Math 445 Number Theory

November 15, 2004

Sums of four squares.

For every $n \in \mathbb{N}$, there are $x, y, z, w \in \mathbb{Z}$ so that $x^2 + y^2 + z^2 + w^2 = n$.

Elements of the proof:

$$(x_1^2 + y_1^2 + z_1^2 + w_1^2)(x_2^2 + y_2^2 + z_2^2 + w_2^2) =$$
$$(x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2)^2 + (x_1y_2 - x_2y_1 + z_2w_1 - z_1w_2)^2$$
$$+ (x_1z_2 - x_2z_1 + y_1w_2 - w_1y_2)^2 + (x_1w_2 - x_2w_1 + y_2z_1 - y_1z_2)^2$$

So we may focus on primes p. $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, so focus on odd primes. Then

Proposition: $0 \le x, y \le (p-1)/2$ and $x \ne y$ implies $x^2 \not\equiv y^2 \pmod p$. This is because $p | x^2 - y^2 = (x-y)(x+y)$ implies $p | x - y$ and $-(p-1)/2 \le x - y \le (p-1)/2$ so $x = y$, or $p | x + y$ and $0 \le x + y \le p - 1$ so $x + y = 0$ so $x = y = 0$. Then

Proposition: For any a, x^2 and $a - y^2$, with $0 \le x, y \le (p-1)/2$ must have a value, mod p, in common. For otherwise, since x^2 and $a - y^2$ each take on $(p+1)/2$ different values, $x^2 + y^2 - a = x^2 - (a - y^2)$ would take on $p+1$ different values, mod p. So in particular, $x^2 + y^2 \equiv -1 \pmod p$ has a solution.

Then $x^2 + y^2 + 1^2 + 0^2 = Mp$ for some M; with the restrictions on x, y above, we have $M < p$. Choose the smallest positive M with $Mp = x^2 + y^2 + z^2 + w^2$. We claim: $M = 1$ (so $p = x^2 + y^2 + z^2 + w^2$ is a sum of 4 squares).

First, M is odd, since if M is even, then $x^2 + y^2 + z^2 + w^2$ is even, so an even number of x, y, z, w are even. After renaming the variables to group them by parity, we have $\frac{M}{2}p = (\frac{x-y}{2})^2 + (\frac{x+y}{2})^2 + (\frac{z-w}{2})^2 + (\frac{z+w}{2})^2$ where each of the numbers on the right are integers. If $M > 1$ is odd, then choose $-\frac{M}{2} \le x_1, y_1, z_1, w_1 \le \frac{M}{2}$ with $x \equiv x_1 \pmod M$, etc. Then $x_1^2 + y_1^2 + z_1^2 + w_1^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod M$, so $x_1^2 + y_1^2 + z_1^2 + w_1^2 = NM$; since $|x_1|, |y_1|, |z_1|, |w_1| < \frac{M}{2}$, $x_1^2 + y_1^2 + z_1^2 + w_1^2 < M^2$, so $N < M$. Note also that $N > 0$, since otherwise $x_1 = y_1 = z_1 = w_1 = 0$, so $M | x, y, z, w$, so $M^2 | x^2 + y^2 + z^2 + w^2 = Mp$, so $p | M$, contradicting $M < p$. Then

$$NM^2p = (x_1^2 + y_1^2 + z_1^2 + w_1^2)(x^2 + y^2 + z^2 + w^2) =$$
$$(x_1x + y_1y + z_1z + w_1w)^2 + (x_1y - xy_1 + zw_1 - z_1w)^2$$
$$+(x_1z - xz_1 + y_1w - w_1y)^2 + (x_1w - xw_1 + yz_1 - y_1z)^2 = a^2 + b^2 + c^2 + d^2$$

and we can check that, mod M,

$a = x_1x + y_1y + z_1z + w_1w \equiv x^2 + y^2 + z^2 + w^2 \equiv 0$,
$b = x_1y - xy_1 + zw_1 - z_1w \equiv xy - xy + zw - zw \equiv 0$,
$c = x_1z - xz_1 + y_1w - w_1y \equiv xz - xz + yw - yw \equiv 0$,
and $d = x_1w - xw_1 + yz_1 - y_1z \equiv xw - xw + yz - yz \equiv 0$.

So $a = MA, b = MB, c = MC, d = MD$ and $NM^2p = M^2(A^2 + B^2 + C^2 + D^2)$ so $A^2 + B^2 + C^2 + D^2 = Np$ with $0 < N < M$, a contradiction. So $M = 1$, as desired.