Introduction

2025-11-29

Some history

On Christmas day (25 December 1640), Pierre de Fermat wrote a letter to Marin Mersenne where he stated that every prime number of the form $4n + 1$ could be written as the sum of two squares. He claimed to have an irrefutable proof of the statement.

The result was already conjectured by Albert Girard, but the first complete proof was given by Leonhard Euler, who announced it in a letter sent to Christian Goldbach.

Today the theorem is known as "Fermat's theorem on sums of two squares" or "Fermat's Christmas Theorem", because of the date in which Fermat claimed to have the proof.

Detailed historical information can be found in the relevant chapter of Dickinson (1938).

Random thoughts sometimes are nice

We're bored, so we start writing some useless calculations in our notebook. We really like prime numbers (we'll explain why later in the posts), so we start by writing a few of them:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 \ldots \tag{1}$$

Since we have nothing better to do, we start asking some questions about them, like:

- how many prime numbers are there?
- which numbers could be expressed as the product of prime numbers?

We like these questions (and will answer them in the next few posts), but in the process we ask a more subtle one:

Question: When can we write a prime number p as the sum of two squares? In other words, when can we write

$$p = a^2 + b^2$$

with a and b are integers?

We try to approach the problem by trial and error to understand it better.

- Consider the prime number 2. Can we write it as the sum of two squares? Well, there aren't many ways to write 2 as a sum of two integers:

  $$2 = 1 + 1$$

  But since $1^2 = 1$ we have

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

  therefore we can indeed write 2 as the sum of two squares.

- Let's try with 3: the only possible ways of writing 3 as a sum of two numbers are $3 = 1+2$ and $3 = 0 + 3$. However 2 and 3 are not squares, so 3 does not have the property.

- We move on to the number 5: we can write it as $5 = 2 + 3$, but since 2 and 3 are not squares, we have to search for another writing, that we find in $5 = 4 + 1$, since $4 = 2^2$ and $1 = 1^2$.

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

- What about 7? Well, we can write 7 as:

  - $7 = 0 + 7$, but 7 is not a square;
  - $7 = 1 + 6$, but 6 is not a square;
  - $7 = 2 + 5$, but neither 2 nor 5 are squares;
  - $7 = 3 + 4$, but 3 is not a square. therefore 7 cannot be written as the sum of two squares.

Continuing this process, we find that among the primes in the list above, those that satisfy the property are:

$$2, 5, 13, 17, 29, 37, 41 \ldots \tag{2}$$

We want to investigate further the properties of these primes. First, observe that we are only interested in odd primes (i.e., all primes other than 2), since we already know that 2 can be written as the sum of two squares. Therefore, we start to look at them carefully and conjecture the following fact:

> All *odd* primes that can be written as the sum of two squares have remainder 1 when divided by 4.

However, this only tells us that *if* an odd prime is a sum of two squares, then it leaves remainder 1 when divided by 4. But in general it's not easy to check whether a prime is the sum of two squares, since we'd have to try many possibilities (look at 7 and imagine larger primes). If we just want to know whether a prime has remainder 1 when divided by 4, we can compute that quickly and save time.

But maybe we didn't waste our time thinking about this problem. Since we can easily check what is the remainder of a prime when divided by 4, what if **we can write an odd prime as the sum of two squares each time it has remainder** 1 **in such a division?** That would be great: we could avoid long case checks and simply compute the remainder, like we learned in elementary school. Luckily, the theorem we want to focus on gives us the answer:

Theorem 0.1 (Fermat's Christmas Theorem)**.** *An odd prime number p can be written as the sum of two squares if and only if it has remainder* 1 *when divided by* 4*.*

Now we see why the theorem is nice: it simplifies a difficult problem (determining whether an odd prime is the sum of two squares) to a simple one (checking whether its remainder is 1 when divided by 4).

Some plan for the future

I chose to talk about this theorem because, to me, the most interesting part is its proof. As a math student I spend most of my time trying to understand proofs (for me, mathematics is mostly about them).

Maybe some of you are asking yourselves:

> What is a mathematical proof?

This isn't an easy question (it's rather philosophical). Anyway, we can think of a proof as an argument convincing us about the truth of some proposition. Probably not all the arguments I share will be full formal proofs, since I won't always be very formal. My goal is to convey the general ideas rather than the technical details. I hope the careful reader will forgive me if I sometimes prefer simplicity to rigor.

The aim is to help interested readers convince themselves of Fermat's Christmas Theorem and to explain some basic mathematical ideas along the way.

A rough plan for the proof will involve:

- talking about general properties of integers

- talking about modular arithmetic
- talking about Gaussian integers
- putting everything together

I hope you enjoy the process as much as I did the first time I learned these beautiful ideas.

See you soon!

Dickinson, L. J. 1938. *History of the Theory of Numbers*. New York: Chelsea Publishing Company.