FERMAT COMES TO SCHOOL

Let $p$ be a prime number of the form $4k+1$. Fermat’s two squares theorem asserts that $p$ is always a sum of two squares. For example, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$. Fermat did not provide a valid proof for the theorem — but Euler did so later. Modern proofs usually require a significant knowledge of algebraic number theory (a graduate course) until recently Don Zagier produced a one sentence proof that can be taught in school. Actually, Zagier’s one sentence was a little convoluted and it takes a little time to expound.

If we are able to solve the equation $p = a^2 + b^2$, then one of $a, b$ must be even and the other odd (why?). So we may as well try to solve the equation $p = x^2 + 4yz$, where $x, y$ have to be whole numbers. We can certainly solve the three variable equation $p = x^2 + 4yz$. Just take $x = 1, y = 1, z = k$. Let $S$ be the set of all triples $(x, y, z)$ where $x, y, z$ are positive whole numbers such that $p = x^2 + 4yz$. None of $x, y, z$ can exceed $p$ (why?) and so $S$ is a finite set. The proof is complete when we show that $S$ contains a triple $(x, y, z)$ with $y = z$. We can express this latter condition in different terms. Let $(x, y, z)^* = (x, z, y)$. We want to find a triple in $S$ with $(x, y, z)^* = (x, y, z)$. Notice that $*$ is an involution on $S$, that is, a function from $S$ to itself such that $(x, y, z)^{**} = (x, y, z)$. Any triple in $S$ can be paired off with its star. If the number of triples in $S$ is odd, then at least one triple in $S$ must be equal to its own star — which is what we want! All that remains is to prove that $S$ contains an odd number of triples. This is achieved by constructing on $S$ another involution $♭$ such that $(1, 1, k)$ is the only triple with $(x, y, z)^♭ = (x, y, z)$. The remaining triples must come in pairs, $(x, y, z)$ and $(x, y, z)^♭$. The construction of $♭$ is a little messy.

Show first that $S$ can be cut into three non-overlapping sets $A, B, C$ by the conditions:

$A : x < y - z, \quad B : y - z < x < 2y, \quad C : x > 2y.$

Now define $♭$ on $S$ by the rules

$(x, y, z)^♭ = (x + 2z, z, y - x - z) \quad (x, y, z) \in A$

$(x, y, z)^♭ = (2y - x, y, x - y + z) \quad (x, y, z) \in B$

$(x, y, z)^♭ = (x - 2y, x - y + z, y) \quad (x, y, z) \in C.$
It is straightforward, if tedious, to check that \((x, y, z)^b\) is always in \(S\) and that \((x, y, z)^{b^2} = (x, y, z)\). In checking this, notice that \((x, y, z)\) is in \(A\) (or \(C\)) if and only if \((x, y, z)^b\) is in \(C\) (or \(A\)). So the only place to find a fixed point of \(b\) (that is, \((x, y, z)^b = (x, y, z)\)) is in \(B\). For a fixed point we thus need to solve the three equations:

\[
2y - x = x, \quad y = y, \quad x - y + z = z.
\]

We get \(x = y\), and so our defining equation (for \(S\)) now becomes

\[
4k + 1 = p = x^2 + 4xz = x(x + 4z).
\]

Since \(p\) is a prime number, the only solution is given by \(x = 1\) (so \(y = 1\)) and \(z = k\). So \(b\) has exactly one fixed point, and the proof is complete. A thing of beauty is a joy forever. (John Keats)

Postscript. The formulas that appear in \(b\) come by considering simple examples of linear transformations that leave the expression \(X^2 + 4YZ\) unchanged. The ingenuity in the proof consisted in finding how to piece together three of these formulas to give an involution on \(S\) with exactly one fixed point. Zagier acknowledged that he was helped by earlier work by Liouville (19th century) and Heath-Brown (20th century).