A Short Proof That Every Prime $p \equiv 3 \pmod 8$ Is of the Form $x^2 + 2y^2$

Terence Jackson

In 1984 Heath-Brown [**1**] gave an interesting new proof of the Girard-Fermat theorem that every prime congruent to 1 modulo 4 is a sum of two squares. This was subsequently presented for students and mathematics teachers in [**2**] and [**3**], and it inspired Zagier [**4**] to give a one-sentence proof in 1990. A similar idea can be used to give a direct proof of Euler's result that every prime $p \equiv 3 \pmod 8$ is of the form $x^2 + 2y^2$.

Let p be an odd prime and S be the non-empty finite set $\{(x, y, z) \in \mathbb{N}^3 : x^2 + 2yz = p\}$. We define a map with domain S as follows:

$$(x,y,z) \mapsto \begin{cases} (x-2y, z+2x-2y, y) & \text{if } y < x/2, \\ (2y-x, y, z+2x-2y) & \text{if } x/2 < y < x+z/2, \\ (3x-2y+2z, 2x-y \\ \quad +2z, -2x+2y-z) & \text{if } x+z/2 < y < \frac{3}{2}x+z, \\ (-3x+2y-2z, -2x \\ \quad +2y-z, 2x-y+2z) & \text{if } \frac{3}{2}x+z < y < 2x+2z, \\ (x+2z, z, y-2x-2z) & \text{if } y > 2x+2z. \end{cases}$$

It is not hard, although somewhat tedious, to check that this is a well-defined map from S to S that is its own inverse. The requirement that $p \equiv 3 \pmod 8$ forces the only fixed point to be $(1, 1, (p-1)/2)$. This means that S contains an odd number of elements and so the involution on S that interchanges y and z must have a fixed point, giving $p = x^2 + 2y^2$.

The full result about odd primes of the form $p = x^2 + 2y^2$ is that any prime congruent to either 1 or 3 modulo 8 can be expressed in that way. If $p \equiv 1 \pmod 8$ our map is still an involution on S, but now it has three fixed points: $(1, 1, (p-1)/2)$ and also the points $(x_0, x_0 + z_0, z_0)$, where $p = (x_0 + z_0)^2 + z_0^2$, and $(x_1, 2x_1 + z_1, z_1)$, where $p = (x_1 + 2z_1)^2 - 2z_1^2$. It is classical, though not immediate, that when $p \equiv 1 \pmod{8}$ there are positive values of x_0, z_0, x_1, z_1 satisfying these conditions. So although S still has an odd number of elements we no longer have a short proof.

REFERENCES

1. D. R. Heath-Brown, Fermat's two-squares theorem, *Invariant* (1984) 3–5.
2. I. Varouchas, Une démonstration élémentaire du théorème des deux carrés, *I.R.E.M. Bull.* **6** (1984) 31–39.
3. K. S. Williams, Heath-Brown's elementary proof of the Girard-Fermat theorem, *Carleton Coordinates* (1985) 4–5.
4. 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.

University of York, York, England YO10 5DD
thj1@york.ac.uk