Sums of Two Squares theorem (An account of Zagier's Proof)

Theorem: (Fermat's two squares theorem, "if part") Every prime p such that $p \equiv 1 \pmod 4$ is a sum of two squares.

We start with a series of lemmas which serve to expand and elaborate upon the different steps of Zagier's one-sentence proof.

Definition 1: An involution is a function that is its own inverse, $\varphi(\varphi(x)) = x$.

So an involution is a map when applied twice yields the identity.

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

(i) The cardinality of S is odd or even respectively if the cardinality of the fixed point set of φ is odd or even respectively.

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

Proof: (i) This easily follows from the fact that an involuton either has fixed points or interchanges two points.

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

□

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

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

is finite.

Proof: Say there was a solution where $x = 1$ and $z = 1$. In this specific case, we find that y take the value, $\frac{p-1}{4}$. This serves as an upper bound for y when x and z are not equal to 1. A similar argument applies when y and z are exchanged. Therefore, $y \leq \frac{p-1}{4}$ and $z \leq \frac{p-1}{4}$. So there are only finitely many possible values for y and z, and given y and z, there is one value for x.

□

The obvious involution $(x, y, z) \mapsto (x, z, y)$ of $\mathbb{Z}^3$ maps S to itself. 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 subsets of S:

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

These are obviously disjoint, as can be seen from $y - z < 2y$.

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 (i) $x \neq y - z$ and (ii) $x \neq 2y$ for each point in S.

(i) If $x = y - z$, then $p = x^2 + 4yz = (y-z)^2 + 4yz = (y+z)^2$, hence not a prime. (ii) If $x = 2y$, then $p = 4y^2 + 4yz$ is divisible by 4, hence not a prime. Alternatively, as we are only considering primes of the form $4k+1$ we can concentrate on odd primes. As such x is odd and cannot be equal to $2y$.

□

Henceforth we shall assume that p is a prime and consider Zagier's involution $\varphi : S \to \mathbb{Z}^3$ is 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 We have that $\varphi(A) \subseteq C$, $\varphi(B) \subseteq B$, $\varphi(C) \subseteq A$, thus $\varphi(S) \subseteq S$.

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

$$x'^2 + 4y'z' = (x+2z)^2 + 4z(y-x-z) = x^2 + 4yz, \qquad x' = x + 2z > 2z = 2y',$$

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

$$x'^2 + 4y'z'w = (2y-x)^2 + 4y(x-y-z) = x^2 + 4yz, \qquad y' - z' = 2y - x - z < 2y - x = x' < 2y = 2v,$$

hence $(x',y',z') \in B$. For $(x,y,z) \in B$ we have

$$x'^2 + 4y'z' = (x-2y)^2 + 4y(x-y-z) = x^2 + 4yz, \qquad x' = x - 2y < x + z - 2y = y' - z',$$

hence $(u, v, w) \in C$.

$\square$

Lemma 5 The 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

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

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

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

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

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

$\square$

Lemma 6: If $p = 4k + 1$, 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 $p = x^2 + 4yz = x(x + 4z)$ we conclude that $x = 1$ and $z = k$. Obviously, $(1, 1, k)$ is in S, and in particular in B, and is a fixed point.

$\square$

Lemma 7: The cardinality of S is odd.

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

$\square$

This finishes the proof of the theorem by the remark after Lemma 2 with regard to the obvious involution.

References

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

[2] D. Zagier: A one sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. Amer. Math. Monthly (1990), 144.

Additional

We prove the "only if" part of Fermat's two squared theorem, therby proving the full theorem.

Theorem: (Fermat's two squares theorem) Every prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.

Lemma 1: No number $n = 4m + 3$ is a sum of two squares.

Proof: The square of an even number is $(2k)^2 = 4k^2 \equiv 0 \pmod 4$, while the square of an odd number is $(2k + 1)^2 = 4(k^2 + k) + 1 \equiv 1 \pmod 4$. Thus any sum of two squares is congruent to $0, 1$ or $2 \pmod 4$.

□

This finishes the proof of the theorem.