Fermat's Christmas Theorem

David Meyer

dmm@{1-4-5.net,uoregon.edu}

Last update: December 26, 2020

Fermat's Christmas Theorem

Fermat's Christmas Theorem [1] is a beautiful and simply stated theorem. It is called Fermat's Christmas Theorem because Fermat announced a proof of the theorem in a letter to Mersenne dated December 25, 1640. And of course, Fermat didn't include a proof in the letter.

Fermat's Christmas Theorem (aka Fermat's theorem on sums of two squares) states that an odd prime number p can be expressed as

$$p = r^2 + s^2$$

where $r, s \in \mathbb{N}$, if and only if $p \equiv 1 \pmod 4$. That is, the theorem holds iff $p = 4n + 1$ for some $n \in \mathbb{N}$.

For example, the primes 5, 13, 17, 29, 37 and 41 are all congruent to 1 modulo 4 and can be expressed as sums of two squares in the following ways:

$$\begin{aligned}
5 &= 1^2 + 2^2 \\
13 &= 2^2 + 3^2 \\
17 &= 1^2 + 4^2 \\
29 &= 2^2 + 5^2 \\
37 &= 1^2 + 6^2 \\
41 &= 4^2 + 5^2
\end{aligned}$$

On the other hand, the primes 3, 7, 11, 19, 23 and 31 are all congruent to 3 modulo 4 and none of them can be expressed as the sum of two squares. This is the easier part of the theorem since it follows immediately from the observation that all squares are congruent to 0 or 1 modulo 4.

The prime numbers p for which Fermat's Christmas Theorem is true are called Pythagorean primes. See [3] for more on Pythagorean primes.

A variety of proofs of Fermat's Christmas Theorem can be found in [2].

References

[1] Wikipedia contributors. Fermat's theorem on sums of two squares — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Fermat%27s_theorem_on_sums_of_two_squares&oldid=990575323`, 2020. [Online; accessed 26-December-2020].

[2] Wikipedia contributors. Proofs of fermat's theorem on sums of two squares — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares&oldid=989540767`, 2020. [Online; accessed 27-December-2020].

[3] Wikipedia contributors. Pythagorean prime — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Pythagorean_prime&oldid=985939468`, 2020. [Online; accessed 26-December-2020].