Lagrange's Four Square Theorem:

November 7, 2012

We have seen that any number n of the form $n = p_1^{k_1} \cdots p_m^{k_m} q_1^{l_1} \cdots q_r^{k_r}$ where the p_i's and q_j's are primes, $p_i = 1 \bmod 4$ and l_i are even, can be written as a sum of two squares. Here we investigate which integers can be written as sums of more squares.

1 Sums of Three Squares:

It is easy to see that not everything can be written as the sum of two squares (for example 3.) So if we allow ourselves 3 squares we are bound to get more integers, in particular we can write 3=1+1+1. However, we again quickly see that this is not sufficient to write all integers because we cannot write 7 in this way. So first let us be more precices about which integers we can write as a sum of 3 squares.

Theorem 1.1. *No positive integer of the form $4^n(8m + 7)$ can be written as the sum of three squares.*

Proof. First let us show this for $n = 0$. Let us look at squares mod 8. They are exactly 0, 1, and 4. So if we add three squares mod 8 the only possibility for the sums are 0, 1, 2, 3, 4, 5, 6. In particular 7 is not a possibility. So $8m + 7$ cannot be the sum of three squares.

Not let us say that we have an $n \geq 1$ with $4^n(8m + 7) = a^2 + b^2 + c^2$. This implies that $a^2 + b^2 + c^2$ is divisible by 4. Looking mod 4 we see that the only squares are 0, 1. So if we add three of them to get 0 the only way this is possible is if they are all 0. Thus we get that each of a, b, c is even. So we can write them as $a = 2a_1, b = 2b_1, c = 2c_1$.

In this case, we get that $4^{n-1}(8m+7) = a_1^2+b_1^2+c_1^2$. We can simply repeat this process to show that $(8m + 7)$ can be written as a sum of 3 squares which is a contradiction $\square$

So in fact we have many integers which cannot be written as the sum of three squares. Thus we would like to expand this to see which ones can be written as the sum of 4 squares. Naturally we will get more numbers (including 7=4+1+1+1). In fact, any integer can be written in this way, that is our next goal.

2 Lagrange's Four Sqaure Theorem:

First we need some prepatory lemmas, the first merely states that the set of integers which can be written as the sum of four squares is closed under multiplication, which allows us to prove the four square theorem only for primes.

Lemma 2.1. *Let n and k be integers that can be written as the sum of 4 squares. Then so can nk*

Lemma 2.2. *The proof of this lemma is simply by brute force. Let $n = a^2 + b^2 + c^2 + d^2$ and $k = x^2 + y^2 + w^2 + z^2$, then*

$$nk = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + w^2 + z^2) =$$

$$= (ax + by + cw + dz)^2 + (ay - bx + cz - dw)^2 + (aw - bz - cx + dy)^2 + (az + bw - cy - dx)^2$$

(multiply the both lines out if you don't believe me)

The following is the key lemma in our argument.

Lemma 2.3. *If p is an odd prime, the the congruence*

$$x^2 + y^2 + 1 = 0 \qquad \text{mod } p$$

has a solution x_0, y_0 where $0 \leq x_0, y_0 \leq \frac{p-1}{2}$.

Proof. Consider the following sets

$$S_1 = \left\{ 1, 2, 5, 10, ..., 1 + \left(\frac{p-1}{2}\right)^2 \right\}$$

$$S_2 = \left\{ 0, -1, -4, -9, ..., -\left(\frac{p-1}{2}\right)^2 \right\}$$

Now let us assume that two integers in S_1 are the same mod p. So we have $1+x^2 = 1+y^2$ this implies that $x = y$ or $x = -y$ mod p. But since $0 \leq x, y \leq \frac{p-1}{2}$ this is not possible. So the integers in S_1 are distinct, and a similar fact fan be shown for the elements of S_2. Together S_1 and S_2 have $p+1$ elements. Since they are in $\mathbb{Z}/p\mathbb{Z}$ it must be that they have a common element. Thus $1 + x^2 = -y^2$ and we are done. □

Corollary 2.4. *Given an odd prime p there is an integer $k < p$ such that kp can be written as a sum of four squares.*

Proof. By the above theorem we have that there are x_0, y_0 with $0 \leq x_0, y_0 \leq \frac{p-1}{2}$ such that $x_0^2 + y_0^2 + 1 = 0$ mod p. This means that there is a k such that $x_0^2 + y_0^2 + 1 + 0 = kp$. Th fact about the size of x_0 and y_0 implies the fact about the size of k □

Theorem 2.5. *Any prime p can be written as a sume of four squares.*

Proof. Clearly this is true for $p = 2$ so let us focus on odd primes. Consider the set

$$\{a > 0 : ap = x^2 + y^2 + w^2 + z^2\}$$

By the previous corollary we know that the set is nonempty. So it has a smallest element, let us call it k. We also know by the corollary that $k < p$.

First let us assume that k is even. Then we must have that two of the x, y, w, z are even and two are odd, or they are all odd, or all even. In particular we can rearrange them so that

$$x = y \qquad w = z \qquad \mod 2$$

Thus we get that the numbers

$$\frac{1}{2}(x-y) \quad \frac{1}{2}(x+y) \quad \frac{1}{2}(z-w) \quad \frac{1}{2}(z+w)$$

are all integers. Thus we have

$$\frac{kp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2$$

But this contradicts the fact that k is the least such integer. Thus we have that k is odd.

So now assume that $k > 1$ then $k \geq 3$.

So now we can chose a, b, c, d such that $|a|, |b|, |c|, |d| < \frac{k}{2}$ and

$$a = x \qquad b = y \qquad c = w \qquad d = z \qquad \mod k$$

We just choose a for example to be either the value in $[x]_k$ with the smallest absolute value. Then we have

$$x^2 + y^2 + w^2 + z^2 = a^2 + b^2 + c^2 + d^2 = 0 \qquad \mod k$$

Which implies that

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

For some n. Now we know that

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2$$

So we have $0 \leq nk < k^2 \Rightarrow 0 \leq n < k$. Now note that if $n = 0 \Rightarrow a = b = c = d = 0 \Rightarrow k$ divides each of x, y, w, z. This would in turn implies that $k^2 | (x^2 + y^2 + w^2 + z^2) = kp \Rightarrow k | p$ which contradicts that $0 < k < p$. Thus we must have $n \neq 0$. So $0 < n < k$. Now we would

like to show that np can be written as a sum of four squares to complete our contradiction proof. First let us consider

$$(kn)(kp) = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + w^2 + z^2)$$

$$= (ax + by + cw + dz)^2 + (ay - bx + cz - dw)^2 + (aw - bz - cx + dy)^2 + (az + bw - cy - dx)^2$$

$$= r^2 + s^2 + t^2 + u^2$$

Where $r = ax + by + cw + dz$, $s = ay - bx + cz - dw$, $t = aw - bz - cx + d$, and $u = az + bw - cy - dx$. It is not hard to see that each of these is equal to 0 mod k. Thus we can write

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2$$

and this is our contradiction, since we assumed that $k > 1$ we get that $k = 1$ and so we are done. □

Now we can state and prove our key result.

Theorem 2.6. *Every positive integer can be written as a sum of four squares.*

Proof. We have proven it for primes and proven that the set of integers which can be written in this way is closed under multiplication thus we are done. □