



M. F. Gilmullin, "Fermat's Christmas Theorem," *Mathematics with Mansur*, Dec. 21, 2024. [Online]. Available: <https://history-math.org/publications/hm-tt-4c57329c14a2-en/>.

ESSAY

Fermat's Christmas Theorem

The history of mathematics contains many remarkable achievements and problems associated with Pierre de Fermat, its "great amateur".

Mansur Gilmullin · 21.12.2024 · EN

[Read this article on the journal website](#)



· [Source](#)

The history of mathematics contains many remarkable achievements and problems associated with its "great amateur", [Pierre de Fermat](#) (1601–1665), a founder of algebraic number theory and a lawyer from Toulouse. One of these is the remarkable "Fermat's Christmas theorem".



Portrait of Pierre de Fermat (1601–1665), a self-taught French mathematician and a founder of algebraic number theory · [Source](#)

It states:

“Every prime p of the form $p = 4n + 1$, where n is a positive integer, can be expressed as the sum of the squares of two positive integers.”

In other words, there are positive integers x and y such that $p = x^2 + y^2$.

Other names for it are the “Fermat–Euler theorem” and the “theorem on expressing primes as the sum of two squares”.

Examples

$$5 = 1^2 + 2^2$$

$$13 = 2^2 + 3^2$$

$$17 = 1^2 + 4^2$$

$$29 = 2^2 + 5^2$$

$$37 = 1^2 + 6^2$$

The result is called “Fermat’s Christmas theorem” because it became known through a letter Pierre de Fermat sent on 25 December 1640.

That is what mathematicians do at Christmas!

Historical background

The statement first appeared in the work of the Dutch mathematician Albert Girard in 1632. In his letter to Mersenne in 1640, Pierre de Fermat announced that he had proved the theorem, but supplied no proof. In a letter to Pierre de Carcavi in August 1659, 20 years later, Fermat hinted that the proof used the method of infinite descent.

The first published proof by infinite descent was found by Leonhard Euler between 1742 and 1747, 100 years later. Joseph Lagrange, Carl Gauss, Hermann Minkowski and Don Zagier subsequently gave proofs based on other ideas. The result therefore proved to be less than obvious.

Using Brahmagupta's identity, one can derive a more general statement from "Fermat's Christmas theorem":

A positive integer can be expressed as a sum of two integer squares if and only if no prime of the form $4n + 3$ occurs to an odd power in its prime factorisation.

Sometimes it is this result that is meant by the Fermat–Euler theorem.

Notes

Infinite descent is a method of proof by contradiction based on the fact that the positive integers are well ordered. Pierre de Fermat developed it substantially.

It is often used to prove that an equation has no solutions, as follows. Assuming a solution exists, one proves that another solution exists which is smaller in some sense. This produces an infinite chain of solutions, each smaller than the last. That contradicts the fact that every nonempty subset of the positive integers has a least element. The assumption that an initial solution exists must therefore be false.

Example. The irrationality of the square root of 2 can be proved by infinite descent, beginning with the assumption that it is rational.

The Brahmagupta–Fibonacci identity, also called Brahmagupta's identity or the Diophantus identity, is an algebraic identity showing how a product of two sums of squares can itself be expressed as a sum of squares, in two ways:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2$$

More information about "Fermat's Christmas theorem", including its proofs, can be found in the following works:

1. Buchstab, A. A. *Number Theory*. — Moscow: Prosveshchenie, 1966. — 384 pp.
2. Merzon, G. "Fermat's Christmas Theorem and Spivak's Winged Squares" // *Kvantik*. — 2022. — No. 5. — Pp. 14–22.
3. Senderov, V., and Spivak, A. "Sums of Squares and Gaussian Integers" // *Kvant*. — 1999. — No. 3. — Pp. 14–22.
4. Dickson L. E. History of the Theory of Numbers // Vol. II. — Ch. VI. Sum of two squares.