LAGRANGE'S FOUR SQUARE THEOREM

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

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

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

Proof. In view of Euler's identity and $1^2 + 1^2 = 2$, it suffices to prove that every odd prime is such a sum.

Lemma 1. *If n is even and is a sum of four squares, then so is $\frac{n}{2}$.*

Proof of Lemma 1. When $n = a^2 + b^2 + c^2 + d^2$ is even, an even number of the squares will be odd. and so the a, b, c, d can be rearranged so that a, b have the same parity and so do c, d. Thus $\frac{n}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$.

Lemma 2. *If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.*

Proof of Lemma 2. The $\frac{p+1}{2}$ numbers $0^2, 1^2 \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p. Hence, by a box argument there are u, v such that $u^2 \equiv -v^2 - 1 \pmod p$ and $0 < u^2 + v^2 + 1 \leq \frac{p^2-2p+3}{2}$.

By Lemma 2 there is an integer m with $0 < m < p$ so that for some a, b, c, d we have

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

and we may suppose that m is chosen minimally. Moreover, by Lemma 1 we may suppose that m is odd. If $m = 1$, then we are done. Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$. Choose w, x, y, z so that $w \equiv a \pmod m$, $|w| \leq \frac{m-1}{2}$, $x \equiv -b \pmod m$, $|x| \leq \frac{m-1}{2}$, $y \equiv -c \pmod m$, $|y| \leq \frac{m-1}{2}$, $z \equiv -d \pmod m$, $|z| \leq \frac{m-1}{2}$, and then not all of w, x, y, z can be 0. Moreover $w^2+x^2+y^2+z^2 \equiv 0 \pmod m$ and so $0 < w^2+x^2+y^2+z^2 = mn \leq 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$. Thus $0 < n < m$. Now $aw-bx-cy-dz \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod m$, $ax+bw+cz-dy \equiv -ab + ab - cd + dc \equiv 0 \pmod m$, $ay + cw + dx - bz \equiv -ac + ac - db + db \equiv 0 \pmod m$, $az + dw + by - cx \equiv -ad + ad - bc + bc \equiv 0 \pmod m$. By Euler's identity m^2np is the sum of four squares and each of the squares is divisible by m^2. Hence np is the sum of four squares. But $n < m$ contradicting the minimality of m.