Fermat's Two-Squares Theorem

Zagier's one-sentence proof and windmills

Alex Massarenti

Abstract

We explain Fermat's classical criterion: an odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$. After a quick modular warm-up accessible to high-school students, we present the parity-of-fixed-points principle for involutions, state Zagier's one-sentence proof, and give its geometric "windmill" interpretation.

1 The question

A few examples:

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2.$$

But $3, 7, 11, 19$ stubbornly refuse to be written as $a^2 + b^2$. What is the hidden pattern?

2 Squares mod 4

Lemma 1 (Squares mod 4)**.** *For any integer n, one has $n^2 \equiv 0$ or $1 \pmod 4$.*

Proof. If n is even, $n = 2k$ so $n^2 = 4k^2 \equiv 0 \pmod 4$. If n is odd, $n = 2k+1$ so $n^2 = 4k(k+1)+1 \equiv 1 \pmod 4$. □

Proposition 1 (A quick necessary condition)**.** *If an odd prime p can be written as $p = a^2 + b^2$, then $p \equiv 1 \pmod 4$.*

Proof. By the lemma, each square is 0 or $1 \pmod 4$, hence $a^2 + b^2 \equiv 0, 1,$ or $2 \pmod 4$. So $a^2 + b^2$ can never be $3 \pmod 4$. An odd prime is not 0 or $2 \pmod 4$, so only $1 \pmod 4$ remains. □

3 The theorem

Theorem 1 (Fermat's Two-Squares Theorem for primes)**.** *Let p be an odd prime. Then*

$$p = a^2 + b^2 \text{ for some integers } a, b \iff p \equiv 1 \pmod 4.$$

We already proved the "only if" direction (the easy half). The surprise is the converse: *every* prime $p \equiv 1 \pmod 4$ is a sum of two squares.

4 A combinatorial principle: involutions and parity

Definition 1. *An* involution *on a set S is a function $f : S \to S$ such that $f(f(s)) = s$ for all $s \in S$. A* fixed point *is an element s with $f(s) = s$.*

Proposition 2 (Counting in pairs)**.** *If S is finite and $f : S \to S$ is an involution, then*

$$|S| \equiv \#\mathrm{Fix}(f) \pmod 2.$$

In particular, if $|S|$ is odd, then f has at least one fixed point.

Proof. Every element of S is either a fixed point or belongs to a 2-cycle $\{s, f(s)\}$ with $s \neq f(s)$. So S is partitioned into disjoint pairs plus fixed points, and the parity statement follows. □

5 Zagier's one-sentence proof

Fix a prime $p \equiv 1 (\mathrm{mod}\ 4)$. Write $p = 4k + 1$.

5.1 The key finite set

Consider

$$S \ = \ \{(x, y, z) \in \mathbb{N}^3 \ : \ x^2 + 4yz = p\}.$$

This set is finite: $x^2 \leq p$ so $x \leq \lfloor \sqrt{p} \rfloor$, and then $yz \leq p/4$ gives only finitely many possibilities.

5.2 Two involutions on the same set

There are two involutions on S:

(1) The obvious swap involution

$$\tau(x, y, z) = (x, z, y).$$

Its fixed points are exactly the triples with $y = z$, i.e. (x, y, y).

(2) Zagier's involution $\sigma : S \to S$ defined by

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

One checks (a fun algebra exercise) that σ is well-defined on S and that $\sigma(\sigma(x, y, z)) = (x, y, z)$.

Zagier proved that σ has *exactly one* fixed point, namely $(1, 1, k)$. Therefore $\#\mathrm{Fix}(\sigma) = 1$ is odd, hence $|S|$ is odd by the parity principle. But then the *other* involution τ must also have an odd number of fixed points, in particular at least one. So there exists $(x, y, y) \in S$, i.e.

$$p = x^2 + 4y^2 = x^2 + (2y)^2,$$

which is a representation of p as a sum of two squares. □

6 Windmills: a picture for triples $p = x^2 + 4yz$

Given a triple $(x, y, z) \in S$, think of $p = x^2 + 4yz$ as an area decomposition:

- a central square of area x^2;
- four congruent rectangles, each of area yz, arranged like a "windmill" around the square.

6.1 A windmill diagram

The exact geometry is not unique; what matters is that the total area is $x^2 + 4yz$ and that rotating the picture cyclically corresponds to permuting the arms.

Total area $= x^2 + 4yz$
(four rectangles of area yz)

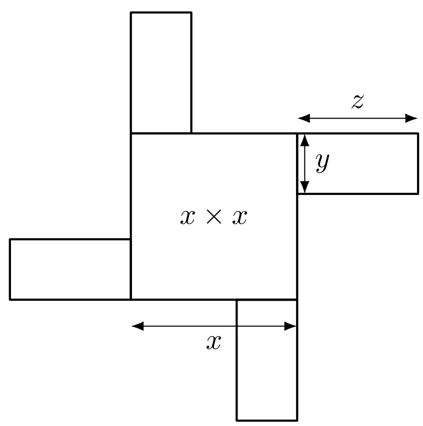

Figure 1: A "windmill" for a triple (x, y, z) with $p = x^2 + 4yz$.

Swapping y and z corresponds (morally) to turning each rectangle $y \times z$ into a $z \times y$ rectangle. A fixed point of τ is a configuration with $y = z$, i.e. each arm is a *square*.

$$\text{If } y = z, \text{ then } p = x^2 + 4y^2 = x^2 + (2y)^2.$$

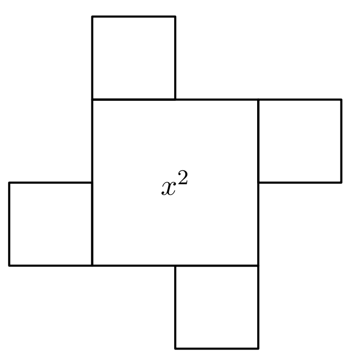

Figure 2: A symmetric windmill ($y = z$) directly yields a sum of two squares.

6.2 What Zagier's involution does (conceptually)

Zagier's map σ is an algebraic rule that (geometrically) "slides" and "re-centers" the largest possible square you can recognize inside the windmill, then reinterprets the leftover area as a new windmill. Doing this twice brings you back where you started, so it is an involution. Its unique fixed point is the most rigid windmill of all: the one coming from $(1, 1, k)$.

7 A worked example

Take $p = 29 = 4 \cdot 7 + 1$. Start from the special triple $(1, 1, 7) \in S$ since $1^2 + 4 \cdot 1 \cdot 7 = 29$. Zagier's proof guarantees that some triple in S has $y = z$, hence must be of the form (x, y, y) with

$$29 = x^2 + 4y^2 = x^2 + (2y)^2.$$

A quick check finds $29 = 5^2 + 2^2$ (so $x = 5$, $2y = 2$).

8 Turning the proof into an algorithm

A beautiful enhancement (not needed for existence) is that alternating the two involutions,

$$(x, y, z) \longmapsto \sigma(x, y, z) \longmapsto \tau(\sigma(x, y, z)) \longmapsto \sigma(\tau(\sigma(x, y, z))) \longmapsto \cdots$$

starting from $(1, 1, k)$, eventually lands on a τ-fixed point (x, y, y), producing $p = x^2 + (2y)^2$.

References

- D. Zagier, *A One-Sentence Proof That Every Prime* $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares*, Amer. Math. Monthly 97 (1990), 144.
- H. L. Chan, *Windmills of the Minds: An Algorithm for Fermat's Two Squares Theorem*, arXiv:2112.02556.