Fermat's Two Squares Theorem

AKA Fermat's Christmas Theorem

A tour through two proofs

Dave Neary

April 2021

AoPS Academy
Lexington Campus

Outline

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:

- Every 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 $4k + 1$, and their squares, can be written as the sum of two squares of positive integers in exactly one way.

Which primes are sums of squares?

Primes	Sum of squares	Primes	Sum of squares
2	$1^2 + 1^2$	23	—
3	—	29	$2^2 + 5^2$
5	$1^2 + 2^2$	31	—
7	—	37	$1^2 + 6^2$
11	—	41	$4^2 + 5^2$
13	$2^2 + 3^2$	43	—
17	$1^2 + 4^2$	47	—
19	—	53	$2^2 + 7^2$

The first few primes, written as sums of two squares

Can any primes of the form $4k + 3$ 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:

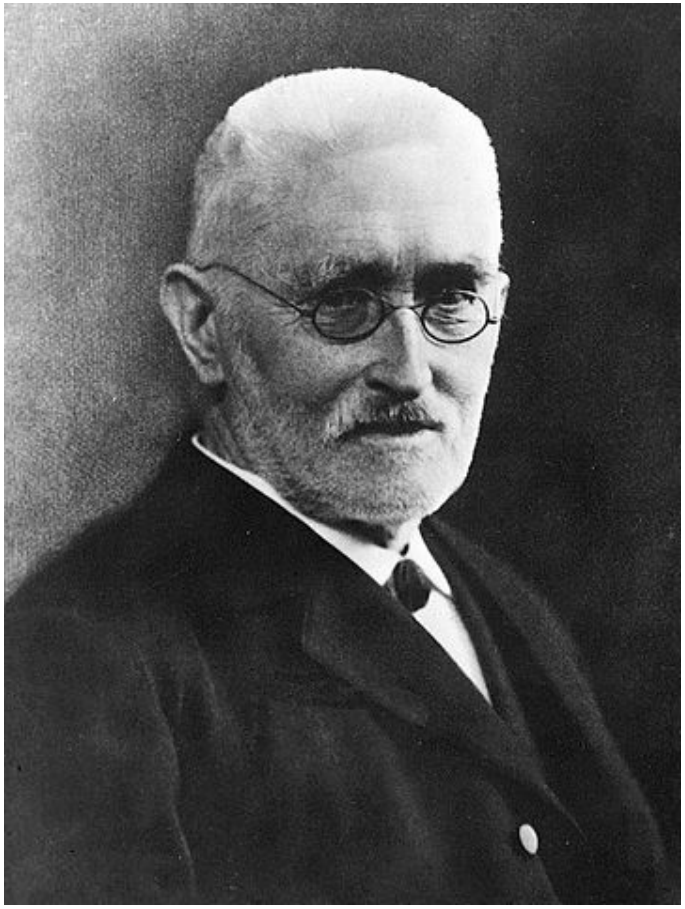
$$x^2 + y^2 \not\equiv 3 \pmod 4$$

Leonhard Euler, 1747

Leonard Euler

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

Dedekind's proof using Gaussian Integers (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 the one we will explore in 1894.

Prime and composite numbers

A reminder of what it means for a whole number to be prime or composite:

- If p is prime, then it has only two positive integer factors, itself and 1.
- If a prime p divides a composite number $n = ab$, then p divides a, or p divides b
- If a number q divides a number ab with $q > a, q > b$, then q must be composite. For example, $12|72 = 8 \cdot 9$, and $12 > 8$, $12 > 9$, so 12 must be composite.

Gaussian Integers

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 addition:
  $a + ib + c + id = (a + c) + i(b + d)$
- It is also closed under multiplication:
  $(a+ib)(c+id) = ac+ibc+iad+i^2bd = (ac-bd)+i(ad+bc)$

In the same way as we have unique factorization in $\mathbb{N}$, we have the same thing in $\mathbb{Z}[i]$! In particular, the same rules for determining whether a number is prime or composite apply to the Gaussian integers.

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:

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

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

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

Determining size of $a + ib$

Earlier, I said "if a number q divides a number ab with $q > a, q > b$, then q must be composite". But how can we tell if one Gaussian integer is bigger than another?
We define a "norm" function $N(x) : \mathbb{Z}[i] \to \mathbb{N}$:

- $N(a + ib) = a^2 + b^2$, the square of the length from the origin to the point.
- The norm function is multiplicative: $N(xy) = N(x)N(y)$

Since the norm function is multiplicative, we know that if $x = qy$, then $N(y)|N(x)$. Also, if $x|ab$ and $N(x) > N(a), N(x) > N(b)$, hten x must be composite in $\mathbb{Z}[i]$.

Fermat's Little Theorem

Fermat's Little Theorem states that for a prime p, and any number a coprime with p (that is, $\gcd(a, p) = 1$):

$$a^{p-1} \equiv 1 \pmod{p}$$

In fact, we can go further, and say that for every $a \not\equiv 0 \pmod{p}$, there exists an exponent e such that $a^e \equiv 1 \pmod{p}$, and $e|(p-1)$.

Quadratic residues

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 $\pmod{7}$.

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Powers of a $\pmod{7}$

Dedekind's proof (1)

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 $p = 4k + 1, (-1)^{\frac{p-1}{2}} = (-1)^{2k} \equiv 1 \pmod{p}$.
1 has two square roots $\pmod{p}$: itself and -1. For a quadratic non-residue a, $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
Therefore, for a quadratic non-residue a, $(a^{\frac{p-1}{4}})^2 = -1 \pmod{p}$.

Dedekind's proof (2)

If we can find a quadratic non-residue a, then we can set $b \equiv a^{\frac{p-1}{4}} \pmod{p}$ and we are guaranteed that $b^2 \equiv -1 \pmod{p}$, or $p|b^2+1$.
Factoring b^2+1 over $\mathbb{Z}[i]$ we get:

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

But since $b < p$, $N(b+i) < N(p)$, so 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 - that is, a number a where $a^{\frac{p-1}{2}} = -1$.
Let's try an example with $p = 41 = 4(10) + 1$ 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 $9^2 + 1 = 82$

Finding the squares (2)

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, 1990

Don Zagier

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

Don Zagier proof

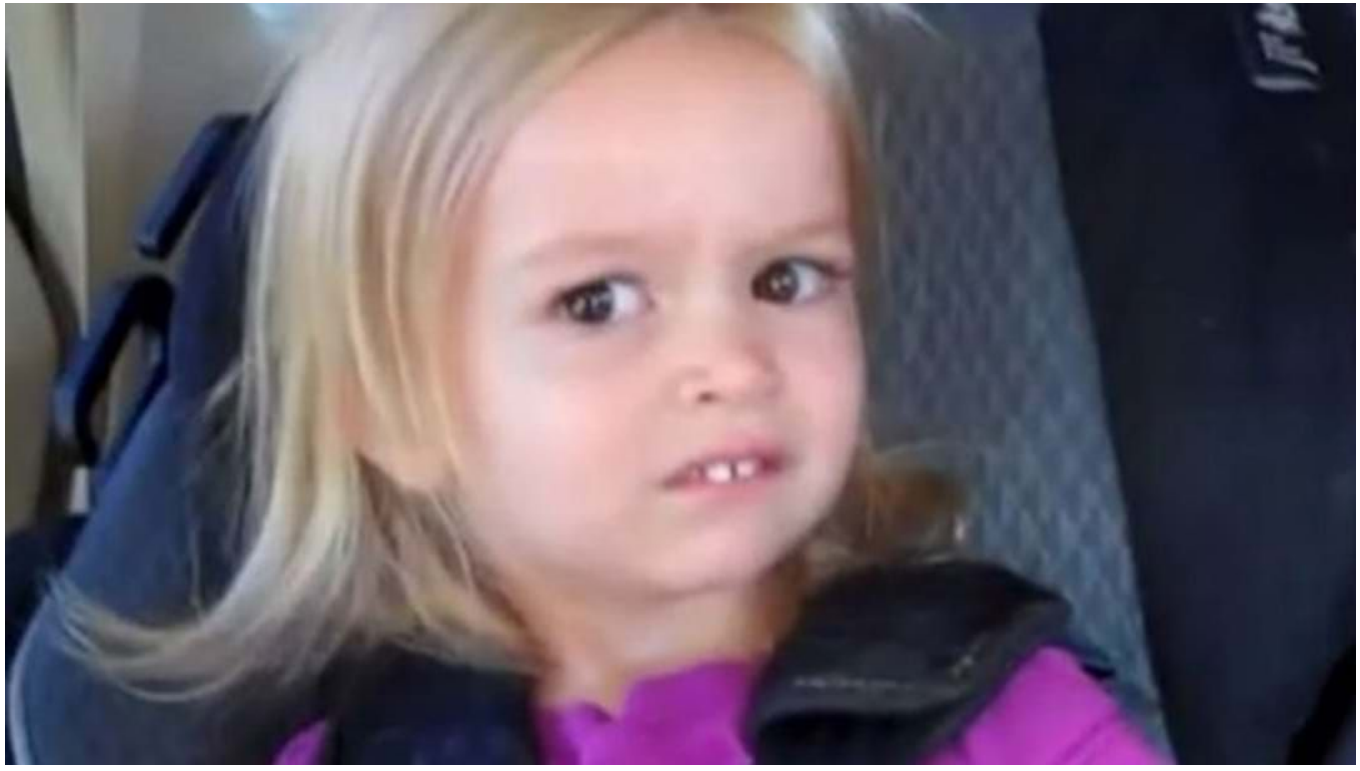
A one-sentence proof that every prime $p \equiv 1 \pmod 4$ *is a sum of two squares.*

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:

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

Involutions on finite sets

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.

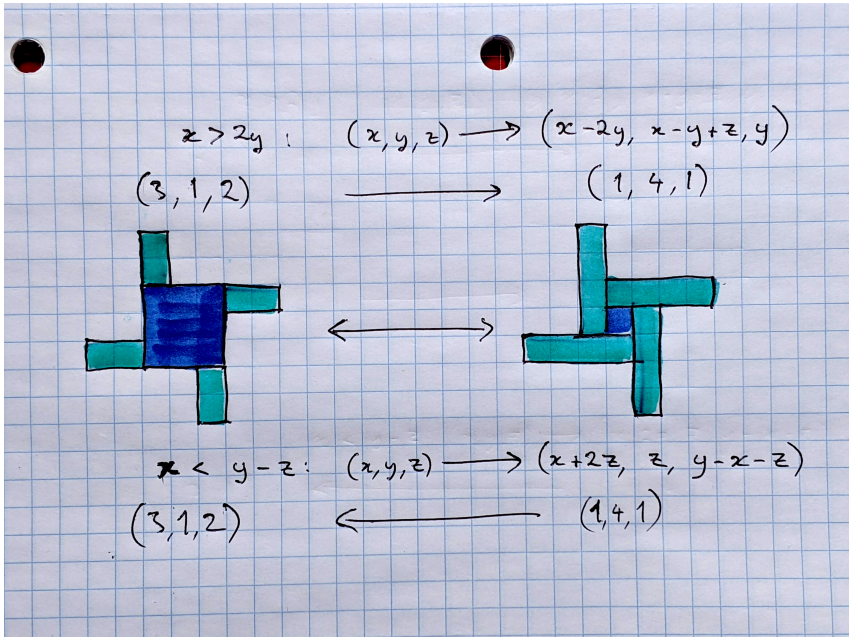
The complicated involution

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

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

Let's talk about windmills

A geometric interpretation



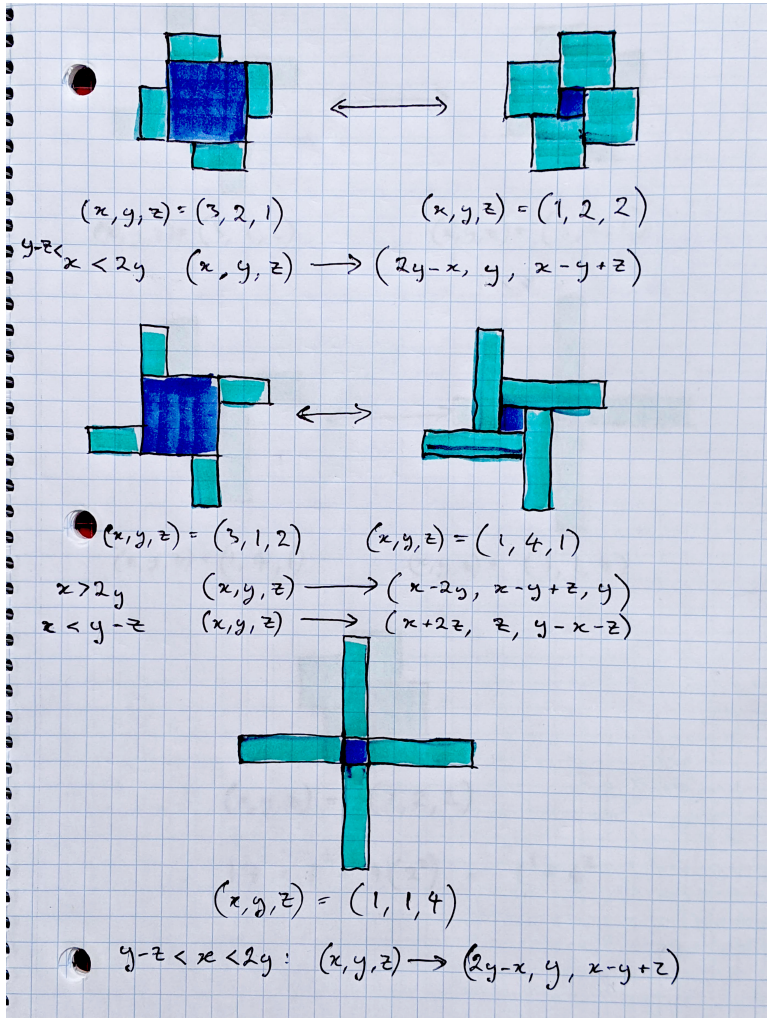
$$(3, 1, 2) \leftrightarrow (1, 4, 1)$$

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.

A geometric interpretation

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

These are all of the transformations for $p = 17$.

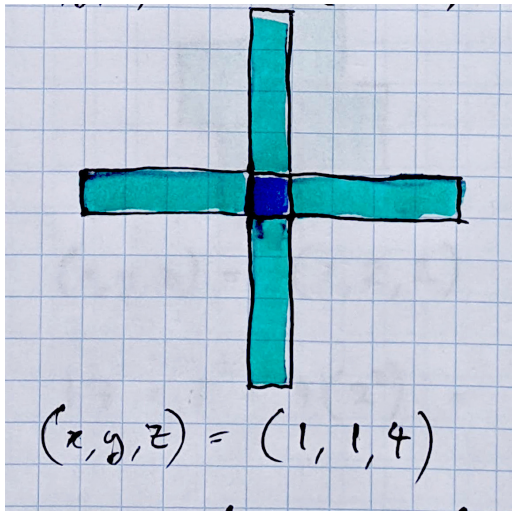


A unique fixed point

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. This point is a fixed point for the mapping, and it is guaranteed to be the only one!

$$(x, y, z) \to (2y - x, y, x - y + z)$$

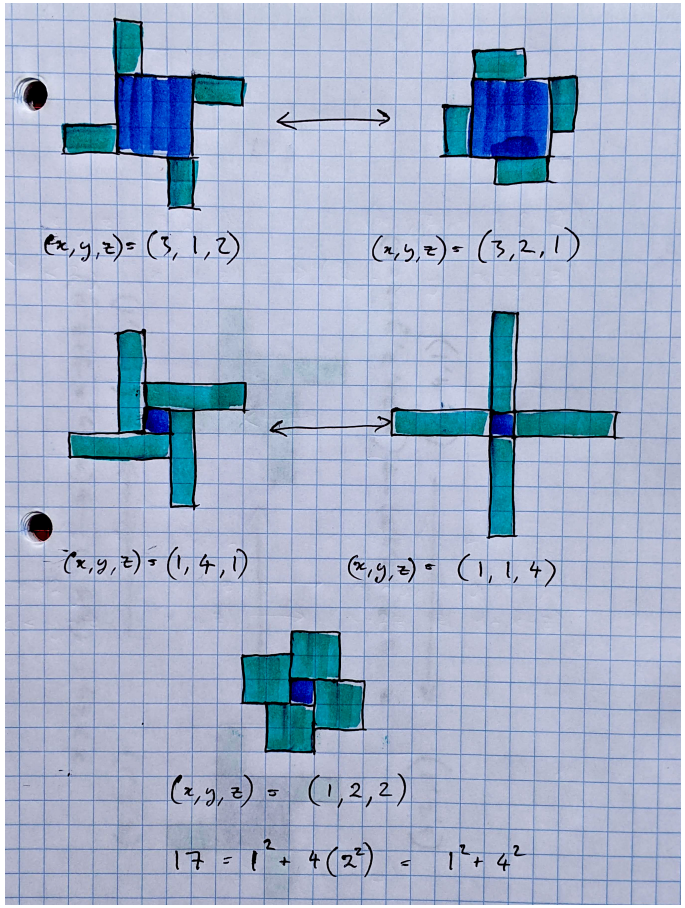


Fixed point in standard involution

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 $y = z$.

In our example of $p = 17$, we see that

$$p = 1^2 + 4(2)(2) = 1^2 + 4^2$$



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