19 Sums of Four Squares

The following result of Lagrange is surprising at first; it had been predicted earlier, i.e., before Lagrange, by Fermat.

Theorem (Lagrange) Every positive integer n is a sum of four squares.

Proof. We may take n to be > 1, as $1 = 0^2 + 0^2 + 0^2 + 1^2$. We need two lemmas.

Lemma 1 Let $x_j, y_j \in \mathbb{Z}$, with $1 \geq j \geq 4$. Then

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_1^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

where $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, $z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$, $z_3 = x_1y_3 + x_3y_1 + x_4y_2 + x_2y_4$, and $z_4 = x_1y_4 + x_4y_1 + x_2y_3 + x_3y_2$.

The checking of this, called Euler's identity, is straightforward and is left as an exercise.

Lemma 2 Let p be an odd prime. Then $\exists$ integers x, y, m, with $1 \leq m < p$, such that $mp = x^2 + y^2 + 1$.

Proof of Lemma 2: Put $T = \{1 \leq j \leq \frac{p-1}{2}\}$. Then we have seen earlier that the squares of elements of T are pairwise unequal, i.e., the set $T_1 = \{x^2 | x \in T\}$ has cardinality $\frac{p-1}{2}$. But the set $T_2 = \{-1 - y^2 | y \in T\}$ has the same property. As p is odd, there are exactly $\frac{p-1}{2}$ squares in $(\mathbb{Z}/p)^*$. So we must have $T_1 \equiv T_2 \pmod{p}$. Consequently, $\exists x, y \in T$ such that $x^2 + y^2 + 1 = mp$, for some integer m, which is evidently ≥ 1. Moreover, as $x, y \in T$, x^2, y^2 are bounded from above by $\frac{p^2}{4}$. Hence

$$mp = x^2 + y^2 + 1 < \frac{p^2}{2} + 1 < p^2,$$

which implies that $m < p$.

This proves the Lemma.

Proof of Lagrange's theorem (cont.)

Thanks to Lemma 1, and the fact that $2 = 1^2 + 1^2 + 0^2 + 0^2$, it suffices to prove the Theorem for odd primes. Pick any odd prime p. Let m_0 be the smallest integer with $1 \leq m_0 < p$ such that

$$m_0p = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{1}$$

for some $x_1, x_2, x_3, x_4 \in \mathbb{Z}$. By Lemma 2, $\exists$ such an m_0. If $m_0 = 1$ we are done, so **assume not** and derive a contradiction.

Claim: m_0 is odd.

Proof of Claim Suppose m_0 is even. Then either all the x_i's are even or all of them are odd, or exactly half of them are odd. In the third case we may, after renumbering the x_j, assume that x_1, x_2 are even and x_3, x_4 are odd. It follows from (1) that

$$\frac{m_0 p}{2} = \left(\frac{x_1 + x_2}{2}\right) + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 \qquad (2)$$

Then as $\frac{x_1 \pm x_2}{2}$ and $\frac{x_3 \pm x_4}{2}$ are integers, we get a contradiction to the minimality of m_0. Hence the claim.

Proof of Theorem (cont.)

So m_0 is odd and ≥ 3. Let us write $(\forall j)$

$$x_j = y_j + a_j m_0, \qquad (3)$$

with $a_j \in \mathbb{Z}$ chosen such that $|y_j| < \frac{m_0}{2}$ (check that this can be done; the oddness of m_0 is essential).

Since $m_0 < p$, not all the x_j can be divisible by m_0. Consequently,

$$\sum_{j=1}^{4} y_j^2 > 0 \qquad (4)$$

We also have

$$\sum_{j=1}^{4} y_j^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2. \qquad (5)$$

But (1) + (3) implies that

$$\sum_{j=1}^{4} y_j^2 \equiv 0 \pmod{m_0}. \qquad (6)$$

This means we have

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 = k m_0, \qquad (7)$$

with $0 < k < m_0$.

Applying Lemma 1 with the z_j defined by the $x_j + y_j$, we get

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 kp. \tag{8}$$

But

$$z_1 = \sum_{j=1}^{4} x_j y_j = \sum_{j=1}^{4} x_j (x_j - a_j m_0) \equiv \sum_{j=1}^{4} x_j^2 \equiv 0 \pmod{m_0}$$

Similarly, $z_2 \equiv z_3 \equiv z_4 \equiv 0 \pmod{m_0}$. So $z_j = m_0 w_j$, with $w_j \in \mathbb{Z},\ \forall j \leq 4$. Substituting this in (8) we get

$$kp = w_1^2 + w_2^2 + w_3^2 + w_4^2, \tag{9}$$

with $1 \leq k < m_0 < p$.

Since this contradicts the minimality of m_0, we get the derived contradiction.