

**Euler's four squares identity.** For any  $a, b, c, d, w, x, y, z$

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (aw + bx + cy + dz)^2 + (ax - bw - cz + dy)^2 + (ay + bz - cw - dx)^2 + (az - by + cx - dw)^2.$$

**Lagrange's Theorem.** Every natural number is the sum of four squares.

Lemma A. If  $2m$  is the sum of two squares, then so is  $m$ .

Proof. If both squares are even, then  $m/2$  is the sum of two squares, and since  $1^2 + 1^2 = 2$  so then is  $m$  by Euler's identity. If they are both odd, then  $4m = (x + y)^2 + (x - y)^2$  with  $x, y$  odd and we can reduce to the previous case.

Lemma B. If  $p$  is an odd prime, then there are  $r, s, m$  such that  $r^2 + s^2 + 1 = mp$  and  $m < p/2$ .

Proof. Immediately by a box argument there are  $r, s, m$  such that  $r^2 + s^2 + 1 = mp$  and  $0 \leq r, s \leq (p - 1)/2$ . Thus  $mp \leq \frac{p^2}{2} - p + 3/2$ .

To prove Lagrange's, in view of Euler's identity and  $1^2 + 1^2 = 2$ , it suffices to prove that every odd prime is such a sum. By Lemma B there is an  $m < p/2$  such that  $mp$  is such a sum, say

$$a^2 + b^2 + c^2 + d^2 = mp.$$

Choose  $m$  minimally. Then  $m$  is odd since if it were even, then  $mp$  would be the sum of four squares with exactly none, two or all four even, and we could replace  $m$  by  $m/2$  by an appeal to Lemma A. Suppose  $m > 1$ . Then not all of  $a, b, c, d$  are divisible by  $m$  and so we may choose  $w, x, y, z$  not all 0 such that  $w \equiv a(\text{mod } m)$ ,  $x \equiv b(\text{mod } m)$ ,  $y \equiv c(\text{mod } m)$ ,  $z \equiv d(\text{mod } m)$  and  $|w|, |x|, |y|, |z| < m/2$ . Then there is a natural number  $n$  such that

$$w^2 + x^2 + y^2 + z^2 = nm$$

and  $nm < 4(m/2)^2 = m^2$ , so that  $n < m$ . By Euler's identity

$$\begin{aligned} m^2 np &= (a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \\ &= (aw + bx + cy + dz)^2 + (ax - bw - cz + dy)^2 + (ay + bz - cw - dx)^2 \\ &\quad + (az - by + cx - dw)^2. \end{aligned}$$

It is easily verified that each square here is a multiple of  $m^2$  and hence that  $np$  is the sum of four squares contradicting the minimality of  $m$ .