On Sums of Two Squares
(Zagier's One-Sentence Proof)

Klaus Pommerening

April 2020

Theorem 1 (Fermat-Euler) *Every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares.*

We start with a series of lemmas that blow up the steps of Zagier's one-sentence proof.

Lemma 1 *Let* S *be a finite set and* φ *be an involution of* S*. Then:*

(i) *The cardinalities of* S *and of the fixed point set of* φ *have the same parity.*

(ii) *If the cardinality of* S *is odd, then* φ *has a fixed point.*

Proof. (i) Le $n = \#S$. The orbits of φ have lengths 1 (the fixed points) or 2. If their numbers are n_1 and n_2 resp., then $n = n_1 + 2n_2$. Hence $n \equiv n_1 \pmod 2$.

(ii) By (i) the number of fixed points cannot be zero. ◇

Lemma 2 *For* $p \in \mathbb{N}$ *the set*

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid x, y, z > 0,\ x^2 + 4yz = p\}$$

is finite.

Proof. Each of the coordinates x, y, z is bounded by p. ◇

The involution $(x, y, z) \leftrightarrow (x, z, y)$ of $\mathbb{Z}^3$ maps S to itself—the defining conditions are symmetric in y and z. Each fixed point $(x, y, y) \in S$ yields a representation $p = x^2 + 4y^2$ of p as a sum of two squares. So by Lemma 1 we only have to show that $\#S$ is odd.

To this end we construct another involution of S that has exactly one fixed point. We consider three (obviously disjoint) subsets of S:

$$\begin{aligned} A &= \{(x, y, z) \in S \mid x < y - z\}, \\ B &= \{(x, y, z) \in S \mid y - z < x < 2y\}, \\ C &= \{(x, y, z) \in S \mid x > 2y\}. \end{aligned}$$

Note that $y - z < 2y$.

Lemma 3 *If p is prime, then these three sets form a partition: $S = A \cup B \cup C$.*

Proof. We only have to show that $x \neq y - z$ and $x \neq 2y$ for each point in S.
If $x = y - z$, then $p = x^2 + 4yz = (y-z)^2 + 4yz = (y+z)^2$, hence not a prime.
If $x = 2y$, then $p = 4y^2 + 4yz$ is divisible by 4, hence not a prime. ◇

Henceforth we assume that p is prime and consider the map $\varphi : S \longrightarrow \mathbb{Z}^3$ defined by

$$\varphi(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{if } (x,y,z) \in A, \\ (2y-x, y, x-y+z) & \text{if } (x,y,z) \in B, \\ (x-2y, x-y+z, y) & \text{if } (x,y,z) \in C. \end{cases}$$

Lemma 4 *$\varphi(A) \subseteq C$, $\varphi(B) \subseteq B$, $\varphi(C) \subseteq A$, thus $\varphi(S) \subseteq S$.*

Proof. Let $(x,y,z) \in S$ and $(u,v,w) = \varphi(x,y,z)$. By the defining conditions for A, B, and C all of $u, v, w > 0$. For $(x,y,z) \in A$ we have

$$u^2 + 2vw = (x+2z)^2 + 4z(y-x-z) = x^2 + 4yz, \quad u = x + 2z > 2z = 2v,$$

hence $(u,v,w) \in C$. For $(x,y,z) \in B$ we have

$$u^2 + 2vw = (2y-x)^2 + 4y(x-y-z) = x^2 + 4yz, \quad u - v = y - x < 2y - x = u < 2y = v,$$

hence $(u,v,w) \in B$. For $(x,y,z) \in C$ we have

$$u^2 + 2vw = (x-2y)^2 + 4y(x-y-z) = x^2 + 4yz, \quad u = x - 2y < x + z - 2y = v - w,$$

hence $(u,v,w) \in C$. ◇

Lemma 5 *φ is an involution of S.*

Proof. We show that φ applied twice is the identity map. Again this is a simply evaluation for each of our three cases: For $(x,y,z) \in A$ we have

$$\begin{aligned} (u,v,w) &= \varphi(x,y,z) = (x+2z, z, y-x-z) \in C, \\ \varphi(u,v,w) &= (u-2v, u-v+w, v) = (x,y,z). \end{aligned}$$

For $(x,y,z) \in B$,

$$\begin{aligned} (u,v,w) &= \varphi(x,y,z) = (2y-x, y, x-y+z) \in B, \\ \varphi(u,v,w) &= (2v-u, v, u-v+w) = (x,y,z). \end{aligned}$$

For $(x,y,z) \in C$,

$$\begin{aligned} (u,v,w) &= \varphi(x,y,z) = (x-2y, x-y+z, y) \in A, \\ \varphi(u,v,w) &= (u+2w, w, v-u-w) = (x,y,z). \end{aligned}$$

◇

Lemma 6 *If p is a prime $\equiv 1 \pmod 4$, $p = 4k+1$, then φ has exactly one fixed point, namely* $(1, 1, k)$.

Proof. Any fixed point must lie in B. In particular $2y - x = x$, hence $y = x$. From $p = x^2 + 4yz = x \cdot (x + 4z)$ we conclude that $x = 1$ and $z = k$. Clearly $(1, 1, k)$ is in S, even in B, and is a fixed point of φ. ◇

Lemma 7 *The cardinality $\#S$ is odd.*

Proof. Immediate from Lemmas 1 (i) and 6 ◇

This finishes the proof of the theorem by the remark after Lemma 2.

References

[1] D. R. Heath-Brown: Fermat's two squares theorem. Invariant 11 (1984), 3–5

[2] S. Wagon: Editor's corner. Amer. Math. Monthly 97 (1990), 125–129.

[3] 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.