Proof of a theorem of Fermat that every prime number of the form $4n + 1$ is a sum of two squares *

Leonhard Euler

1. When I recently [1] considered these numbers which arise from the addition of two squares, I proved many properties which such numbers are endowed with: it was not permitted to prolong adequately my thoughts about this so that I could show for certain the truth of this theorem, which Fermat once proposed to be proved via geometry. Nevertheless, I then published an attempt at the proof, from which the certainty of this theorem shines much brighter, although it is lacking, according to the criteria of a rigorous proof: I did not doubt that by continuing in the same path, the desired proof could more easily be obtained, which indeed since that time came to me with experience, so that the attempt, if some other slick idea appears, may become a rigorous proof. Indeed, I can boast of having provided nothing new about this subject, because Fermat himself already claimed to have elicited a proof of this theorem, but in fact did not make it public anywhere, just as with the many other exceptional discoveries of this man, so that what now at last from these lost things we recover, as it were, these things not unjustly are regarded as new discoveries. Because certainly no one ever so successfully delved into the arcana of numbers as Fermat, all additional work in this science to be developed appears to be spent in vain, except previously, which things from this excellent man are now investigated, as if they are brought to light anew. Although after him, many learned men in this field of studies have exerted their own efforts, still generally nothing has followed which can be compared with the ingenuity of this man.

2. As for the proof of the theorem, which I consider here, I have arranged two propositions it is necessary to call upon for assistance, the proof of which I have already given elsewhere. The first is that all numbers which are divisors of sums of two squares prime between themselves are themselves sums of two squares;

*Originally published as *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum*, Novi Commentarii academiae scientiarum Petropolitanae **5** (1760), pp. 3–13. E241 in the Eneström index. Translated from the Latin by Paul R. Bialek, Department of Mathematics, Trinity International University, Deerfield, Illinois, email: pbialek@tiu.edu

[1] Translator: Euler is referring to E228, *De numeris, qui sunt aggregata duorum quadratorum.*

thus, if a and b are numbers prime between themselves, and d is a divisor of a number of the form $aa+bb$, then d will also be a sum of two squares; I have given a proof of this theorem in a work mentioned earlier, in which I consider numbers which are sums of two squares. The first proposition which the following proof requires is that if p is a prime number and a and b are any numbers not divisible by p, then $a^{p-1} - b^{p-1}$ will always be divisible by the prime number p; I have already given the proof of this result in *Commentarii Academiae Petropolitanae, Volume VIII.*

3. So if $4n+1$ is a prime number, all numbers contained in the form $a^{4n} - b^{4n}$ will be divisible by it, as long as neither of the numbers a or b is divisible by $4n+1$. Therefore, if a and b are numbers less than $4n+1$ but not equal to 0, then a number of the form $a^{4n} - b^{4n}$ will be divisible by the given prime number $4n+1$ without any limitation. Because $a^{4n} - b^{4n}$ is a product of the factors $a^{2n} + b^{2n}$ and $a^{2n} - b^{2n}$, it is necessary that one of the two factors is divisible by $4n+1$; in other words, it cannot be that neither or both have $4n+1$ as a divisor. For if indeed it can be shown to be the case in which the form $a^{2n} + b^{2n}$ is divisOKible by $4n+1$, since $a^{2n} + b^{2n}$, on account of its even exponent $2n$, is a sum of two squares, neither of which is divisible by $4n+1$, from this it follows that the number $4n+1$ is a sum of two squares.

4. Certainly the sum $a^{2n} + b^{2n}$ will be divisible by $4n+1$ whenever the difference $a^{2n} - b^{2n}$ is not divisible by this same number. Therefore, anyone who will say that the prime number $4n+1$ is not a sum of two squares is forced to deny that any number of the form $a^{2n} + b^{2n}$ is divisible by $4n+1$. Thus, one should affirm the same, namely, that all numbers contained in the form $a^{2n} - b^{2n}$ are divisible by $4n+1$, as long as neither a nor b is divisible by $4n+1$. Accordingly, it is to be proved here by me that not all numbers contained in the form $a^{2n} - b^{2n}$ are divisible by $4n+1$; indeed, in this, if I will have succeeded. it will certainly be the case, if numbers are substituted for a and b for which the form $a^{2n} - b^{2n}$ is not divisible by $4n+1$; then, in those cases, the other form $a^{2n} + b^{2n}$ will necessarily be divisible by $4n+1$. From this, because a^{2n} and b^{2n} are squares, that which is proposed will have been finished, namely, that the number $4n+1$ is a sum of two squares.

5. Therefore, so that I may prove that not all numbers contained in the form $a^{2n} - b^{2n}$, in other words, not all differences between two powers with exponent $2n$, are divisible by $4n+1$, I will consider the series of powers from 1 up to what is formed from the base $4n$: $1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}, 6^{2n}, \ldots, (4n)^{2n}$. And now I declare that not all differences between two terms of this series are divisible by $4n+1$. For instance, if the terms of the first difference, $2^{2n}-1, 3^{2n}-2^{2n}, 4^{2n}-3^{2n}, 5^{2n}-4^{2n}, \ldots, (4n)^{2n}-(4n-1)^{2n}$ were divisible by $4n+1$, then the differences of the progression which are the second differences of that series would also be divisible by $4n+1$; and by the same reasoning, third differences, fourth, fifth, etc. would all be divisible by $4n+1$, and, finally, also differences of order $2n$, which, as they are constant, are all equal to each other. However, the differences of order $2n$ are equal to $1 \cdot 2 \cdot 3 \cdot 4 \cdots 2n$, which therefore are

not divisible by the prime number $4n+1$, from which it follows in turn that certainly not all first differences are divisible by $4n+1$.

6. By virtue of which, the power of this proof is better observed, it is to be noted that the difference of order $2n$ is produced from $2n+1$ terms of the given series, which, if they are taken from the beginning, are all so collected that differences of whichever pairs should be divisible by $4n+1$ if the truth of the theorem is negated. But if more terms from this last constituted difference were assembled, and they were to proceed beyond the term $(4n)^{2n}$, seeing that the differences arising from the following term $(4n+1)^{2n}$ do not relate to the statement of the theorem, the proof would retain no validity. However, because the last difference which we are considering depends only on $2n+1$ terms, the conclusion which we deduced from it is entirely legitimate. And from this it follows that the first differences will be like $a^{2n}-(a-1)^{2n}$, which is not divisible by $4n+1$, and in such a way that a is not greater than $2n+1$. However, later the sum $a^{2n}+(a-1)^{2n}$, is properly obtained, and therefore the sum of two squares is necessarily divisible by $4n+1$, and thus the prime number $4n+1$ is a sum of two squares.

7. Since the difference of order $2n$ depends on $2n+1$ terms from a series of powers, let us consider only that many terms taken from the beginning of $1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n},\ 6^{2n},\ \ 2n^{2n},\ (2n+1)^{2n}$, from which the first differences will be $2^{2n}-1,\ 3^{2n}-2^{2n},\ 4^{2n}-3^{2n},\ 5^{2n}-4^{2n},\ \ldots,\ (2n+1)^{2n}-(2n)^{2n}$, in which the number of terms in the progression is $2n$. And so, from the preceding demonstration it is evident that not all terms in this progression of differences are divisible by the prime number $4n+1$. If however we examine the special cases in which $4n+1$ is a prime number, from those differences, of which there are $2n$, we will always discover that half are divisible by $4n+1$, and the other half are, of course, not divisible. Even if this observation does not seem to have the strength of a proof, it nevertheless does not oppose at all what is to be explained. Therefore, it will be helpful to re-examine some special cases.

8. The smallest prime number of the form $4n+1$ is 5, which arises if $n=1$. From this will be obtained the two differences 2^2-1 and 3^2-2^2, of which the former is not divisible by 5, but the other is so divisible. For the remaining cases, I use d to indicate the differences which are divisible, [2] and 0 those which are not divisible, the signs of which we write below the differences, according to the case.

[2]Translator: By $4n+1$.

$4n+1$	Differences					
13	$2^6-1,$	$3^6-2^6,$	$4^6-3^6,$	$5^6-4^6,$	$6^6-5^6,$	7^6-6^6
	0	0	d	0	d	d
17	$2^8-1,$	$3^8-2^8,$	$4^8-3^8,$	$5^8-4^8,$	$6^8-5^8,$	$7^8-6^8,$
	d	0	0	0	d	d
	$8^8-7^8,$	9^8-8^8				
	0	d				
29	$2^{14}-1,$	$3^{14}-2^{14},$	$4^{14}-3^{14},$	$5^{14}-4^{14},$	$6^{14}-5^{14},$	$7^{14}-6^{14},$
	0	d	0	d	d	d
	$8^{14}-7^{14},$	$9^{14}-8^{14},$	$10^{14}-9^{14},$	$11^{14}-10^{14},$	$12^{14}-11^{14},$	$13^{14}-12^{14},$
	0	0	0	d	d	0
	$14^{14}-13^{14},$	$15^{14}-14^{14}$				
	0	d				

From this it is evident that the divisible terms and the non-divisible terms are not restricted by a fixed law, although the two are equal in multitude; nevertheless, it is evident that the last term $(2n+1)^{2n}-(2n)^{2n}$ is always divisible by $4n+1$, because it has the factor $(2n+1)^2-4nn=4n+1$. But nothing certain can be determined about the others.

9. Moreover, as to the validity of this proof, it should be carefully observed that that the proof to be examined is appropriate only if the number $4n+1$ is prime, as the nature of the theorem certainly demands it. For if $4n+1$ were not prime, it could not be asserted that it is a sum of two squares, nor that the form $a^{4n}-b^{4n}$ is necessarily divisible by it. Rather, the last conclusion which we announced would be false, and those differences of order $2n$, which are $1\cdot 2\cdot 3\cdot 4\cdots 2n$, are not divisible by $4n+1$. If however $4n+1$ were not a prime number but had factors which were less than $2n$, then certainly the product $1\cdot 2\cdot 3\cdot 4\cdots 2n$ would contain those factors and for that reason would be divisible by $4n+1$. But if $4n+1$ is a prime number, then in fact one can assert that the product $1\cdot 2\cdot 3\cdot 4\cdots 2n$ is clearly not divisible by $4n+1$, because this product can be divided by no other numbers unless they arise as factors in the product.

10. Finally, because this proof to be set forth rests on this foundation, that of the series of powers $1, 2^{2n}, 3^{2n}, 4^{2n}$, etc., the differences of order $2n$ are constant and all equal $1\cdot 2\cdot 3\cdot 4\cdots 2n$; this can be seen more fully explained even if it is found soundly exposited here and there in books of analysis. Therefore, first it is to be noted that if the general term of any series or, in other words, that which corresponds to an indefinite exponent of x, is $Ax^m+Bx^{m-1}+Cx^{m-2}+Dx^{m-3}+Ex^{m-4}+$ etc., then this series is said to be of degree m because m is the exponent of the highest power of x. Then, if this general term is subtracted from the following $A(x+1)^m+B(x+1)^{m-1}+C(x+1)^{m-2}+$ etc., the general term will produce a series of differences in which the highest power of x will be $m-1$ and therefore the series of differences will be of a lower degree, $m-1$. In a similar way, from the general term of the series of first differences is collected

a general term of the series of second differences which, again, has an even lower degree, $m-2$.

11. So if the given series is said to be of degree m, the series of first differences will be of degree $m-1$, the series of second differences will in turn be of degree $m-2$, the series of third differences of degree $m-3$, the series of fourth differences will be of degree $m-4$, and in general the series of nth order differences will be of degree $m-n$. From this, the series of mth order differences will attain degree $m-m=0$, and therefore its general term, because the highest power of x is $x^0=1$, will be a constant quantity, and therefore all differences of order m will be equal to each other. Hence, for series of first degree in which the general term is $Ax+B$, the first differences will be equal to each other, while for series of second degree, which are restricted to the general term Ax^2+Bx+C, the second differences are equal, and so in turn.

12. If, therefore, we consider any series of powers

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

for which the general term is x^m or, in other words, that which corresponds to a base of x, the series of differences of order m will be constant from terms equal to each other. Now the general term of a series of first differences will be

$$(x+1)^m - x^m,$$

which, subtracted from the following

$$(x+2)^m - (x+1)^m$$

will give the general term of the series of second differences, which will be

$$(x+2)^m - 2(x+1)^m + x^m.$$

Thus, in turn, the general term of the series of third differences will be

$$(x+3)^m - 3(x+2)^m + 3(x+1)^m - x^m;$$

and finally the general term of the series of differences of order m is

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

which, because they are constant quantities, will be the same for whatever number is substituted for x; therefore it will be either

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

or

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

where in the former formula we set $x = 0$ and, in the latter, $x = 1$.

13. Let us now consider the special cases of this series and let us ascend from the lowest powers to the highest. And first with m set equal to 1, the general term of the first differences of the series 1, 2, 3, 4, 5, 6, etc. will be

$$\text{either} \quad 1^1 - 1 \cdot 0^1 = 1 \quad \text{or} \quad 2^1 - 1 \cdot 1^1 = 1.$$

If $m = 2$, the second differences of the series $1, 2^2, 3^2, 4^2, 5^2$, etc. are

$$\text{either} \quad 2^2 - 2 \cdot 1^2 \quad \text{or} \quad 3^2 - 2 \cdot 2^2 + 1 \cdot 1^2;$$

but $2^2 - 2 \cdot 1^2 = 2(2^1 - 1 \cdot 1^1)$, from which these second differences are $2 \cdot 1$.

Let $m = 3$; the third differences of the series $1, 2^3, 3^3, 4^3, 5^3$, etc. will be

$$\text{either} \quad 3^3 - 3 \cdot 2^3 + 3 \cdot 1^3 \quad \text{or} \quad 4^3 - 3 \cdot 3^3 + 3 \cdot 2^3 - 1 \cdot 1^3;$$

but

$$3^3 - 3 \cdot 2^3 + 3 \cdot 1^3 = 3(3^2 - 2 \cdot 2^2 + 1 \cdot 1^2) = 3 \cdot 2 \cdot 1,$$

because from the preceding case,

$$3^2 - 2 \cdot 2^2 + 1 \cdot 1^2 = 2 \cdot 1.$$

In a similar fashion, if $m = 4$, the fourth differences of the series $1, 2^4, 3^4, 4^4, 5^4$, etc. will be

$$\text{either} \quad 4^4 - 4 \cdot 3^4 + 6 \cdot 2^4 - 4 \cdot 1^4 \quad \text{or} \quad 5^4 - 4 \cdot 4^4 + 6 \cdot 3^4 - 4 \cdot 2^4 + 1 \cdot 1^4;$$

but

$$4^4 - 4 \cdot 3^4 + 6 \cdot 2^4 - 4 \cdot 1^4 = 4(4^3 - 3 \cdot 3^3 + 3 \cdot 2^3 - 1 \cdot 1^3) = 4 \cdot 3 \cdot 2 \cdot 1.$$

14. In order that this progression might be more easily observed, let the differences of order m of the series $1, 2^m, 3^m, 4^m, 5^m$, etc. equal P, and let the differences of order $m+1$ of the series $1, 2^{m+1}, 3^{m+1}, 4^{m+1}, 5^{m+1}$, etc. equal Q.

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

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

where we expressed P in the former form and Q in the latter form. Here it is evident that the number of terms is equal in each expression, and individual

terms of the expression P are to the individual terms of the expression Q as 1 is to $m+1$. For instance,

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

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

$$\frac{m(m-1)}{1\cdot 2}(m-1)^m : \frac{(m+1)m}{1\cdot 2}(m-1)^{m+1}$$

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

On account of this,

$$P : Q = 1 : m+1$$

and thus $Q = (m+1)P$.

15. From this it is evident that

for the series	the differences
1, 2, 3, 4, 5, etc.	first $= 1$,
$1, 2^2, 3^2, 4^2, 5^2$, etc.	second $= 1\cdot 2$
$1, 2^3, 3^3, 4^3, 5^3$, etc.	third $= 1\cdot 2\cdot 3$
$1, 2^4, 3^4, 4^4, 5^4$, etc.	fourth$= 1\cdot 2\cdot 3\cdot 4$
$1, 2^m, 3^m, 4^m, 5^m$, etc.	of order $m = 1\cdot 2\cdot 3\cdot 4\cdots m$

and therefore,

$1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}$, etc. of order $2n = 1\cdot 2\cdot 3\cdot 4\cdots 2n$.

And thus we have also proved that the differences of order $2n$ in the series of powers $1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}$, etc. are not only constant but also equal to the product $1\cdot 2\cdot 3\cdot 4\cdots 2n$, which we assumed in the proof of the proposed theorem.[3]

Theorem 1

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

Proof

[3]The *Opera Omnia* edition of the paper (*Opera Omnia*: Series 1, Volume 2, pp. 328-337) does not have the following material, but the material appeared in the original publication in *Novi Commentarii academiae scientiarum Petropolitanae* 5, 1760, pp. 3-13.

If for example some square number aa were divisible by the prime number p, because it consists of the factors a and a, it would be necessary for one or the other factor to be divisible by p. Therefore, the square number aa cannot be divisible by the prime number p unless its root a is divisible by p.

Corollary 1

2. Thus, the square numbers arising from the roots $p, 2p, 3p, 4p$, etc., namely, $pp, 4pp, 9pp, 16pp$, etc. are divisible by the prime number p, and all other square numbers will not be divisible by the prime number p.