = 12$, non sequitur numerum $s = 3$ in residuis reperiri: quia r et s non sunt numeri ad p primi: ac reuera etiam numerus s inter non-residua continetur.

COROLL. 2.

39. Sin autem diuisor p sit numerus primus, quia tum omnia residua α, $\mathfrak{B}$, γ, δ, etc. ad eum sunt prima, si in iis occurrant numeri r et rs, tum etiam certo in iis occurret numerus 5.

COROLL. 3.

40. Si inter residua occurrant numeri r et s primi ad p, quia residuo r aequiualentia censenda sunt residua $p + r$; $2p + r$, et in genere $np + r$, si fuerit $np + r = ts$, tum etiam numerus t inter residua reperietur.

SCHOLION.

41. Ne ad huius modi exceptiones, quando residua non sunt numeri ad p primi, respicere obligemur, in sequentibus ponamus diuisorem p semper esse numerum primum; et cum residua ex binario orta sint obuia,

sit diuisor p simul numerus impar, seu $p = 2q + 1$, tum ergo series residuorum formabitur ex his terminis:

$$1, 4, 9, 16, - - - - - - - qq$$

ita vt eorum numerus, quatenus inter se sunt diuersa, maior esse nequeat, quam q. Si igitur residua ex hoc diuisore primo $p = 2q + 1$ sint $1, \alpha, \mathfrak{B}, \gamma, \delta$, etc. in hac serie non solum producta ex binis pluribusue terminorum $\alpha, \mathfrak{B}, \gamma, \delta$, etc. occurrent, sed quia omnia haec residua ad p sunt prima, si inter ea occurrant r et rs, ita vt vnum per aliud sit diuisibile, tum etiam quotus inde natus s in eadem serie residuorum continebitur.

THEOREMA. 8.

42. Si ex diuisore primo $p = 2q + 1$, per quem omnes numeri quadrati diuidantur, nascatur series residuorum $1, \alpha, \mathfrak{B}, \gamma, \delta, \varepsilon$, etc. quorum numerus est $= q$, omnia haec residua inter se erunt inaequalia.

DEMONSTRATIO.

Primo patet, nullum residuum in hac serie esse posse $= 0$, cum enim nascantur ex quadratis ipso qq non maioribus, nullum horum quadratorum per numerum primum $p = 2q + 1$ est diuisibile; igitur cyphra inter residua multo minus bis occurrere poterit. Ponamus autem duo residua, quae ex quadratis aa et bb oriuntur, esse aequalia, eritque differentia horum quadratorum $aa - bb$ per diuisorem $p = 2q + 1$ diuisibilis. At cum omnia haec residua $1, \alpha, \mathfrak{B}, \gamma, \delta$, etc. ex quadratis minimis, quae

quae qq non excedunt, oriantur, quadrata illa aa et bb non ſuperabunt qq, eritque propterea neque $a > q$, neque $b > q$, neque idcirco $a + b > 2q$; vnde certo erit, $a + b < p$. Cum igitur differentia quadratorum $aa - bb$ eſſet per p diuiſibilis, ſiquidem reſidua inde nata eſſent aequalia, et p ſit numerus primus, vel ſumma $a + b$, vel differentia $a - b$ foret per p diuiſibilis; vtrumque autem, ob tam $a - b < p$, quam $a + b < p$, fieri nequit. Ergo omnia reſidua, quae ex diuiſione quadratorum $1, 4, 9, 16, \ldots . qq$ per numerum primum $p = 2q + 1$ reſultant, inter ſe ſunt inaequalia.

COROLL. 1.

43. Numerus igitur omnium reſiduorum diuerſorum, quae ex diuiſione quadratorum per numerum primum $p = 2q + 1$ oriuntur, certo eſt $= q$; ante enim oſtenſum eſt, eum non eſſe maiorem, quam q; hic autem eujcimus, eum non eſſe minorem, quam q.

COROLL. 2.

44. Cum numerus omnium numerorum ipſo diviſore $p = 2q + 1$ minorum ſit $= p - 1 = 2q$, patet, horum numerorum ſemiſſem tantum in ſerie reſiduorum $1, \alpha, \mathfrak{C}, \gamma$, etc. occurrere eamque conſtituere, alterum vero ſemiſſem, conſtituere ſeriem non-reſiduorum: ideoque ſi p ſit numerus primus, ſeriem non-reſiduorum, etiam ex q numeris conſtare.

COROLL.

COROLL. 3.

45. Si ergo x sit numerus quicunque ex serie non-residuorum diuisori p respondentium, certo affirmare possumus, quicquid sit n, nullum numerum in hac forma $np + x$ esse posse quadratum.

SCHOLION.

46. Quia nunc inuestigationes nostras tantum ad diuisores primos dirigimus, expediet tam residua, quam non-residua, quae minoribus numeris primis respondent, hic exhibere. In genere scilicet si diuisor sit p, seriem residuorum per $1, \alpha, \beta, \gamma, \delta$, etc. et seriem non-residuorum per a, b, c, d, e etc. representamus; et quo facilius coniunctim tam residua, quam non-residua, referantur, hoc modo exponemus:

$$p \left\{ \begin{matrix} 1, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta \text{ etc.} \\ a, b, c, d, e, f, g, \text{ etc.} \end{matrix} \right\}$$

duas nimirum series numerorum quouis casu scribemus, quarum superior residua, inferior non-residua continet, et vtrique diuisorem p, ad quem pertinent, praefigemus. Hoc modo residua et non-residua, quae ex diuisoribus primis simplicioribus resultant, ita indicabuntur:

$3 \left\{ \begin{matrix} 1 \\ 2 \end{matrix} \right\}$; $5 \left\{ \begin{matrix} 1, 4 \\ 2, 3 \end{matrix} \right\}$; $7 \left\{ \begin{matrix} 1, 4, 2 \\ 3, 5, 6 \end{matrix} \right\}$; $11 \left\{ \begin{matrix} 1, 4, 9, 5, 3 \\ 2, 6, 7, 8, 10 \end{matrix} \right\}$;

$13 \left\{ \begin{matrix} 1, 4, 9, 3, 12, 10 \\ 2, 5, 6, 7, 8, 11 \end{matrix} \right\}$; $17 \left\{ \begin{matrix} 1, 4, 9, 16, 8, 2, 15, 13 \\ 3, 5, 6, 7, 10, 11, 12, 14 \end{matrix} \right\}$;

$19 \left\{ \begin{matrix} 1, 4, 9, 16, 6, 17, 11, 7, 5 \\ 2, 3, 8, 10, 12, 13, 14, 15, 18 \end{matrix} \right\}$; $23 \left\{ \begin{matrix} 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 \\ 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22, \end{matrix} \right\}$;

$29 \left\{ \begin{matrix} 1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 2 \\ 2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27 \end{matrix} \right\}$;

Residua

Reſidua hic eo ordine, quo ex quadratis naſcuntur, ſunt poſita, non-reſidua autem, quia nullo ordine connectuntur, a minimis ad maiora progrediendo collocauimus. Exempla haec quoque in eum finem ſeruire poterunt, vt in iis proprietates reſiduorum ante demonſtratae examinentur.

THEOREMA 9.

47. Si ex diuiſione quadratorum per numerum primum $p = 2q + 1$ naſcatur haec ſeries reſiduorum, $1, \alpha, \beta, \gamma, \delta$, etc. haecque ſeries non-reſiduorum a, b, c, d, e, etc. atque in hac ſerie non-reſiduorum occurrat numerus r, in eadem quoque occurrent omnes hi numeri $\alpha r, \beta r, \gamma r, \delta r$, etc. vel eorum reſidua diuiſione per p relicta.

DEMONSTRATIO.

Quicunque enim horum numerorum, vt αr, vel in ſerie reſiduorum continetur, vel in ſerie non-reſiduorum. At cum α in ſerie reſiduorum contineatur, ſi αr ibidem contineretur, neceſſario quoque r in ſerie reſiduorum exiſteret. Quare cum per hypotheſin r ſit numerus ex ſerie non-reſiduorum, numerus αr non erit in ſerie reſiduorum, habebit ergo αr locum in ſerie non-reſiduorum, quod idem de numeris $\beta r, \gamma r, \delta r$, etc. valet: Quod autem demonſtrauimus de his productis βr γr, δr, etc. ſi ſint maiora, quam p, id intelligendum eſt de reſiduis, quae haec producta per p diuiſa relinquunt.

COROLL. 1.

48. Quia omnes numeri $1, \alpha, \beta, \gamma, \delta$, etc. quorum numerus est $= q$, sunt inter se diuersi; sequitur quoque, omnes hos numeros $r, \alpha r, \beta r, \gamma r, \delta r$, etc. esse inter se diuersos: vnde, si omnia residua habeantur, ex vnico non-residuo cognito reliqua omnia non-residua definiuntur.

COROLL. 2.

49. Dabit ergo series $r, \alpha r, \beta r, \gamma r, \delta r$, etc. omnia plane non-residua; continet enim q numeros diuersos, totidemque et non plura existunt non-residua, siquidem diuisor p est numerus primus.

COROLL. 3.

50. Si ergo ex serie non-residuorum quilibet alius numerus s capiatur, eius producta $\alpha s, \beta s, \gamma s$, etc. alios numeros pro residuis non praebent, nisi qui ex quouis alio r hoc modo sunt reperti.

THEOREMA 10.

51. Producta ex binis numeris seriei non-residuorum continentur in serie residuorum, siquidem haec residua nascantur ex diuisione numerorum quadratorum per quempiam numerum primum.

DEMON-

DEMONSTRATIO.

Sit enim $p = 2q + 1$ diuisor primus, atque series residuorum sit $1, \alpha, \beta, \gamma, \delta$, etc. series autem non-residuorum sit a, b, c, d, e, etc. Vidimus autem, si r sit non-residuum quodcunque, seriem non-residuorum hoc modo quoque exhiberi: $r, \alpha r, \beta r, \gamma r, \delta r$, etc. Iam productum ex duobus quibuscunque horum terminorum $\alpha\beta r^2$, constat ex duobus factoribus $\alpha\beta$ et rr, quorum vterque in serie residuorum continetur, quia omnia quadrata, ac propterea etiam rr ibi occurrunt; vnde perspicuum est, productum ex binis quibusque non-residuis in serie residuorum contineri.

COROLL. 1.

52. Vt igitur productum ex duobus residuis dat residuum, ita quoque productum ex duobus non-residuis dabit residuum. Sed productum ex residuo et non-residuo semper producit non-residuum.

COROLL. 2.

53. Hinc etiam sequitur, vti residuum per residuum diuisum dat residuum, ita quoque non-residuum per non residuum diuisum dare residuum. Verum residuum per non-residuum, vel viciſſim non-residuum per residuum diuisum praebet non-residuum.

COROLL. 3.

54. Quemadmodum bina non-residua inuicem multiplicata residuum producunt; ita terna non-residua

inuicem multiplicata praebebunt non-residuum: quaterna vero non-residua iterum residuum producunt, at quina non residuum, et sic deinceps.

DEFINITIO.

55. Complementum residui est eius defectus a diuisore, ex quo est ortum: sic si diuisor sit $= p$ et residuum $= r$, erit complementum residui $= p - r$.

COROLL. 1.

56. Quia ratione residuorum omnes hi numeri r, $p + r$, $2p + r$, et in genere $np + r$ pro iisdem habentur, quicunque numerus pro n sumatur, erit eorum complementum $= p - np - r$, vnde si sumatur $n = 1$, complementum residui r erit $= -r$.

COROLL. 2.

57. Si n sumatur $= -1$, residuum r etiam per $r - p$ exprimi potest, ita vt sit negatiuum. In diuisione enim, si quotus nimis magnus accipitur, ad residua negatiua perueniturr. Sic residuum affirmatiuum r aequialebit residuo negatiuo $r - p$.

COROLL. 3.

58. Si sit $r > \frac{1}{2}p$, tum hoc residuum negatiue exprimi poterit per $r - p$, quod erit minus, quam $\frac{1}{2}p$. Ita si expressiones negatiuae in vsum vocentur, omnia residua per numeros exhiberi poterunt, semisse diuisoris

$\frac{1}{2}p$

$\frac{1}{2}p$ non maiores. Sic pro diuisore $p = 23$ habebuntur haec residua per numeros non maiores, quam $\frac{23}{2}$ expressa: 1, 4, 9, −7, 2, −10, 3, −5, −11, 8, 6.

COROLL. 4.

59. Similique modo non-residua etiam per numeros ipso $\frac{1}{2}p$ non maiores exhiberi poterunt, eruntque pro diuisore $p = 23$ haec non-residua: 5, 7, 10, 11, −9, −8, −6, −4, −3, −2, −1. Vnde si $p = 2q + 1$, numerus tam residuorum, quam non-residuorum, erit $= q$, neque in vtraque serie occurrunt numeri maiores, quam q.

COROLL. 5.

60. Si hoc modo residua exprimantur, statim patet, vtrum cuiuspiam residui complementum in eadem serie residuorum contineatur, nec ne. Nempe si r sit residuum, erit $-r$ eius complementum, et viciſſim si $-r$ sit residuum, erit $+r$ eius complementum. Quare nisi in serie residuorum idem numerus bis occurrat, affirmatiue scilicet et negatiue, eius complementum in serie residuorum non continetur.

THEOREMA 11.

61. Si in serie residuorum 1, α, β, γ, δ, etc. quae ex diuisione quadratorum per numerum primum $p = 2q + 1$ generantur, vnius termini occurrit complementum, tum simul omnium terminorum complementa in eadem serie occurrent.

SOLUTIO.

Sit r id residuum, cuius complementum $-r$ quoque in serie $1, \alpha, \beta, \gamma, \delta$, etc. occurrat. Cum igitur $-r$ per r diuisum det -1, in eadem serie quoque numerus -1 occurret; seu valor cuiuspiam litterarum $\alpha, \beta, \gamma, \delta$, etc. erit $= -1$. Quoniam ergo in eadem serie producta ex binis terminis simul reperiuntur, ibidem occurrent termini $-\alpha, -\beta, -\gamma, -\delta$, etc. Cuiusvis ergo residui complementum simul in serie residuorum reperietur, siquidem vnici termini complementum in ea occurrat.

COROLL. 1.

62. Si ergo vnici termini r complementum $-r$ in serie residuorum contineatur, tum quilibet numerus huius seriei bis occurret, primo scilicet affirmatiue, tum vero etiam negatiue. In serie nempe residuorum $1, \alpha, \beta, \gamma, \delta$, etc. etiam continebuntur termini -1, $-\alpha, -\beta, -\gamma, -\delta$, etc.

COROLL. 2.

63. Cum igitur hoc casu in serie residuorum quilibet terminus bis occurrat, numerus omnium terminorum necessario erit par. At numerus omnium terminorum est $= q$. ergo nisi sit q numerus par, fieri nequit, vt complementa residuorum simul in serie residuorum contineantur.

COROLL.

COROLL. 3.

64. Si igitur q eſt numerus impar, puta $q = 2n + 1$, ita vt ſit $p = 4n + 3$, in ſerie reſiduorum nullus plane occurrit numerus, cuius complementum ſimul in ea ſerie contineatur. Omnia ergo complementa hoc caſu in ſeriem non reſiduorum ingredientur, eritque vtrinque terminorum numerus impar $= q = 2n + 1$.

SCHOLION.

65. Hinc ergo ſummum diſcrimen agnoſcitur, quod inter numeros primos $p = 2q + 1$ intercedit, prout q fuerit numerus par, vel impar: cum poſteriori caſu certo ſciamus, nullius reſidui complementum in reſiduorum ſerie contineri. Quodſi ergo priori caſu ponamus $q = 2n$, poſteriori $q = 2n - 1$, illo caſu erit numerus primus $p = 4n + 1$, hoc vero $p = 4n - 1$; vnde patet, omnes numeros primos, binario excepto, vel vnitate ſuperare multiplum quaternarii, vel vnitate ab eo deficere; ſicque duas obtinemus numerorum claſſes, quarum altera in forma $4n + 1$, altera in forma $4n - 1$, continetur. Prioris claſſis $4n + 1$ ſunt ergo numeri primi: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc. poſterioris vero claſſis $4n - 1$ hi: 3, 7, 11, 19, 23, 31, 43 47, 59, 67, 71, 79, 83. De numeris primis claſſis prioris Fermatius olim pronunciauit, ſingulos eſſe aggregata duorum quadratorum, cuius theorematis veritatem nuper tandem poſt plures conatus demonſtraui. De numeris autem poſterioris claſſis facile oſtenditur, nullum eorum eſſe ſummam duorum quadratorum; quin

etiam

etiam mox demonſtrabo, ne quidem ſummam duorum quadratorum $aa + bb$ exhiberi poſſe, quae ſit per eiusmodi numerum primum $p = 4n - 1$ diuiſibilis, niſi vtrumque quadratum aa et bb ſeorſim per eum diuiſibile exiſtat. De his tamen numeris Fermatius affirmauit, ſingulos vel eſſe trium, vel quatuor quadratorum aggregata; ita videmus eſſe $3 = 1 + 1 + 1$; $7 = 1 + 1 + 1 + 4$; $11 = 1 + 1 + 9$; $19 = 1 + 9 + 9$; $23 = 1 + 4 + 9 + 9$; $31 = 4 + 9 + 9 + 9 = 1 + 1 + 4 + 25$; etc. Verum nullum exiſtere huiusmodi numerum, qui non ad minimum in quatuor quadrata reſolui poſſit, etſi Fermatius eius demonſtrationem ſe inueniſſe ſit profeſſus, tamen nusquam eam publicauit, ita vt cum ipſo penitus interiiſſe videatur, neque deinceps quisquam inuentus eſt, qui hanc demonſtrationem, quae in analyſi Diophantaea et vniuerſa numerorum ſcientia maximi eſt momenti, reperire potuerit. Equidem hic demonſtrabo, quocunque propoſito numero primo formae $4n - 1$, ſemper ſummam quatuor quadratorum, quin etiam trium, exhiberi poſſe, quae per eum ſit diuiſibilis. Cum igitur etiam demonſtrari queat, productum ex duobus numeris, quorum vterque eſt ſumma quadratorum, etiam eſſe quatuor quadratorum aggregata, non procul a demonſtratione deſiderata abeſſe videmur. Tantum enim ſupereſt, vt demonſtretur, ſi ſumma quatuor quadratorum fuerit diuiſibilis per numerum, qui etiam ſit ſumma quatuor quadratorum, quotum quoque certo fore ſummam quatuor quadratorum.

THEORE-

THEOREMA 12.

67. Si omnia quadrata per numerum primum $= 4n - 1$ diuidantur, indeque oriatur series residuorum $1, \alpha, \beta, \gamma, \delta$, etc. nullius residui complementum simul in hac serie residuorum continebitur.

DEMONSTRATIO.

Omnia residua resultant ex diuisione horum quadratorum:

$1, 4, 9, 16, 25, \ldots\ldots\ldots (2n-1)^2$

residua: $1, \alpha, \beta, \gamma, \delta, \ldots\ldots\ldots \nu$

numerus ergo horum residuorum est $= 2n - 1$ ideoque impar. At si vnius residui α complementum $p - \alpha$ seu $-\alpha$ in eadem serie extaret, tum simul omnium residuorum complementa ibidem occurrere deberent, sicque cum vnumquodque residuum bis, nempe cum signo $+$ et cum signo $-$ adesset, numerus residuorum esset par. Quare cum sit impar, fieri nequit, vt vel vllici residui complementum simul in eadem residuorum serie contineatur.

COROLL. 1.

67. Si vltimus seriei residuorum terminus ponatur $= \nu$, quia oritur ex quadrato $(2n-1)^2 = 4nn - 4n + 1$ per $4n - 1$ diuiso, erit residuum $\nu = -3n + 1 = n$, sumto quoto $n - 1$. Ergo eius complementum $-n$ seu $3n - 1$ in serie residuorum non reperitur.

Numerus

Numerus ergo $-n$ seu $3n-1$ certo erit in serie non-residuorum.

COROLL. 2.

68. Cum $mp-n$ seu $m(4n-1)-n$ omnes numeros complectatur, qui per $4n-1$ diuisi residuum dant $-n$, patet nullum horum numerorum $m(4n-1)-n$ seu $4mn-m-n$ vnquam esse posse quadratum.

COROLL. 3.

69. Cum in serie residuorum occurrant numeri quadrati 1, 4, 9, 16, etc. in eadem certe non occurrent eorum complementa -1, -4, -9, -16, etc. Numeri ergo quadrati signo $-$ affecti in seriem non-residuorum ingredientur.

THEOREMA 13.

70. Non datur summa duorum quadratorum, quae sit diuisibilis per numerum primum formae $4n-1$, nisi vtrumque quadratum seorsim per eundem sit diuisibile: seu non datur summa duorum quadratorum inter se primorum per numerum primum $4n-1$ diuisibilis.

DEMONSTRATIO.

Ponamus enim summam duorum quadratorum $aa+bb$ esse per numerum primum $4n-1$ diuisibilem, neque tamen vel aa vel bb seorsim esse per $4n-1$ diuisibile. Sit ergo r residuum, quod in diuisione

sione quadrati aa per $4n-1$, relinquitur et s residuum ex diuisione quadrati bb ortum; atque tam r quam s in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. occurret. Iam summa quadratorum $aa+bb$ per $4n-1$ diuisa relinquet residuum $r+s$, quod cum per hypothesin esse debeat $=$ diuisori $4n-1$, erit $s=4n-1-r$, seu $s=-r$, ideoque s erit complementum residui r. Quare si r in serie residuorum contineatur, eius complementum s in ea certe non occurret: vnde sumto quadrato quocunque aa nullum datur aliud quadratum bb eiusmodi, vt summa $aa+bb$ fiat per numerum primum $4n-1$ diuisibilis: nisi ipsum quadratum aa per se sit diuisibile per $4n-1$, quo casu etiam bb per $4n-1$ diuisibile esse debet. Nulla ergo datur summa duorum quadratorum inter se primorum, quae sit per numerum primum $4n-1$ diuisibilis.

COROLL. 1.

71. Non ergo datur huiusmodi formae $aa+1$ numerus, qui sit per numerum primum $4n-1$ diuisibilis. Ad hoc enim opus esset, vt residuum ex quadrato aa ortum esset $=-1$, quod autem in serie residuorum non existit.

COROLL. 2.

72. Cum summa duorum quadratorum $aa+bb$ per nullum numerum primum formae $4n-1$ sit diuisibilis, etiam per nullum numerum compositum p, qui factorem primum habet formae $4n-1$, erit diui-

sibilis, si enim per hunc numerum p esset diuisibilis, etiam per eius factorem $4n-1$ diuisibilis foret.

THEOREMA 14.

73. Siue numerus $4n-1$ sit primus, siue compositus, nulla datur summa duorum quadratorum inter se primorum per eum numerum $4n-1$ diuisibilis.

DEMONSTRATIO.

Si enim numerus $4n-1$ sit primus, iam demonstrata est veritas theorematis. At si $4n-1$ non sit numerus primus, erit productum ex aliquot numeris primis, et quidem imparibus, cum ipse numerus $4n-1$ sit impar. Omnes autem numeri primi sunt vel formae $4m+1$, vel $4m-1$: sed omnes factores numeri $4n-1$ esse nequeunt formae $4m+1$, quotcunque enim numeri huius formae $4m+1$ in se inuicem multiplicentur, productum semper erit numerus formae $4n+1$, seu vnitate excedet multiplum quaternarii. Quare necesse est, vt numerus $4n-1$ vnum ad minimum habeat factorem primum formae $4m-1$, et quia per talem numerum primum nulla summa duorum quadratorum inter se primorum est diuisibilis, nulla etiam datur, quae per numerum compositum $4n-1$ esset diuisibilis.

COROLL. 1.

74. Cum nulla detur summa duorum quadratorum inter se primorum per numerum $4n-1$, siue sit primus

primus, siue compositus, diuisibilis, multo minus numerus $4n-1$ ipse erit summa duorum quadratorum. Si iam esset $4n-1 = aa+bb$, vtrumque quadratum vel bb seorsim per $4n-1$ diuisibile esse deberet, quod fieri nequit, cum vtrumque sit minus quam $4n-1$, fieri nequit.

SCHOLION.

75. Nullum numerum formae $4n-1$ esse posse summam duorum quadratorum, etiam facillime hoc modo ostenditur. Si enim numerus $4n-1$ esset summa duorum quadratorum alterum esse deberet par, alterum impar. At omnia quadrata paria sunt numeri huius formae $4f$, et omnia quadrata imparia numeri huius formae $4g+1$. Summa ergo duorum quadratorum, quorum alterum est par, alterum impar, erit numerus formae $4f+4g+1$, seu $4n+1$; ergo numerus formae $4n-1$ non potest esse summa duorum quadratorum.

COROLL. 2.

76. Nullus etiam numerus, qui factorem habet formae $4n-1$, potest esse diuisor summae duorum quadratorum inter se primorum: si enim esset diuisor, etiam eius factor $4n-1$, foret diuisor, quod fieri nequit.

COROLL. 3.

77. Multo ergo minus huiusmodi numerus, qui factorem habet $4n-1$, esse potest summa duorum quadratorum inter se primorum. Ita impossibile est, vt

ſit $m(4n-1) = aa + bb$, ſi quidem a et b ſint numeri inter ſe primi.

THEOREMA 15.

78. Nullus numerus in hac forma $4mn-m-n$ contentus, quicunque numeri pro m et n capiantur, vnquam eſſe poteſt quadratum.

DEMONSTRATIO.

Cum nullus numerus, qui factorem habet $4n-1$, eſſe queat ſumma duorum quadratorum inter ſe primorum, ſeu quae praeter vnitatem nullum habeant communem diuiſorem, ſequitur fieri non poſſe, vt ſit $(4m-1)(4n-1) = 1 + aa$. Ergo non erit $16mn - 4m - 4n = aa$: vnde ne eius quadrans quidem $4mn-m-n$ vnquam quadratum eſſe poteſt.

THEOREMA 16.

79. Si in ſerie reſiduorum $1, \alpha, \beta, \gamma, \delta$, etc. quae ex diuiſione quadratorum per numerum quemcunque p reſultant, cuiuspiam reſidui complementum in eadem ſerie reſiduorum occurrat, tum duo quadrata exhiberi poterunt, quorum ſumma ſit per eundem numerum p diuiſibilis, etiamſi neutrum ſeorſim per p ſit diuiſibile.

DEMONSTRATIO.

Praebeat quadratum aa reſiduum $= r$, quadratum autem bb reſiduum $= -r$ ſeu $p-r$, quod illius eſt comple-

complementum, ita vt r sit id residuum, cuius complementum simul in serie residuorum contineatur. Iam manifestum est, summam horum quadratorum $aa + bb$ fore per numerum p diuisibilem.

COROLL. 1.

80. Si p sit numerus primus, statim atque vnius residui complementum in serie residuorum occurrit, etiam singulorum residuorum complementa ibidem inerunt. Sumto ergo quadrato quocunque aa, cuius residuum sit $= r$, dabitur aliud xx, cuius residuum erit $= -r$, ita vt x sit non maius, quam $\frac{p}{2}$, atque summa $aa + xx$ erit per p diuisibilis.

COROLL. 2.

81. Si igitur detur summa duorum quadratorum $aa + bb$ per numerum primum p diuisibilis, quia residuorum ex aa et bb ortorum alterum alterius est complementum; residui ex quocunque alio quadrato cc orti complementum in serie residuorum quoque reperietur. Dabitur ergo summa duorum quadratorum $cc + xx$ per numerum p diuisibilis.

COROLL. 3.

82. Ex praecedentibus autem patet, hunc casum locum obtinere non posse, neque si p sit numerus formae $4n - 1$, neque si p saltem habeat factorem huius formae, quia neutro casu datur summa duorum quadratorum

torum

torum per p diuisibilis, quae quidem quadrata sint inter se prima.

COROLL. 4.

83. Nulli ergo alii numeri primi relinquuntur, ad quos theorema hoc accommodari queat, nisi qui contineantur in hac forma $4n + 1$.

SCHOLION.

84. An autem omnes numeri primi formae $4n + 1$ hanc habeant proprietatem, vt in seriebus residuorum inde ortis cuiusque termini complementum simul ibidem reperiatur, hic nondum est demonstratum, neque desperandum videtur, quin ex his iisdem principiis demonstratio elici queat, etsi nondum mihi quidem eo pertingere licuit. Series autem residuorum ex simplicioribus numeris primis huius formae ortae sequenti modo se habent, vbi quidem residua semisse cuiusque numeri maiora per numeros negatiuos exhibere visum est, quo facilius, quaenam sint aliorum complementa, appareat:

5 $\{1,-1\}$; 13 $\{1,4,-4,3,-1,-3\}$; 17 $\{1,4,-8,-1,8,2,-2,-4\}$

29 $\{1, 4, 9, -13, -4, 7, -9, 6, -6, 13, 5, -1, -5, -7\}$

37 $\{1,4,9,16,-12,-1,12,-10,7,-11,10,-4,-16,11,3,-3,-7,-9\}$

In his igitur seriebus perspicuum est, cuiusque termini complementum simul in iis occurrere. Quod autem hoc necessario eueniat, si diuisor sit numerus primus formae $4n + 1$, demonstratio directa adhuc desideratur, quae hoc modo instituí debere videtur. Prodeat ex numero primo $4n + 1$ haec series residuorum $1, \alpha, \beta, \gamma, \delta,$ etc.

etc. quorum terminorum numerus est $2n$, iam si quis neget horum terminorum complementa simul in eadem serie contineri, is dicere debet, omnia complementa $+1, -\alpha, -\beta, -\gamma, -\delta$, etc. seriem non-residuorum constituere; quorum terminorum numerus cum sit $= 2n$, sequeretur, nulla alia praeterea dari non-residua, quare, si assignari posset quispiam numerus, in serie non-residuorum contentus, qui non esset complementum cuiuspiam termini in serie residuorum contentus, simul sequeretur nullum plane complementum seriei residuorum in serie non-residuorum occurrere. Hoc ergo si demonstrari posset, haberetur demonstratio desiderata, et quidem directa. Nam demonstratio indirecta iam inde datur, quod demonstraui, omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum: quare si sit $4n + 1 = aa + bb$, residuorum ex his quadratis aa et bb ortorum alterum alterius erit complementum, hincque porro recte concluditur, cuiusque residui complementum simul in serie residuorum contineri.

THEOREMA 17.

85. *Si in serie residuorum* $1, \alpha, \beta, \gamma, \delta$, etc. *quae ex diuisione quadratorum per numerum quemcunque* p *oriuntur, occurrat terminus, qui sit complementum summae duorum aliorum terminorum, tum summa trium quadratorum exhiberi potest per numerum* p *diuisibilis, ita vt nullius quadrati radix maior sit quam* $\frac{p}{2}$.

DEMONSTRATIO.

Sint r et s residua ex duobus quadratis aa et bb orunda, quorum summa $= r + s$, eiusque ergo com-

plementum $= p - r - s$, seu $- r - s$. Iam si hoc complementum in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. reperiatur, dabitur quadratum $cc < \frac{1}{4} pp$, quod per p diuisum relinquet $- r - s$; sicque manifestum erit, summam horum trium quadratorum $aa + bb + cc$ fore per numerum p diuisibilem; neque horum quadratorum vllum maius esse, quam $\frac{1}{4} pp$.

COROLL. 1.

86. Si igitur in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. occurrat aliquis ex his numeris: -2; $-1-\alpha$; -2α; $-1-\beta$; $-\alpha-\beta$; -2β; $-1-\gamma$; $-\alpha-\gamma$; $-\beta-\gamma$; -2γ; $-1-\delta$, $-\alpha-\delta$, etc. semper summa trium quadratorum exhiberi potest per numerum p diuisibilis.

COROLL. 2.

87. Atque si p sit numerus primus, singulorum horum quadratorum radices a, b, c, cum sint minores, quam $\frac{p}{2}$, erunt numeri ad p primi, ideoque etiam ipsa quadrata, ac nisi ipsa haec tria quadrata fuerint prima inter se, sed communem habeant diuisorem quadratum, quia hic necessario est ad p primus, per eum quadrata illa reducentur ad minora et prima inter se, quorum summa pariter per p erit diuisibilis.

COROLL. 3.

88. Si in serie residuorum singulorum terminorum complementa simul insint, tum etiam summa duorum quadra-

quadratorum assignari potest per numerum p diuisibilis. Quando autem duorum quadratorum summa datur, multo magis dabitur summa trium quadratorum, cum forma $aa + bb$ contineatur in forma $aa + bb + cc$.

SCHOLION.

89. Simili modo demonstratur, si in serie residuorum occurrat numerus, qui sit complementum summae trium residuorum, tum summam quatuor quadratorum exhiberi posse, quae sit per numerum p diuisibilis. Verum si summae binorum vel ternorum residuorum capiantur, tot prodeunt numeri diuersi, vt satis manifestum videatur, eorum omnium complementa in serie non residuorum contineri non posse.

THEOREMA 18.

90. Proposito quocunque numero primo p, si non duorum quadratorum inter se primorum summa per eum diuisibilis exhiberi potest, certo semper summa trium quadratorum per eum diuisibilis assignari potest, ita vt non singula seorsim per p sint diuisibilia.

DEMONSTRATIO.

Sit $1, \alpha, \beta, \gamma, \delta, \varepsilon$, etc. series residuorum ex diuisione quadratorum per numerum propositum primum p orta. Iam in hac serie vel occurrit -1, vel non occurrit. Si -1 ibi occurrit, singulorum residuorum complementa simul ibi occurrunt, ideoque pluribus modis summa duorum quadratorum per p diuisibilis datur.

Sin autem -1 non in ſerie reſiduorum contineatur, in ſerie non-reſiduorum reperietur, vbi ſimul complementa omnium reſiduorum occurrent: hoc ergo caſu nulla dabitur ſumma duorum quadratorum per numerum p diuiſibilis; niſi vtrumque ſeorſim diuiſorem admittat. Dari autem his caſibus ſummam trium quadratorum per numerum primum p diuiſibilem ita oſtendo. Primo notetur, ſi quis numerus r in ſerie reſiduorum occurrat, eius complementum $-r$ certo in ſerie non-reſiduorum eſſe, et viciſſim ſi r ſit non-reſiduum, certo fore $-r$ reſiduum. Ponamus iam negari, vllam dari ſummam trium quadratorum per p diuiſibilem; et quia in ſerie reſiduorum primo adeſt numerus 1, numerus -2 ibidem non occurret, (alias enim daretur ſumma trium quadratorum per p diuiſibilis, contra hyp.) Occurret igitur -2 in ſerie non-reſiduorum, ac propterea numerus $+2$ in ſerie reſiduorum. Iam cum in ſerie reſiduorum habeantur numeri 1 et 2, ſummae eorum complementum -3, erit non-reſiduum, ideoque $+3$ reſiduum. Eodem modo ex reſiduis 1 et 3 concluditur fore -4 non-reſiduum ac proinde $+4$ reſiduum. Atque in genere ſi reſiduum quodcunque ſit r, debebit $-r-1$ eſſe non-reſiduum, hincque $1+r$ foret reſiduum. Ex hac ergo hypotheſi ſequitur, omnes plane numeros 1, 2, 3, 4, 5, 6, etc. in ſerie reſiduorum contineri, ſicque nullos plane numeros pro ſerie non-reſiduorum relinqui; quod cum ſit abſurdum, concludere debemus dari vtique trium quadratorum ſummam per numerum primum p diuiſibilem, quorum quidem nullum ſeorſim ſit per p diuiſibile. Quae ſi forte non fuerint prima inter ſe, per eorum

eorum maximum communem diuiſorem ad prima deprimi poterunt, quia maximus communis diuiſor quadratorum certo eſt quadratus.

COROLL. 1.

91. Simili ratiocinio euincitur, multo magis repugnare, ſi quis negaret, dari quatuor quadratorum ſummam per numerum primum diuiſibilem. Ergo propoſito numero quocunque primo p ſemper dabitur ſumma quatuor quadratorum per eum diuiſibilis.

COROLL. 2.

92. Si numerus primus p non ſit diuiſor vllius ſummae duorum quadratorum, tria illa quadrata aa, bb, cc, quorum ſumma $aa + bb + cc$ eſt per p diuiſibilis, ſingula erunt minora, quam $\frac{1}{4}pp$. Hinc ergo erit $aa + bb + cc < \frac{3}{4}pp$, vnde quotus, qui ex diuiſione huius aggregati $aa + bb + cc$ per p oritur, erit $< \frac{3}{4}p$.

THEOREMA 19.

93. Si ſumma quatuor quadratorum per ſummam quatuor quadratorum diuidatur, quotus erit quoque ſumma quatuor quadratorum ſaltem in fractis.

DEMONSTRATIO.

Sit $aa + bb + cc + dd$ ſumma quatuor quadratorum, quae diuidenda ſit per hanc ſummam quatuor quadratorum $pp + qq + rr + ss$, erit quotus $= \frac{aa+bb+cc+dd}{pp+qq+rr+ss}$, qui ſiue ſit numerus integer, ſiue fractus,

ſemper in quatuor quadrata ſaltem in fractis reſolui poteſt. Multiplicemus enim numeratorem et denominatorem per $pp + qq + rr + ss$, vt denominator fiat quadratus, erit quotus iſte $= \frac{(aa+bb+cc+dd)(pp+qq+rr+ss)}{(pp+qq+rr+ss)^2}$; quod ſi iam numerator in quatuor quadrata reſolui queat, ipſa fractio aequabitur aggregato quatuor quadratorum. At numerator pluribus modis in quatuor quadrata reſolui poteſt; ſi enim ponatur $(aa + bb + cc + dd)(pp + qq + rr + ss) = xx + yy + zz + vv$, erit

$$\left.\begin{aligned} x &= ap + bq + cr + ds \\ y &= aq - bp \pm cs \mp dr \\ z &= ar \mp bs - cp \pm dq \\ v &= as \pm br \mp cq - dp \end{aligned}\right\}$$

qui quatuor numeri, ſi ſinguli diuidantur per communem denominatorem $pp + qq + rr + ss$, dabunt radices quatuor quadratorum, quorum ſumma aequatur quoto propoſito.

Niſi igitur hi numeri x, y, z, et v ſint diuiſibiles per $pp + qq + rr + ss$, ſaltem in fractis aſſignari poſſunt quatuor quadrata, quorum ſumma aequalis eſt quoto $\frac{aa+bb+cc+dd}{pp+qq+rr+ss}$.

COROLL. 1.

94. Quae hic de quatuor quadratorum ſummis ſunt demonſtrata, etiam ad ſummas trium, vel etiam duorum patent, cum nihil impediat, quominus vnus, vel duo ex numeris a, b, c, d, et p, q, r, s ſint aequales nihilo.

COROLL. 2.

94. Si igitur ſumma trium quadratorum per ſummam quatuor, vel etiam trium quadratorum diuidatur, quotus certe erit ſumma quatuor quadratorum.

COROL.

COROLL. 3.

95. Quia productum ex duabus summis quatuor quadratorum est quoque summa quatuor quadratorum, patet, si omnes numeri primi sint summae quatuor quadratorum, vel etiam pauciorum, tum etiam omnes omnino numeros esse summas quatuor quadratorum, vel etiam pauciorum.

SCHOLION.

96. Si summa quatuor quadratorum $aa + bb + cc + dd$ fuerit diuisibilis per summam quatuor quadratorum $pp + qq + rr + ss$, tum quotum non solum in fractis, sed etiam in integris, esse summam quatuor quadratorum, est theorema elegantissimum Fermatii, cuius demonstratio cum ipso nobis est erepta. Fateor, me adhuc hanc demonstrationem inuenire non potuisse, verumtamen hinc via aperitur ad theorema sequens demonstrandum, quo quilibet numerus summa quatuor quadratorum, vel pauciorum asseritur; casu scilicet, quo quadrata fracta non excluduntur: etsi enim hoc theorema in integris quoque semper verum sit, tamen non parum mihi praestitisse videor, quod id semota quadratorum integrorum ratione demonstrauerim. Cum enim demonstratio adhuc post Fermatium sit frustra indagata, me proxime ad hunc scopum pertigisse arbitror.

THEOREMA 20.

97. Omnis numerus est summa quatuor quadratorum, vel etiam pauciorum, siquidem quadrata fracta non excludantur.

DEMON-

DEMONSTRATIO.

Theorema hoc quidem verum est, etiamsi quadrata fracta excludantur; Fermatius enim affirmat, omnem numerum integrum esse aggregatum ex quatuor quadratis integris, vel etiam paucioribus, ego autem fateor, me hanc demonstrationem nondum inuenire potuisse, dabo ergo demonstrationem pro casu, quo quadrata fracta non excluduntur. Iam notaui hanc demonstrationem tantum ad numeros primos reduci, de quibus ergo sufficit theorema demonstrasse. Quoniam igitur nouimus, numeros primos minores vt 2, 3, 5, 7, 11, 13, etc. omnes in quatuor, vel pauciora quadrata resolui posse, si quis id de sequentibus neget, ei dicendum est, dari aliquem numerum primum minimum, qui non sit summa quatuor pauciorumue quadratorum. Sit p iste numerus primus, ita vt omnes numeri primi ipso minores, hincque etiam omnes compositi certo sint summae quatuor pauciorumue quadratorum. Iam per theorema praecedens datur summa trium quadratorum, quae sit $aa + bb + cc$ diuisibilis per numerum istum p, ita vt singula haec quadrata sint minora quam $\frac{1}{4}pp$; vnde erit $aa + bb + cc < \frac{3}{4}pp$. Quotus ergo $\frac{aa+bb+cc}{p}$ erit minor, quam $\frac{3}{4}p$, qui cum idcirco minor sit, quam p, certe erit summa quatuor pauciorumve quadratorum; sit $xx + yy + zz + vv$ iste quotus, erit $p = \frac{aa+bb+cc}{xx+yy+zz+vv}$, ideoque ipse numerus p erit summa quatuor pauciorumue quadratorum, quae in fractionibus etiam assignari possunt. Cum igitur inter numeros primos non detur minimus, qui in quatuor

quatuor vel pauciora quadrata dispertiri nequeat, nullus prorsus datur numerus primus, qui non esset aggregatum quatuor pauciorumue quadratorum, quod cum certum sit de numeris primis, etiam valebit de omnibus numeris compositis, ideoque de omnibus omnino numeris, ita vt nullus omnino detur numerus, qui non sit summa quatuor pauciorumue quadratorum.

COROLL. 1.

98. Cum omnis numerus integer sit summa quatuor pauciorumue quadratorum, eadem proprietas etiam ad omnes numeros fractos patet. Sit enim proposita fractio quaecunque $\frac{m}{n}$, quae transformetur in $\frac{mn}{nn}$. Iam sit $mn = \frac{aa}{pp} + \frac{bb}{qq} + \frac{cc}{rr} + \frac{dd}{ss}$, eritque $\frac{mn}{nn} = \frac{m}{n} = \frac{aa}{npp} + \frac{bb}{nnqq} + \frac{cc}{nnrr} + \frac{dd}{nnss}$; ideoque omnis numerus fractus erit summa quatuor pauciorumue quadratorum.

COROLL. 2.

99. Quoniam, si de resolutione numerorum fractorum in quadrata, fermo est, conditio illa quadratorum integrorum sponte euanescit, theorema in latiori sensu ita acceptum, vt omnes plane numeros, siue integros, siue fractos, in quatuor vel pauciora quadrata resolubiles dicamus, sine vlla restrictione rigide demonstraui.

SCHOLION.

100. Cum igitur Fermatius affirmasset, omnem numerum integrum esse summam vel quatuor vel pau-

ciorum quadratorum integrorum: nunc quidem hoc eſt demonſtratum de quadratis in genere ſpectatis, fractis non excluſis. Quare vt Fermatio ſatisfiat, ſupereſt vt demonſtremus, qui numerus integer in quatuor quadrata fracta reſolui queat, eundem quoque in quatuor vel pauciora quadrata integra reſolui poſſe. In analyſi quidem Diophantaea pro certo aſſumi ſolet, nullum numerum integrum in quatuor quadrata fracta diſpertiri poſſe, niſi eius reſolutio in quatuor quadrata integra vel pauciora conſtet: quod ergo ſi demonſtratione eſſet confirmatum, nihil foret amplius deſiderandum. Verum nusquam adhuc eiusmodi demonſtrationem inueni. Quod autem ad theorema latiſſime patens attinet, his verbis conceptum:

Omnem numerum ſiue integrum ſiue fractum eſſe ſummam quatuor pauciorumue quadratorum.

eius demonſtrationem hic tradidi ita rigoroſam, vt in ea nihil plane deſiderari queat: hocque ipſo non contemnendam partem demonſtrationum Fermatianarum deperditarum mihi equidem videor reſtituiſſe.

OBSER-