
DEMONSTRATIO
 THEOREMATIS FERMATIANI
 OMNEM NUMERUM PRIMUM FORMAE $4n+1$
 ESSE SUMMAM DUORUM QUADRATORUM.

AVCTORE LEONARDO EULERO

§. I.

Cum nuper eos effem contemplatus numeros, qui ex additione duorum quadratorum oriuntur, plures demonstrandi proprietates, quibus tales numeri sunt praediti: neque tamen meas meditationes eo usque perducere licuit, ut huius theorematis, quod Fermatius olim Geometris demonstrandum proposuit, veritatem solide ostendere potuiffem. Tentamen tamen demonstrationis tum exposui, unde certitudo huius theorematis multo luculentius elucet, etiam si criteriis rigidae demonstrationis destituatur: neque dubitavi, quin iisdem vestigiis insistendo tandem demonstratio desiderata facilius obtineri possit; quod quidem ex eo tempore mihi ipsi usu venit, ita, ut tentamen illud, si alia quaedam levis consideratio accedat, in rigidam demonstrationem abeat. Nihil quidem novi 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 inventorum efficit, ut, quae nunc demum de his deperditis rebus quasi recuperamus, ea non immerito pro novis inventis habeantur. Cum enim nemo unquam

tam feliciter in arcana numerorum penetrauerit, quam Fermatius, omnis opera in hac scientia ulterius 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. Ut autem demonstrationem theorematis, quod hic considero, instituum, 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 his 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 quicumque 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

THEOREMATIS FERMATIANI. §

tamen excepta), numerus inde formatus $a^{2^n} - b^{2^n}$ sine
 vlla limitatione per numerum primum propositum
 $4n + 1$ erit diuisibilis. Cum autem $a^{2^n} + b^{2^n}$ sit pro-
 ductum horum factorum $a^{2^n} + b^{2^n}$ et $a^{2^n} - b^{2^n}$, necesse
 est, vt alteruter horum factorum sit per $4n + 1$ di-
 uisibilis; fieri enim nequit, vt vel neuter, vel vterque
 simul diuisorem habeat $4n + 1$. Quodsi iam demon-
 strari posset, dari casus, quibus forma $a^{2^n} + b^{2^n}$ sit diui-
 sibilis per $4n + 1$, quoniam $a^{2^n} + b^{2^n}$, ob exponen-
 tem $2n$ parem, est summa duorum quadratorum, quo-
 rum neutrum seorsim per $4n + 1$ diuisibile existit,
 inde sequeretur, hunc numerum $4n + 1$ esse sum-
 mam duorum quadratorum.

§. 4. Verum summa $a^{2^n} + b^{2^n}$ toties erit per
 $4n + 1$ diuisibilis, quoties differentia $a^{2^n} - b^{2^n}$ per
 eundem numerum non est diuisibilis. Quare qui nega-
 uerit, numerum primum $4n + 1$ esse summam duo-
 rum quadratorum, is negare cogitur, vllum numerum hu-
 ius formae $a^{2^n} + b^{2^n}$ per $4n + 1$ esse diuisibilem: eun-
 dem propterea affirmare oportet, omnes numeros in
 hac forma $a^{2^n} - b^{2^n}$ contentos per $4n + 1$ esse diui-
 sibles; siquidem neque a , neque b per $4n + 1$ sit di-
 uisibile. Quamobrem mihi hic demonstrandum est, non
 omnes numeros in forma $a^{2^n} - b^{2^n}$ contentos per
 $4n + 1$ esse diuisibiles; hoc enim si praestitero,
 certum erit, dari casus, seu numeros pro a et b substi-
 tuendos, quibus forma $a^{2^n} - b^{2^n}$ non sit per $4n + 1$
 diuisibilis; illis ergo casibus altera forma $a^{2^n} + b^{2^n}$ neces-
 sario per $4n + 1$ erit diuisibilis: vnde cum a^{2^n} et
 b^{2^n} 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 unitate vsque ad eam, quae a radice $4n$ formatur.

$1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}, 6^{2n}, \dots, (4n)^{2n}$
 ac iam dico, non omnes differentias inter binos terminos huius seriei esse per $4n + 1$ diuisibiles. Si enim singulae differentiae primae
 $2^{2n} - 1; 3^{2n} - 2^{2n}; 4^{2n} - 3^{2n}; 5^{2n} - 4^{2n}; \dots (4n)^{2n} - (4n - 1)^{2n}$
 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
 $= 1. 2. 3. 4. \dots 2n$, 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

THEOREMATIS FERMATIANI. 7

plures termini ad hanc differentiam ultimam constituendam concurrerent, iique ultra terminum $(4n)^{2n}$ progredierentur, quoniam differentiae a termino sequente $(4n+1)^{2n}$ ortae ad enunciata theorematis non pertinent, demonstratio nullam vim retineret. Hinc autem, quod differentia ultima, 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, ut 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

$1; 2^{2n}; 3^{2n}; 4^{2n}; 5^{2n}; 6^{2n} \dots (2n)^{2n}; (2n+1)^{2n}$
 vnde differentiae primae erunt: $2^{2n} - 1; 3^{2n} - 2^{2n};$
 $4^{2n} - 3^{2n}; 5^{2n} - 4^{2n}; \dots (2n+1)^{2n} - (2n)^{2n}$
 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 observatio 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 $n = 1$; unde 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 utamur 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	$2^2 - 1$ o	$3^2 - 2^2$ o
17	$2^4 - 1$ d	$3^4 - 2^4$ o
29	$2^{14} - 1$ o	$3^{14} - 2^{14}$ d
	$4^6 - 3^6$ d	$5^6 - 4^6$ o
	$6^6 - 5^6$ d	$7^6 - 6^6$ d
	$8^8 - 7^8$ o	$9^8 - 8^8$ d
	$10^{14} - 9^{14}$ o	$11^{14} - 10^{14}$ d
	$12^{14} - 11^{14}$ d	$13^{14} - 12^{14}$ o
	$14^{14} - 13^{14}$ o	$15^{14} - 14^{14}$ d

Hinc patet, terminos diuisibiles et non diuisibiles nulla certa lege contineri, etiamsi utrique 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.

THEOREMATIS FERMATIANI. 9

§. 9. Porro quoque ad vim demonstrationis penitus perspiciendam notari oportet, demonstrationem solum locum habere, si numerus $4n + 1$ sit primus; prorsus uti natura theorematis postulat. Nam si $4n + 1$ non esset numerus primus, neque de eo affirmari posset, quod sit summa duorum quadratorum, neque forma $a^{2n} - b^{2n}$ per eum esset necessario divisibilis. Quia etiam ultima conclusio foret falsa, qua pronunciauimus, differentias illas ordinis $2n$, quae sunt $1. 2. 3. 4. \dots 2n$, non esse per $4n + 1$ divisibiles. Si enim $4n + 1$ non esset numerus primus, sed factores haberet, qui essent minores, quam $2n$, tum utique productum $1. 2. 3. 4. \dots 2n$ hos factores contineret, foretque idcirco per $4n + 1$ divisibile. At si $4n + 1$ est numerus primus, tum demum affirmare licet, productum $1. 2. 3. 4. \dots 2n$ plane non esse per $4n + 1$ divisibile: 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 $1. 2. 3. 4. \dots 2n$, 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 seriei 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 depressoerem $m - 2$ 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 quarumarum ad gradum $m - 4$; et in genere series differentiarum ordinis n ad gradum $m - n$ pertinebit. Vnde series differentiarum ordinis m ad gradum $m - m = 0$ perveniet, 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

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

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

THEOREMATIS FERMATIANI. 11

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 $= (x+m)^m - m(x+m-1)^m + \frac{m(m-1)}{1 \cdot 2}(x+m-2)^m - \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3}(x+m-3)^m + \text{etc.}$ qui cum fit quantitas constans, idem erit quicumque numerus pro x substituatur, erit ergo

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

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

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: acposito primo $m = 1$, seriei 1, 2, 3, 4, 5, 6, etc. terminus generalis differentiarum primarum erit $= 1^1 - 1 \cdot 0^1 = 1$; vel $= 2^1 - 1 \cdot 1^1 = 1$. Si $m = 2$, seriei 1; 2²; 3²; 4²; 5²; etc. differentiae secundae sunt vel $2^2 - 2 \cdot 1^2$, vel $3^2 - 2 \cdot 2^2 + 1 \cdot 1^2$; at est $2^2 - 2 \cdot 1^2 = 2(2^1 - 1 \cdot 1^1)$, unde hae differentiae secundae sunt $= 2 \cdot 1$. Sit $m = 3$, et seriei 1, 2³, 3³, 4³, 5³, etc. differentiae tertiae erunt vel $3^3 - 3 \cdot 2^3 + 3 \cdot 1^3$, vel $4^3 - 3 \cdot 3^3 + 3 \cdot 2^3 - 1 \cdot 1^3$; at $3^3 - 3 \cdot 2^3 + 3 \cdot 1^3 = 3(3^2 - 2 \cdot 2^2 + 1 \cdot 1^2) = 3 \cdot 2 \cdot 1$, quia ex casu praecedente est $3^2 - 2 \cdot 2^2 + 1 \cdot 1^2 = 2 \cdot 1$. Simili modo si $m = 4$ seriei 1, 2⁴, 3⁴, 4⁴, 5⁴,

B 2

etc.

etc. differentiae quartae erunt vel $4^4 - 4 \cdot 3^4 + 6 \cdot 2^4 - 4 \cdot 1^4$;
 vel $5^4 - 4 \cdot 4^4 + 6 \cdot 3^4 - 4 \cdot 2^4 + 1 \cdot 1^4$. At est $4^4 - 4 \cdot 3^4$
 $+ 6 \cdot 2^4 - 4 \cdot 1^4 = 4 (4^3 - 3 \cdot 3^3 + 3 \cdot 2^3 - 1 \cdot 1^3)$
 $= 4 \cdot 3 \cdot 2 \cdot 1$.

§. 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 $P = (m + 1)^m - m \cdot m^m + \frac{m(m-1)}{1 \cdot 2} (m-1)^m - \frac{m(m-2)(m-1)}{1 \cdot 2 \cdot 3} (m-2)^m + \text{etc.}$
 $Q = (m + 1)^{m+1} - (m + 1) m^{m+1} + \frac{(m+1)m}{1 \cdot 2} (m-1)^{m+1} - \frac{(m+1)m(m-1)}{1 \cdot 2 \cdot 3} (m-2)^{m+1} + \text{etc.}$ Vbi P ex forma posteriori, at Q ex forma priori expressimus. Hic primo patet, in utraque expressione parem esse terminorum numerum, et singulos terminos expressionis P esse ad singulos terminos expressionis Q , uti 1 ad $m + 1$. Namque est

$$\begin{aligned} (m + 1)^m : (m + 1)^{m+1} &= 1 : m + 1; \\ m \cdot m^m : (m + 1) m^{m+1} &= 1 : m + 1; \\ \frac{m(m-1)}{1 \cdot 2} (m-1)^m : \frac{(m+1)m}{1 \cdot 2} (m-1)^{m+1} &= 1 : m + 1; \\ \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3} (m-2)^m : \frac{(m+1)m(m-1)}{1 \cdot 2 \cdot 3} (m-2)^{m+1} &= 1 : m + 1; \\ &\text{etc.} \end{aligned}$$

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

§. 15. Hinc ergo patet fore

seriei	Differentias
$1, 2, 3, 4, 5, \text{etc.}$	primas $= 1$
$1, 2^2, 3^2, 4^2, 5^2, \text{etc.}$	secundas $= 1 \cdot 2$
	$1, 2^3, 3^3, \text{etc.}$

THEOREMATIS FERMATIANI. 13

$1; 2^3; 3^3; 4^3; 5^3; \text{etc.}$ tertias $= 1. 2. 3$
 $1; 2^4; 3^4; 4^4; 5^4; \text{etc.}$ quartas $= 1. 2. 3. 4$

$1; 2^m; 3^m; 4^m; 5^m; \text{etc.}$ ordinis $m = 1. 2. 3. \dots m$,
 ergo

$1; 2^{2n}; 3^{2n}; 4^{2n}; 5^{2n}; \text{etc.}$ ordinis $2n = 1. 2. 3. \dots 2n$.
 Atque ita quoque demonstremus, seriei potestatum
 $1; 2^{2n}; 3^{2n}; 4^{2n}; 5^{2n}; \text{etc.}$ differentias ordinis $2n$ non
 solum esse constantes, sed etiam aequari producto
 $1. 2. 3. \dots 2n$, uti in demonstratione theorematis
 propositi assumimus.

THEOREMA I.

1. Ex serie quadratorum $1, 4, 9, 16, 25, \text{etc.}$
 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, ut 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. I.

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

E. 3 COROLL.