1760

Demonstratio theorematis Fermatiani omnem numerum primum formae $4n+1$ esse summam duorum quadratorum

Leonhard Euler

E241

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 leuis 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 feliciter 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 $4n + 1$ fuerit 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.

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

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: $2^{2n}-1$; $3^{2n}-2^{2n}$; $4^{2n}-3^{2n}$; $5^{2n}-4^{2n}$; ...... $(2n+1)^{2n}-(2n)^{2n}$ 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 $= 2 \cdot n$, 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. Quia 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.

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 $m - m = o$ perueniet, eiusque ergo terminus generalis, quia summa ipsius x potestas est $= x^o = 1$, erit quantitas constans, ideoque omnes differentiae ordinis m inter se erunt aequales. Hinc serierum primi gradus, quarum terminus generalis est $= A x + B$, iam differentiae primae sunt inter se aequales: serierum autem secundi gradus, quae hoc termino generali $A x^2 + B x + C$ continentur, differentiae secundae sunt aequales, et ita porro.

§. 12. Quodsi ergo seriem quamcunque potestatum consideremus

$$1, 2^m, 3^m, 4^m, 5^m, 6^m, 7^m, 8^m, \text{ etc.}$$

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.

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