**Theorem 1** (Lagrange, 1770). Any positive integer is the sum of four integral squares.

**Proof.** Because of the four squares identity, it suffices to prove the theorem for primes \( p \). Since \( 2 = 1^2 + 1^2 + 0^2 + 0^2 \), we may suppose \( p \) is an odd prime.

Consider \( x^2 \) for all integers \( 0 \leq x \leq (p-1)/2 \). All these are incongruent mod \( p \). Consider also \(-1 - y^2\) for all integers \( 0 \leq y \leq (p-1)/2\); these are also incongruent mod \( p \). Therefore, by the pigeonhole principle, there are integers \( x \) and \( y \) such that \( x^2 + y^2 + 1 \equiv 0 \pmod{p} \) and \( 0 \leq x, y \leq (p-1)/2 \).

Note that \( x^2 + y^2 + 1 < 1 + 2(p/2)^2 < p^2 \), and hence \( x^2 + y^2 + 1 = mp \) for some \( 1 \leq m < p \). Let \( \ell \) be the smallest positive integer such that \( \ell p \) may be written as a sum of four integral squares, say, \( \ell p = x^2 + y^2 + z^2 + w^2 \). Then \( \ell \leq m < p \).

We claim that \( \ell \) is odd. Indeed, if \( \ell \) were even, then an even number of \( x, y, z, \) and \( w \) would be odd, and hence without loss of generality we may suppose that \( x - y, x + y, z - w, \) and \( z + w \) are all even. Moreover, we have

\[
\frac{1}{2} \ell p = \left( \frac{1}{2}(x - y) \right)^2 + \left( \frac{1}{2}(x + y) \right)^2 + \left( \frac{1}{2}(z - w) \right)^2 + \left( \frac{1}{2}(z + w) \right)^2,
\]

which contradicts the minimality of \( \ell \). Therefore \( \ell \) is indeed odd.

If \( \ell = 1 \), then we are done. So suppose that \( \ell > 1 \). Take \( x', y', z', \) and \( w' \) congruent to, respectively, \( x, y, z, \) and \( w \) modulo \( p \). Moreover, choose \( x', y', z', \) and \( w' \) with smallest possible absolute value. Clearly, \( n = (x')^2 + (y')^2 + (z')^2 + (w')^2 > 0 \), for otherwise \( x' = y' = z' = w' = 0 \), and \( x, y, z, \) and \( w \) would all be divisible by \( \ell \), and hence \( \ell^2 \) would divide \( x^2 + y^2 + z^2 + w^2 = \ell p \), which tells us that \( \ell \) divides \( p \). Since \( 1 < \ell < p \), this is a contradiction, and hence indeed \( n > 0 \).

Since \( \ell \) is odd, we have \( |x'|, |y'|, |z'|, \) and \( |w'| < \ell/2 \), whence \( n = (x')^2 + (y')^2 + (z')^2 + (w')^2 < 4(\ell/2)^2 = \ell^2 \). Since \( n \equiv \ell p \equiv 0 \pmod{\ell} \), we have \( n = \ell k \) for some \( 1 \leq k < \ell \).

We now use the four squares identity to obtain that \( (\ell k)(\ell p) \) is a sum of four squares. More precisely, let

\[
\begin{pmatrix} t_1 & t_2 & t_3 & t_4 \end{pmatrix} = \begin{pmatrix} x' & y' & z' & w' \end{pmatrix} \begin{pmatrix} x & -y & -z & -w \\ y & x & w & -z \\ z & -w & x & y \\ w & z & -y & x \end{pmatrix}.
\]

**Date:** February 17, 2003.

Math and CS, Emory University.
(The matrix above is $H(x, -y, -z, -w)$, in the notation used in the proof of the Bruck–Ryser theorem.) Then $kp\ell^2 = ((x')^2 + (y')^2 + (z')^2 + (w')^2)(x^2 + y^2 + z^2 + w^2) = t_1^2 + t_2^2 + t_3^2 + t_4^2$. However, all the $t_i$ are divisible by $\ell$, and hence $kp$ is a sum of four integral squares, which contradicts the choice of $\ell$. This contradiction shows that $\ell = 1$, and the theorem is proved.