Fermat's Two Squares Theorem

AKA Fermat's Christmas Theorem
A tour through two proofs

Dave Neary

April 2021

1. Fermat's statement of the Two Squares "Theorem"
2. Dedekind's proof using Gaussian integers
3. Zagier's "one-sentence proof"

Fermat's Christmas Theorem

2. Sur le sujet des triangles rectangles ([1]), voici mes fondements :

1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.

2° Le même nombre et son quarré sont chacun une fois la somme de deux quarrés ;

Original statement of "Fermat's Christmas Theorem"

Fermat wrote this statement, without proof, in a letter to Mersenne, dated December 25th, 1640.

Fermat's Christmas Theorem: Statement

"On the subject of right triangles, here are my findings:

- Ever prime number that is one more than a multiple of four can be written in exactly one way as the sum of two squares, and in one way as the hypotenuse of a right triangle
- The same number and its square can be written in exactly one way as the sum of two squares."

In modern terms: All primes of the form $4k + 1$ can be written as the sum of two squares of integers.

Which primes are sums of squares?

Primes	Sum of squares
2	$1^2 + 1^2$
3	—
5	$1^2 + 2^2$
7	—
11	—
13	$2^2 + 3^2$
17	$1^2 + 4^2$

First few primes

Can any primes of the form $4k-1$ be a sum of squares?

For all integers x, y:

$$x^2, y^2 \equiv 0 \text{ or } 1 \pmod 4$$

$$x^2 + y^2 \in \{0, 1, 2\} \pmod 4$$

Therefore:

$$x^2 + y^2 \not\equiv 3 \pmod 4$$

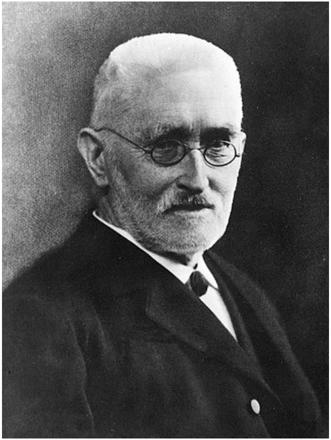
Leonhard Euler, 1747

Leonard Euler

The first published proof, using a method called "infinite descent" was published in 1747 by Leonhard Euler.

Proof 1: Dedekind's proof using Gaussian Integers

Richard Dedekind, 1894



Richard Dedekind, a German mathematician born in 1831. His domain of research was Number Theory, and his doctoral advisor was Carl Friedrich Gauss.
He published two proofs of Fermat's Two Squares Theorem using the ring of Gaussian integers, one in 1877, and this one, in 1894.

The Gaussian integers $\mathbb{Z}[i]$ is the set $\{a + ib : a, b \in \mathbb{Z}, i^2 = -1\}$
$\mathbb{Z}[i]$ is closed under multiplication and addition, and has additive and multiplicative identities.

- For $x, y \in \mathbb{Z}[i], x \times y, x + y \in \mathbb{Z}[i]$
- There exist elements $0, 1 \in \mathbb{Z}[i]$ such that, for all $x \in \mathbb{Z}[i], 0 + x = x, 1 \times x = x$

Factoring "primes"

An interesting characteristic of the Gaussian integers is that we can factor some expressions that do not have a factorization over the real numbers. For example:

$$a^2 + b^2 = (a + ib)(a - ib)$$

In this way, we can factor numbers that are prime in the natural numbers!

$$5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i)$$
$$13 = 2^2 + 3^2 = (2 + 3i)(2 - 3i)$$

By defining an appropriate "norm" function $N(x)$, we can also use the Euclidean division algorithm to find the GCD of elements of $\mathbb{Z}[i]$!

- Define the norm $N(a + ib) = a^2 + b^2$
- For all $x, y \in \mathbb{Z}[i]$, there exist $q, r \in \mathbb{Z}[i]$ such that $x = q \times y + r$, with $N(r) < N(y)$

We have a way to determine prime numbers for $\mathbb{Z}[i]$ that will be different from the primes we know in $\mathbb{N}$, and to express any Gaussian integer as a unique product of primes and units.

Let's find the GCD of $11 + 7i$ and $18 - i$ to see how it works.

$$\begin{aligned} N(11+7i) &= 11^2 + 7^2 = 170 \\ N(18-i) &= 18^2 + 1^2 = 325 \\ \frac{18-i}{11+7i} &= \frac{(18-i)(11-7i)}{(11+7i)(11-7i)} \\ &= \frac{205-137i}{170} \end{aligned}$$

We can round this to the nearest Gaussian integer $1 - i$ to get:

$$18 - i = (1-i)(11+7i) + 3i$$

Now we repeat the step to get:

$$\frac{11+7i}{3i} = \frac{7}{3} - \frac{11i}{3}$$

And we round to $2-4i$:

$$11+7i = (2-4i)(3i) + i$$

And since i is a unit, the greatest common denominator is 1.

In modular arithmetic, a quadratic residue is a number that has a square root $\pmod{p}$. For example, looking at the numbers $\pmod{7}$, we see that only 0, 1, 2, and 4 have square roots in $\mathbb{Z}/p\mathbb{Z}$, the numbers $\pmod{7}$:

a	$a^2 \pmod{7}$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Quadratic residues $\pmod{7}$

From Fermat's Little Theorem, we know that $a^{p-1} \equiv 1 \pmod{p}$ for all $a \neq 0 \pmod{p}$. We also can show that $(-1)^{\frac{p-1}{2}} = 1$ since $\frac{p-1}{2} = 2k$. Therefore, for a quadratic non-residue a, $(a^{\frac{p-1}{4}})^2 = -1 \pmod{p}$.
That means, we can find $a \in \mathbb{Z}/p\mathbb{Z}$ such that $p|a^2 + 1$, and factoring it over $\mathbb{Z}[i]$ we get:

$$a^2 + 1 = (a + i)(a - i)$$

But since $N(a + i) < N(p)$, p does not divide either of these factors - which means that p must be divisible by some other Gaussian prime factors $(n + im)(n - im) = p$.

Finding the squares (1)

We have proved that there must be some factors of p in $\mathbb{Z}[i]$, but we have not found them. The tricky part is finding a square root of -1. To do this, we look for a quadratic non-residue of p (look up "Euler's criterion", out of scope for this talk).

Let's try $p = 41 = 4(10 + 1)$ to see how it works.

$$3^4 = 81 \equiv -1 \pmod{41}$$

$$3^{20} = (-1)^5 \equiv -1 \pmod{41}$$

So 3 is a non-residue of 41. Now to find a square root of -1, find 3^{10}:

$$3^{10} = 9 \times (3^4)^2 \equiv 9 \pmod{41}$$

Therefore, 41 divides $9^2 + 1 = 82$

We know that $41|9^2+1=(9+i)(9-i)$. How we can find the prime factors of 41 using the Euclidean division algorithm with either of these factors:

$$\begin{aligned} \frac{41}{9-i} &= \frac{(41)(9+i)}{9^2+1^2} \\ &= \frac{1}{82}(369+41i) \\ 41 &= 4(9-i)+(5+4i) \\ 9-i &= (1-i)(5+4i) \end{aligned}$$

We have calculated that $5+4i$, is the GCD of 41 and $9-i$, and it is easy to check that $41=5^2+4^2$.

Don Zagier

In 1990, Don Zagier published a "one-sentence proof", based on a prior geometric proof.

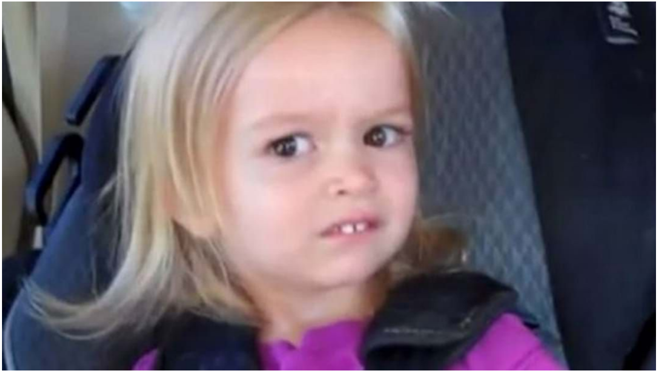
A one-sentence proof that every prime $p \equiv 1 \pmod 4$ *is a sum of two squares.*

The involution on the finite set
$S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by:

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point.

What!?!?!



What is an involution?

An *involution* is a function which is its own inverse. That is:

$$f : A \to A : f(f(x)) = x \text{ for all } x \in A$$

Examples:

- $f : \mathbb{R}^+ \to \mathbb{R}^+ : f(x) = \frac{1}{x}$
- $f : \mathbb{R}/\{-1\} \to \mathbb{R}/\{-1\} : f(x) = \frac{1-x}{1+x}$

Every involution on a finite set with an odd number of elements has at least one fixed point.
Involutions are "swapping" functions - if you have an odd number of elements, at least one of the elements must not get swapped.

What about $S = \{x^2 + 4yz = p\}$?

For any prime of the form $4k + 1$ we are guaranteed to find solutions of the form $x^2 + 4yz$ for $x, y, z \in \mathbb{N}$. One obvious solution: $x = 1, y = 1, z = k$.
For $p = 17$:

x	y	z
1	1	4
1	2	2
1	4	1
3	1	2
3	2	1

Possible values of x, y, z for $p = 17$

What about $S = \{x^2 + 4yz = p\}$?

For $p = 17$:

x	y	z
1	1	4
1	2	2
1	4	1
3	1	2
3	2	1

Possible values of x, y, z for $p = 17$

Notice that we get pairs of solutions when $y \neq z$ by swapping y and z.
Also, notice that the number of solutions is odd. If we can prove it is *always* odd, then we are guaranteed at least one solution with $y = z$.
If $y = z$, then $x^2 + 4yz = x^2 + (2y)^2$ is a sum of two squares, and the theorem is proved.

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

Where did this come from? What does it represent? How do we prove that it is an involution?

First, let's show that the cases are all that there are. By definition, $0 < x, y, z \in \mathbb{N}$. If $x = y - z$ then:

$$\begin{aligned} x^2 + 4yz &= (y - z)^2 + 4yz \\ &= y^2 + 2yz + z^2 \\ &= (y + z)^2 \end{aligned}$$

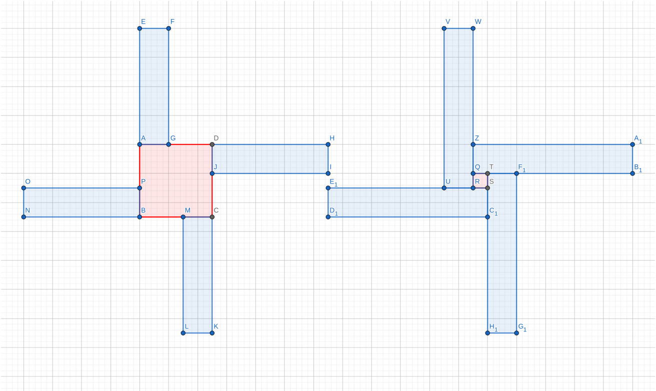
Similarly, if $x = 2y$, then:

$$\begin{aligned} x^2 + 4yz &= (2y)^2 + 4yz \\ &= 4y(y + z) \end{aligned}$$

In both cases, $x^2 + 4yz$ is not a prime.

Let's talk about windmills

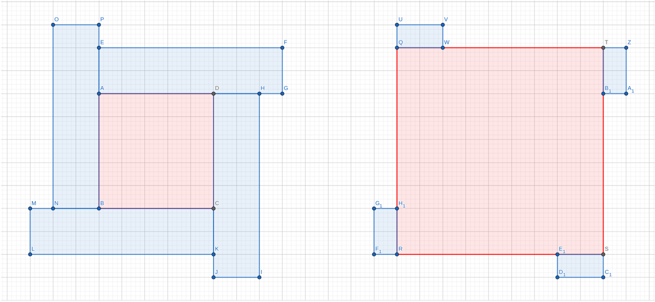
A geometric interpretation



$$(5, 2, 8) \to (1, 11, 2)$$

We interpret x as the side of a square, with y the base from the top left corner and z the height of 4 symmetrically arranged rectangles.

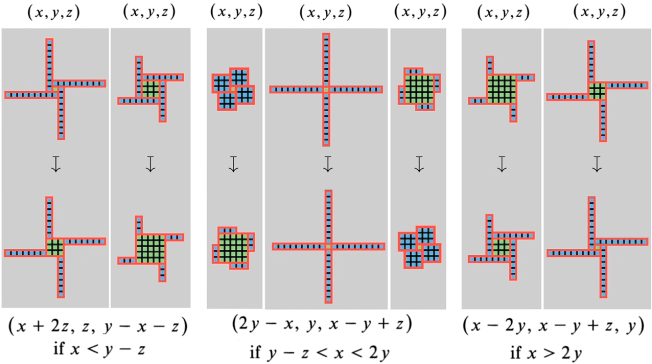
The translations from one arrangement to another represent the different ways to wrap rectangles around a square.



$$(5, 8, 2) \to (9, 2, 1)$$

A geometric interpretation

Each translation represents a different type of transformation which conserves the silhouette.



All the translations (and mappings) (thank you Mathologer)

In all of the shapes we have seen, there are two solutions with the same silhouette. Except one.
When $x = 1, y = 1, z = k$, we get a big "plus" sign. Since $y - z < x < 2y$ in this case:

$$(1, 1, k) \to (2 \times 1 - 1, 1, 1 - 1 + k) = (1, 1, k)$$

is a fixed point for the mapping, and it is guaranteed to be the only one!
Therefore, there will *always* be an odd number of solutions to $x^2 + 4yz = p$, and the alternative involution on the same set $(x, y, z) \to (x, z, y)$ *also* has a fixed point $y = z$.

Thank you! There's more! References

- I learned about this theorem from Mathologer's awesome video about Zagier's proof: Why was this visual proof missed for 400 years?
- You can get *all* the proofs of Fermat's two squares theorem (including a reference to a new proof from 2016!) on Wikipedia: Proofs of Fermat's theorem on sums of two squares
- If you're interested in some additional materials that use Gaussian integers, you might enjoy 3blue1brown's video on Pythagorean triples: All possible Pythagorean triples, visualized