Proof of Fermat's Theorem That Every Prime Number of the Form $4n + 1$ is the Sum of Two Squares*

by Leonhard Euler

Translated by Mark R. Snavely and Phil Woodruff

Transcription by Phil Woodruff

1. When I had recently considered numbers which arise from the addition of two squares, I proved several properties which such numbers possess. However, I could not explain my thoughts to the extent that I would have been able to show fully the truth of the theorem, which Fermat once conjectured, and left to be proven by the Geometers. I next put forth an attempt of the proof from which the validity of this theorem is revealed much more clearly, even if it should be set aside by the standards of rigorous proof. Nor did I doubt that by following these same methods, the desired proof could at last be obtained quite easily; because indeed from that time it came to me by experimentation in such a way that, if a certain other consideration should agree, the attempt would transform into a rigorous proof. Indeed I am not able to boast that I have shown anything new in this matter since Fermat himself claims that he has already produced a proof of this theorem; but because he did not

*L. Euler, *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum* (E241). Acta *Novi Commentarii academiae scientiarum Petropolitanae* 5, 1760, pp. 3-13. Reprinted in *Opera Omnia*: Series 1, Volume 2, pp. 328 - 337, and in *Commentat. arithm.* 1, 1849, pp. 210-215 [E241a]. Original article available online at www.eulerarchive.org.

make it public anywhere, just as with the loss of this and many other famous ideas of this man, it follows that the ideas which now at last we recover, as if they were lost, should not undeservedly be considered as new findings. For since no one has ever entered so happily into the mysteries of numbers as Fermat, every effort expended even more in this field seems to be expended in vain, unless first the things which had already been investigated by this excellent man should be brought to light as if new. For even if after him many more learned men have applied their powers in this area of studies, still for the most part they pursued nothing which could be compared to the talent of this man.

2. But in order that I may begin a proof of the theorem which I consider here, two propositions must be called upon for help, a proof of which I have already given elsewhere. One is, that all numbers which are divisors of the sum of two squares and which are prime numbers unto each other [relatively prime], should themselves be the sum of two squares. Thus, if a and b should be prime numbers unto each other and the number formed from these, $a^2 + b^2$, is divisible by d, d also will be the sum of two squares. I gave a proof of this theorem in a writing recounted previously where I considered numbers which are the sums of two squares. A second proposition, which the following proof requires, is as follows: If p is a prime number and some numbers a and b are not divisible by p, $a^{p-1} - b^{p-1}$ will always be divisible by the prime number p; I have already given a proof of this matter in Comment. Acad. Petrop. Volume. VIII[†].

3. Now if $4n + 1$ is a prime number, all numbers of this form $a^{4n} - b^{4n}$ will be divisible by it $[4n + 1]$, if in fact neither of the numbers a and b separately are divisible by $4n + 1$.

[†]Available line at www.eulerarchive.com, article E54.

Therefore if a and b should be numbers smaller than $4n+1$, (zero excepted), then the number formed, $a^{4n} - b^{4n}$, without any limitation [i.e., for any n], will be divisible by the proposed prime number $4n+1$. But since $a^{4n} + b^{4n}$ [Ed: believed to be $a^{4n} - b^{4n}$] is a product of these factors $a^{2n} + b^{2n}$ and $a^{2n} - b^{2n}$, it is necessary that one of the two of these factors be divisible by $4n+1$. For it is not possible that either neither [factor] or each [factor] would have the divisor $4n+1$ at the same time. Now if it could be shown that cases arise in which the form $a^{2n} + b^{2n}$ is divisible by $4n+1$, since $a^{2n} + b^{2n}$, because of the even exponent $2n$, is the sum of two squares of which neither separately is divisible by $4n+1$, then it would follow that this number $4n+1$ is the sum of two squares.

4. But as often as the sum of $a^{2n} + b^{2n}$ will be divisible by $4n+1$, so too the difference of $a^{2n} - b^{2n}$ is not divisible by the same number. Therefore, the one who denies that the prime number $4n+1$ is the sum of two squares is compelled to deny that any number of the form $a^{2n} + b^{2n}$ is divisible by $4n+1$; thus, one must affirm the same [statement]: that all numbers of the form $a^{2n} - b^{2n}$ are divisible by $4n+1$, if indeed neither a nor b is divisible by $4n+1$. And for this reason I had to prove that not all numbers of the form $a^{2n} - b^{2n}$ are divisible by $4n+1$. Indeed, for if I show this, it will be certain that cases arise, or numbers can be substituted for a and b, in which the form $a^{2n} - b^{2n}$ is not divisible by $4n+1$. Therefore, for those cases, the other form $a^{2n} + b^{2n}$ by necessity will be divisible by $4n+1$. From this then, since a^{2n} and b^{2n} are square numbers, that which is proposed will be proven; obviously, that the number $4n+1$ is the sum of two squares.

5. Therefore, so that I might prove that not all numbers of this form, $a^{2n} - b^{2n}$, or that

not all differences among the paired exponentials of the power $2n$ are divisible by $4n+1$, I shall consider a series of these exponentials from one up to the (exponential) which is formed by the base $4n$.

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

And so I say that not all differences among the paired terms of this series are divisible by $4n+1$. For if the first differences, one by one,

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

should be divisible by $4n+1$, the differences of this progression, which are the second differences of that series, would also be divisible by $4n+1$; and so for this same reason, the third differences, the fourth, fifth, etc.; all would be divisible by $4n+1$. And finally also the differences of the order $2n$, which are, as is agreed, all equal among themselves. The differences of the order $2n$ are $= 1.2.3.4\ldots 2n$,§ which therefore, are not divisible by the prime number $4n+1$. From this it follows in turn that not all first differences are divisible by $4n+1$.

6. So that the force of this proof should be better ascertained, it must be noted that the differences of order $2n$, to be taken from the $2n+1$ expressions of the proposed series, all of which, if they should be taken from the beginning, are arranged in such a way that the differences of any paired expression should be divisible by $4n+1$, if the truth of the theorem

‡Ed: Believed to be $2^{2n}-1, 3^{2n}-2^{2n}, 4^{2n}-3^{2n}, 5^{2n}-4^{2n}, \ldots (4n)^{2n}-(4n-1)^{2n}$ throughout the paper.

§Ed: $1.2.3\ldots 2n = 1\cdot 2\cdot 3\ldots(2n) = (2n)!$ throughout the paper.

should be denied. But if, however, more expressions should be put together to determine this last value, and these extend beyond the expression $(4n)^{2n}$, since the differences, which arise from the following expression $(4n+1)^{2n}$ do not pertain to the propositions of the theorem, the proof would have no force. From here then, because the final difference, which we have considered, depends so much from the $2n+1$ expression, the conclusion, which we have deduced therefrom, is entirely correct. It follows that first differences arise, such as $a^{2n} - (a-1)^{2n}$, which are not divisible by $4n+1$, and so indeed, a becomes not larger than $2n+1$. From here, then, it is correctly inferred that the sum $a^{2n} + (a-1)^{2n}$, and likewise the sum of two squares, is by necessity divisible by $4n+1$; and for that reason the prime number $4n+1$ is the sum of two squares.

7. Since the difference of the order $2n$ depends on the $2n+1$ expressions of the series of powers, let us consider the same number of expressions taken just from the beginning:

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

from which the first differences will be:

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

the number of expressions of this progression is $= 2n$. And thus from the proceeding proof it is clear that not all expressions of this progression of differences are divisible by the prime number $4n+1$; nor do we understand from this part how many and which ones are those expressions not divisible by $4n+1$. For proof (of this) it is sufficient if even one expression, whatever that is, not be divisible by $4n+1$. Now if we should reveal special cases in which

$4n+1$ is a prime number from those differences of which the number is $= 2n$, we will discover that the half [factor] is always divisible by $4n+1$, while the other half [factor] is not divisible; though this observation does not relate to the force of the proof, still it helps significantly to illustrate it. Therefore it will help to submit a few special cases to the test.

8. The smallest prime number of the form $4n + 1 = 5$, which arises if $n = 1$, from which the two differences $2^2 - 1$ and $3^2 - 2^2$ will be considered, of which the first is not divisible by 5, but the other is divisible [by 5]. For the remaining cases we use the sign d to indicate the differences which are divisible [Ed. by $4n + 1$] and with the sign $\circ$ we note those which are not divisible [Ed. by $4n + 1$]; these signs for the differences for whatever case we write below:

Differences

$4n+1$								
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		

From here it is evident that the divisible and non-divisible expressions are held by no fixed rule even if each be equal in number; still it is clear, in and of itself, that the last expression $(2n+1)^{2n}-(2n)^{2n}$ is always divisible by $4n+1$ since it has the factor $(2n+1)^2-4nn = 4n+1$, but from the rest nothing certain can be determined.

9. Furthermore, it must also be noted, to ascertain the force of the proof more completely, that the proof is only valid if the number $4n + 1$ is prime; of course, as the nature of the

theorem demands. For if $4n+1$ should not be prime, neither would the proof be affirmed from it, because it is the sum of two squares, nor by necessity would the form $a^{4n}-b^{4n}$ be divisible by it. Indeed, the final conclusion should be clear, where we have asserted that those differences of the order $2n$, which are $= 1.2.3.4\ldots 2n$, are not divisible by $4n+1$. For if $4n+1$ should not be a prime number but should have factors which would be less than $2n$, then, of course, the product $1.2.3.4.\ldots 2n$ would contain these factors and would therefore be divisible by $4n+1$. But if $4n+1$ is a prime number, then indeed one can assert that the product $1.2.3.4.\ldots 2n$ is clearly not divisible by $4n+1$, since this product can be divided by no other numbers except those factors which enter into that [product].

10. Since, in short, the proposed proof relies on this foundation, inasmuch for the series of powers 1, 2^{2n}, 3^{2n}, 4^{2n}, etc., the differences of the order $2n$ are constant and all $= 1.2.3.4.\ldots 2n$, it seems that this should be explained more fully, although it is found clearly explained here and there in the books of the analysts. Therefore, it first must be noted, if a general expression of any series, or perhaps one which corresponds to x with an indefinite exponent, becomes $= Ax^m+Bx^{m-1}+Cx^{m-2}+Dx^{m-3}+Ex^{m-4}+$etc., that this series is carried out to step m, since m is the exponent of the greatest power of x itself. Then, if the general expression should be carried out from the following $A(x+1)^m+B(x+1)^{m-1}+C(x+1)^{m-2}+$ etc., it will turn out to be a general expression of a series of differences in which the exponent of the highest power of x itself will be $= m-1$, and for that reason a series of differences to the lesser step $m-1$ will apply. In similar fashion from a general expression for a series of first differences will be deduced a general expression for a series of second differences which

therefore, in turn, will apply to the lesser step $m-2$.

11. Thus, if a proposed series should be carried to step m, a series of first differences, it will be carried to step $m-1$; next a series of second differences to step $m-2$, a series of third differences to step $m-3$; a series of fourth differences to step $m-4$; and in the same way a series of values of the order n will extend to the step $m-n$. From which the series of differences of the order m will reach to the step $m-n=0$, and therefore its general expression, since the greatest power of x itself is the power $= x^0 = 1$, will be a constant quantity, and therefore all the values of the order m will be equal among themselves. From here, the first step of a series, of which the general expression is $= Ax+B$, the first differences are now equal among themselves; but the second steps of a series, which are contained in the general expression Ax^2+Bx+C, the second differences are equal, and so on.

12. Now we should consider some series of powers

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

its general expression of which is $= x^m$, or more accurately, the series which corresponds to the unit x, of differences of the order m will be consistent from expressions equal among themselves. But for a series of first differences the general expression will be $= (x+1)^m - x^m$, which, when subtracted from the following $(x+2)^m-(x+1)^m$, will give the general expression for a series of second differences, which will be $= (x+2)^m - 2(x+1)^m + x^m$. From here, then, for a series of third differences the general expression will be $= (x+3)^m - 3(x+2)^m + 3(x+1)^m - x^m$; and finally for the series of differences of the order m results in the general expression

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

which, when it becomes a constant quantity will be the same should any number be substituted for x; and will be therefore:

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

or

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

where in the first formula we placed $x = 0$, in the second, $x = 1$.

13. Now let us develop special cases of this series and let us ascend from the lowest powers to the higher ones. And so, with $m = 1$ as the first example, for the series $1, 2, 3, 4, 5, 6,$ etc. the general expression of first differences will be $= 1^1 - 1.0^1 = 1$; or $= 2^1 - 1.1 = 1$. If $m = 2$, for the series $1; 2^2; 3^2; 4^2; 5^2 \ldots$ etc. the second differences are either $2^2 - 2.1^2$,[¶] or $3^2 - 2.2^2 + 1.1^2$; but $2^2 - 2.1^2 = 2(2^1 - 1.1^1)$, from which these second differences are $= 2.1$. Let $m = 3$, and for the series $1, 2^3, 3^3, 4^3, 5^3$, etc., the third differences will be either $= 3^3 - 3.2^3 + 3.1^3$ or $4^3 - 3.3^3 + 3.2^3 - 1.1^3$; but $3^3 - 3.2^3 + 3.1^3 = 3(3^2 - 2.2^2 + 1.1^2) = 3.2.1$, since from the preceding case $3^2 - 2.2^2 + 1.1^2 = 2.1$. In a similar fashion, if $m = 4$, for the series $1, 2^4, 3^4, 4^4, 5^4$, etc. the fourth differences will be $4^4 - 4.3^4 + 6.2^4 - 4.1^4$; or $5^4 - 4.4^4 + 6.3^4 - 4.2^4 + 1.1^4$. But $4^4 - 4.3^4 + 6.2^4 - 4.1^4 = 4(4^3 - 3.3^3 + 3.2^3 - 1.1^3) = 4.3.2.1$.

14. So that this progression might be better understood, for the series $1, 2^m, 3^m, 4^m, 5^m,$ etc. let the differences of the order be m be $= P$; for the series $1;\ 2^{m+1};\ 3^{m+1};\ 4^{m+1};\ 5^{m+1}$etc.[‖] the differences of order $m + 1 = Q$. [The expression] P will be

[¶]Ed. Adding a 0 to the beginning of the series.

[‖]Ed: Believed to be $1,\ 2^{m+1},\ 3^{m+1},\ 4^{m+1},\ 5^{m+1}$etc

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

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

where we have described P from the latter pattern, but Q from the former. Here, it is first clear that in each statement the number of terms is equal and each of the terms of the statement P correspond to each of the terms of the statement Q, as 1 is to $m+1$. For it is

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

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

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

$\frac{m(m-1)(m-2)}{1.\ 2.\ 3}(m-2)^m : \frac{(m+1)m(m-1)}{1.\ 2.\ 3}(m-2)^{m+1} = 1 : m+1;$

On account of this it will be $P : Q = 1 : m+1$, and likewise $Q = (m+1)P$.

15. From here, therefore, it is clear that there will be

for the series	the differences
$1;\ 2;\ 3;\ 4;\ 5;$ etc.	First $= 1$
$1;\ 2^2;\ 3^2;\ 4^2;\ 5^2;$ etc.	Second $= 1.2$
$1;\ 2^3;\ 3^3;\ 4^3;\ 5^3;$ etc.	Third $= 1.2.3$
$1;\ 2^4;\ 3^4;\ 4^4;\ 5^4;$ etc.	Fourth $= 1.2.3.4$
$1;\ 2^m;\ 3^m;\ 4^m;\ 5^m;$ etc.	Of the order $m = 1.2.3 \ldots m$,
	Therefore
$1;\ 2^{2n};\ 3^{2n};\ 4^{2n};\ 5^{2n};$ etc.	Of the order $2n = 1.2.3 \ldots 2n$

And so we have thus also shown that for the series of powers $1;\ 2^{2n};\ 3^{2n};\ 4^{2n};\ 5^{2n};$ etc. the differences of the order $2n$ not only are constant but also equal the product 1. 2. 3. ... $2n$

** Believed to be $Q = (m+1)^{m+1} - (m+1)(m)^{m+1} + \frac{(m+1)m}{1.\ 2}(m-1)^{m+1} - \frac{(m+1)m(m-1)}{1.\ 2.\ 3}(m-2)^{m+1} + \text{etc.}$

as we have asserted in the proof of the proposed theorem.

Theorem 1

From the series of squares $1, 4, 9, 16, 25$ etc., no numbers are divisible by the prime number p unless the roots of these are divisible by the same number p.

Proof

For if some square number aa, which consists of the factors a and a, will be divisible by the prime number p, it is necessary that one of the two be a factor divisible by p, therefore the square number aa cannot be divisible by the prime number p, unless its root a be divisible by p.

Corollary 1

Therefore, square numbers divisible by the prime number p arise from the roots $p, 2p, 3p, 4p \ldots$, etc. and are therefore pp, $4pp$, $9pp$, $16pp$, etc. and all the remaining square numbers will not be divisible by the prime number p.

Demonstatio Theorematis Fermatiani Omnem Numerum Primum Formae $4n + 1$ Esse Summam Duorum Quadratorum

Auctore Leonardo Eulero

1. Cum nuper eos essem contemplatus numeros, qui ex additione duorum quadratorum oriuntur, plures demonstravi 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 potuissem. Tentamen tamen demonstrationis tum exposui, unde certitudo huius theorematis multo luculentius elucet, etiamsi criteriis rigidae demonstrationis destituatur: neque dubitavi, quin iisdem vestigiis insistuendo 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 penetraverit, quam Fermatius, omnis opera in hac scientia ulterius excolenda frustra impendi videtur, nisi ante, quae ab hoc excellenti Viro iam fuerunt investigata, quasi de novo 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, instituam, duas propositiones in subsidium vocari oportet, quarum demonstrationem iam alibi dedi. Altera est, quod omnes numeri, qui sunt divisores 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 $aa + bb$ divisor fit 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 fit numerus primus, atque a et b numeri quicunque per p non divisibiles, erit semper $a^{p-1} - b^{p-1}$ per numerum primum p divisibilis: demonstrationem huius rei iam dudum in Comment. Acad. Petrop. Tom. VIII dedi.

3. Quodsi iam $4n + 1$ fit numerus primus, per eum omnes numeri in hac forma $a^{4n} - b^{4n}$ contenti erunt divisibiles, siquidem neuter numerorum a et b seorsim per $4n + 1$ fuerit divisibilis. Quare si a et b sint numeri minores, quam $4n + 1$, (cyphra tamen excepta), numerus inde formatus $a^{4n} - b^{4n}$ sine ulla limitatione per numerum primum propositum $4n + 1$ erit divisibilis. Cum autem $a^{4n} + b^{4n}$ [Ed: Believed to be $a^{4n} - b^{4n}$.] fit productum horum factorum $a^{2n} + b^{2n}$ et $a^{2n} - b^{2n}$, necesse est, ut alteruter horum factorum fit per $4n + 1$ divisibilis; fieri enim nequit, ut vel neuter, vel uterque simul divisorem habeat $4n+1$. Quodsi iam demonstrari posset, dari casus, quibus forma $a^{2n} + b^{2n}$ fit divisibilis per $4n + 1$, quoniam $a^{2n} + b^{2n}$, ob exponentem $2n$ parem, est summa duorum quadratorum, quorum neutrum seorsim per $4n + 1$ divisibile existit, inde sequeretur, hunc numerum $4n + 1$ esse summam

duorum quadratorum.

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

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

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

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

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

per $4n + 1$ essent divisibiles, etiam differentiae huius progressionis, quae sunt differentiae

††Ed: Believed to be $2^{2n} - 1,\ 3^{2n} - 2^{2n},\ 4^{2n} - 3^{2n},\ 5^{2n} - 4^{2n},\ \ldots\ (4n)^{2n} - (4n-1)^{2n}$

secundae illius seriei per $4n+1$ essent divisibiles: atque ob eandem rationem differentiae tertiae, quartae, quintae etc. omnes forent per $4n+1$ divisibiles; ac denique etiam differentiae ordinis $2n$, qui sunt, ut constat, omnes inter se aequales. Differentiae autem ordinis $2n$ sunt $= 1.\ 2.\ 3.\ 4.\ \ldots\ 2n$,[‡‡] quae ergo per numerum primum $4n+1$ non sunt divisibiles, ex quo vicissim sequitur, ne omnes quidem differentias primas per $4n+1$ esse divisibiles.

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, ut binorum quorumvis differentiae per $4n+1$ divisibiles esse debeant, si theorematis veritas negetur. Sin autem plures termini ad hanc differentiam ultimam constituendam concurrerent, iique ultra 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 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 $4n+1$ divisibiles, atque ita quidem, ut a non fit maior, quam $2n+1$. Hinc autem porro recte infertur, summam $a^{2n} + (a-1)^{2n}$, ideoque summam duorum quadratorum per $4n+1$ necessario esse divisibilem: 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

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

[‡‡]Ed: $1.2.3 \ldots 2n = 1 \cdot 2 \cdot 3 \ldots (2n) = (2n)!$ throughout the paper.

unde differentiae primae erunt:

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

cuius progressionis terminorum numerus est $= 2n$. Ex demonstratione itaque praecedente patet, non omnes terminos huius progressionis differentiarum esse per numerum primum $4n+1$ divisibiles; neque tamen hinc intelligimus, quot et quinam sint illi termini, per $4n+1$ non divisibiles. Ad demonstrationem enim sufficit, si vel unicus terminus, quisquis ille fit, per $4n+1$ non sit divisibilis. Quodsi autem casus speciales evolvamus, quibus $4n+1$ est numerus primus ex differentiis istis, quarum numerus est $= 2n$, reperiemus, semper semissem esse per $4n+1$ divisibilem, alterum vero semissem non divisibilem: quae observatio etsi ad vim demonstrationis non spectat, tamen ad eam illustrandam non parum confert, quare aliquot casus speciales ad examen revocasse iuvabit.

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 divisibilis per 5, altera vero est divisibilis. Pro reliquis casibus utamur signo d ad eas differentias indicandas, quae sunt divisibiles, at signo o eas notemus, quae non sunt divisibiles, quae signa differentiis pro quovis casu, subscribamus:

Differentiae

$4n+1$								
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 divisibiles et non divisibiles nulla certa lege contineri, etiamsi utrique sint multitudine pares: tamen per se est perspicuum, ultimum terminum $(2n+1)^{2n} - 2n^{2n}$ semper per $4n+1$ esse divisibilem, quia factorem habet $(2n+1)^2 - 4nn = 4n+1$: at de reliquis nihil certi statui potest.

9. Porro quoque ad vim demonstrationis penitius perspiciendam notari oportet, demonstrationem tum solum locum habere, si numerus $4n+1$ fit primus; prorius uti natura theorematis postulat. Nam si $4n+1$ non esset numerus primus, neque de eo affirmari posset, quod sit summa duorum quatratorum, neque forma $a^{4n} - b^{4n}$ per eum esset necessario divisiblis. Quin etiam ultima conclusio foret salsa, qua pronunciavimus, differentias illas ordinis $2n$, quae sunt $= 1.\ 2.\ 3.\ 4.\ \ldots\ 2n$, 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 $1.\ 2.\ 3.\ 4.\ \ldots\ 2n$ hos factores contineret, foretque idcirco per $4n+1$ divisibile. At si $4n+1$ est numerus primus, tum demum affirmare licet, productum $1.\ 2.\ 3.\ 4.\ \ldots\ 2n$ plane non esse per $4n+1$ divisibile: quia hoc productum per nullos alios numeros dividi 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 $= 1.\ 2.\ 3.\ 4.\ \ldots\ 2n$, hoc uberius 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, fit $= Ax^m + Bx^{m-1} + Cx^{m-2} + Dx^{m-3} + Ex^{m-4} + \text{etc.}$ hanc seriem ad gradum m referri, quia m est exponens maximae potestatis ipsius x. Deinde si

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 serei 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. Unde 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

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

eius 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 $(x+2)^m - (x+1)^m$ subractus 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 fit 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

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

13. Evolvamus 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 $= 2^1 - 1.1 = 1$. 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 $2^2 - 2.1^2 = 2(2^1 - 1.1^1)$, unde 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. †

Ubi 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

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

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

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

$\frac{m(m-1)(m-2)}{1.\ 2.\ 3}(m-2)^m : \frac{(m+1)m(m-1)}{1.\ 2.\ 3}(m-2)^{m+1} = 1 : m+1;$

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 $= 1.2$
$1;\ 2^3;\ 3^3;\ 4^3;\ 5^3;$ 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 demonstravimus, seriei potestatum $1;\ 2^{2n},;\ 3^{2n};\ 4^{2n};\ 5^{2n};$ etc. differentias ordinis $2n$ non solum esse constantes, sed etiam aequari producto $1.\ 2.\ 3.\ \ldots\ 2n$, uti in demonstratione theorematis propositi assumsimus.

†Believed to be $Q = (m+1)^{m+1} - (m+1)(m)^{m+1} + \frac{(m+1)m}{1.\ 2}(m-1)^{m+1} - \frac{(m+1)m(m-1)}{1.\ 2.\ 3}(m-2)^{m+1} +$ etc.

THEOREMA 1.

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

DEMONSTRATIO

Si enim quispiam numerus quadratus aa fuerit per numerum primum p divisibilis, qui ex factoribus a et a constat, necesse est, ut alteruter factor per p fit divisibilis, quare numerus quadratus aa per numerum primum p divisibilis esse nequit, nisi eius radix a fit divisibilis per p.

COROLL. 1

2. Numeri ergo quadrati per numerum primum p divisibiles 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 divisibiles.

PROPOSITION: Let m and n be natural numbers with $0 \leq n \leq m$. Then

$$\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^n = \begin{cases} 0 \text{ if } 0 \leq n < m, \text{ and} \\ \\ m! \text{ if } n = m. \end{cases}$$

COROLLARY: Let m be a natural number. Then

$$\sum_{k=0}^{m}(-1)^{k}\binom{m}{k}(m-k)^m = m!.$$

PROOF OF PROPOSITION: The Binomial Theorem states that

$$(1+x)^m = \sum_{k=0}^{m}\binom{m}{k}x^k. \tag{1}$$

Substituting $x = -1$ yields

$$0 = \sum_{k=0}^{m}\binom{m}{k}(-1)^k = \sum_{k=0}^{m}\binom{m}{m-k}(-1)^{m-k} = \sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k},$$

the $n = 0$ case. Differentiating (1) yields

$$m(1+x)^{m-1} = \sum_{k=1}^{m}k\binom{m}{k}x^{k-1} = \sum_{k=0}^{m}k\binom{m}{k}x^{k-1}.$$

Substituting $x = -1$ yields

$$0 = \sum_{k=0}^{m}k\binom{m}{k}(-1)^{k-1} \Rightarrow \sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k = 0.$$

One more derivative of (1) yields

$$m(m-1)(1+x)^{m-2} = \sum_{k=1}^{m}k(k-1)\binom{m}{k}x^{k-2},$$

and by substituting $x = -1$ we learn that

$$\begin{aligned} 0 &= \sum_{k=0}^{m} k(k-1)\binom{m}{k}(-1)^{k-2} \\ &= \sum_{k=0}^{m} k^2\binom{m}{k}(-1)^{m-k} - \sum_{k=0}^{m} k\binom{m}{k}(-1)^{m-k} \\ &= \sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^2. \end{aligned}$$

Continuing in this fashion yields

$$\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^n = 0$$

for $0 \leq n < m$. When $n = m$, after differentiating m times we have

$$m!(1+x)^0 = \sum_{k=0}^{m}\binom{m}{k}k!x^{k-m} \Rightarrow$$

$$\begin{aligned} m!(1+x)^0 &= \sum_{k=0}^{m}\binom{m}{k}k(k-1)(k-2)\ldots(3)(2)(1)x^{k-m} \Rightarrow \\ m! &= \sum_{k=0}^{m}\binom{m}{k}k(k-1)(k-2)\ldots(3)(2)(1)(-1)^{k-m} \end{aligned}$$