

Sums of two and four squares

Siddhartha Sahi
Rutgers University

November 14, 2007

1 Sums of two squares

Consider the following question: which integers n are the sum of squares of two integers, i.e., can be written as $n = x_1^2 + x_2^2$? Here is the situation for small n :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x_1	0	1		0	1			2	0	1			2			0	1
x_2	1	1		2	2			2	3	3			3			4	4

Thus 1, 2, 4, 5, 8, 9, 10, 13, 16, 17 can be written as the sum of two squares, while 3, 6, 7, 11, 12, 14, 15 cannot.

Lemma 1 *If $n = n_1 \dots n_k$ and each n_i is a sum of two squares then so is n .*

Proof. We proceed by induction on k . The result is obvious for $k = 1$, and assuming the result for $k - 1$ we get: $(n_1 \dots n_{k-1}) n_k = (x_1^2 + x_2^2) (y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$. ■

We now consider the case of prime numbers. Note that in the above table the “inexpressible” primes 3, 7, 11 are all of the form $4k + 3$, while the “expressible” primes 5, 17 are of the form $4k + 1$. This is true in general.

Lemma 2 *Every prime of the form $p = 4k + 1$ is the sum of two squares.*

Proof. Let S be the following set of pairs of integers

$$\{(x_1, x_2) : x_1^2 + x_2^2 \text{ is divisible by } p, \text{ and } p^2 > x_1^2 + x_2^2 > 0\}.$$

Since -1 is a quadratic residue mod p , we can find $0 < x < p/2$ such that $x^2 + 1 \equiv 0 \pmod{p}$. Then $(x, 1)$ belongs to S , hence S is nonempty.

Let $(x_1, x_2) \in S$ be such that $x_1^2 + x_2^2$ is minimal; we claim that $x_1^2 + x_2^2 = p$. If this is not true, we must have

$$x_1^2 + x_2^2 = tp; \quad p > t > 1. \tag{1}$$

Then we can choose integers y_1, y_2 such that $x_i \equiv y_i \pmod{t}$ and $|y_i| \leq t/2$. Now $y_1^2 + y_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{t}$, hence $y_1^2 + y_2^2 = st$ for some integer s . Also $y_1^2 + y_2^2$

$\leq t^2/4 + t^2/4 < t^2$, hence $s < t$. Moreover x_1, x_2 cannot both be divisible by t , otherwise (1) would imply $t|p$, which is impossible; hence y_1, y_2 cannot both be 0, hence $s > 0$.

By the identity in the previous lemma we can write $(x_1^2 + x_2^2)(y_1^2 + y_2^2) = z_1^2 + z_2^2$ where $z_1 = x_1y_1 + x_2y_2$ and $z_2 = x_1y_2 - x_2y_1$. Now $z_1 \equiv x_1^2 + x_2^2 \equiv 0 \pmod t$ and $z_2 \equiv x_1y_1 - x_2y_1 \equiv 0 \pmod t$. Thus we may define integers $w_1 = \frac{z_1}{t}$, $w_2 = \frac{z_2}{t}$ and then we have

$$w_1^2 + w_2^2 = \frac{z_1^2 + z_2^2}{t^2} = \frac{(x_1^2 + x_2^2)(y_1^2 + y_2^2)}{t^2} = \frac{(tp)(st)}{t^2} = sp.$$

Since $0 < s < t$, this contradicts the minimality of $x_1^2 + x_2^2$. ■

We introduce the following terminology: for a prime number p , we define its *power in n* to be the largest integer a such that p^a divides n .

Theorem 3 *A positive integer n can be written as the sum of two squares if and only if every prime p of the form $4k + 3$ has even power in n .*

Proof. First suppose that every prime of the form $4k + 3$ has even power $2a$ in n . Then the corresponding prime power factors of n are sums of two squares $p^{2a} = (p^a)^2 + 0^2$. By the previous lemma all other odd prime factors are sums of two squares, as is $2 = 1^2 + 1^2$. Thus n is a product of sums of two squares and, by Lemma 1, n is itself a sum of two squares.

Now let $n = x^2 + y^2$ and write $x = du, y = dv$ where $d = \gcd(x, y)$, so that $x^2 + y^2 = d^2(u^2 + v^2)$. It suffices to show that if p is a prime of the form $4k + 3$ then p does not divide $u^2 + v^2$; for then the power of p in n will be twice its power in d , hence it will be even.

Assume to the contrary that p does divide $u^2 + v^2$. Now p cannot divide both u, v since they are coprime. Say p does not divide v and let \bar{v} be the inverse of $v \pmod p$. Then we get $(u\bar{v})^2 + 1 \equiv \bar{v}^2(u^2 + v^2) \equiv 0 \pmod p$. But this is impossible since -1 is not a quadratic residue for p of the form $4k + 3$. ■

2 Sums of four squares

We now consider the question: which integers are the sum of squares of four integers? Checking the previous list we see that every integer up to 17 can be so written. We also observe that 7 cannot be written as the sum of three squares.

Lemma 4 *If $n = n_1 \dots n_k$ and each n_i is a sum of four squares then so is n .*

Proof. This is proved just like Lemma 1 using the identity

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

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

. ■

Theorem 5 *Every positive integer is the sum of four squares.*

Proof. By the previous lemma it is enough to prove this for prime numbers. Indeed it suffices to treat primes of the form $p = 4k + 3$. (The others are sums of two squares and we can add two 0²s.)

Let S be the following set of quadruples of integers

$$S = \left\{ (x_1, x_2, x_3, x_4) : \sum x_i^2 \text{ is divisible by } p, \text{ and } p^2 > \sum x_i^2 > 0 \right\}.$$

We first show that S is not empty. Let $d > 1$ be the smallest quadratic non-residue mod p . Then $d - 1$ is a quadratic residue, as is $-d$ since we have $\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{d}{p}\right) = (-1)^{2k+1} (-1) = 1$. Therefore we can find a, b in $H(p)$ such that $a^2 \equiv d - 1 \pmod{p}$, $b^2 \equiv -d \pmod{p}$. Then we have $a^2 + b^2 + 1^2 + 0^2 \equiv d - 1 - d + 1 \equiv 0 \pmod{p}$. Since $a, b < p/2$ we get $0 < a^2 + b^2 + 1^2 + 0^2 < p^2/4 + p^2/4 + 1 < p^2$. Hence $(a, b, 1, 0)$ belongs to S .

Let $(x_1, x_2, x_3, x_4) \in S$ be such that $\sum x_i^2$ is minimal; then we claim that $\sum x_i^2 = p$. If this is not true, we must have

$$\sum x_i^2 = tp \text{ with } p > t > 1. \quad (2)$$

First suppose t is even. Two of the x_i , say x_1 and x_2 , must have the same parity. Since t is even, by (2) x_3 and x_4 must then have the same parity. Thus we can define integers $w_1 = (x_1 + x_2)/2$, $w_2 = (x_1 - x_2)/2$, $w_3 = (x_3 + x_4)/2$, $w_4 = (x_3 - x_4)/2$. Now we get

$$\sum w_i^2 = \left(\sum x_i^2\right)/2 = (t/2)p$$

which contradicts the minimality of $\sum x_i^2$.

If $t > 1$ is *odd*, we can choose integers y_1, y_2, y_3, y_4 such that $x_i \equiv y_i \pmod{t}$ and $|y_i| < t/2$. Then $\sum y_i^2 \equiv \sum x_i^2 \equiv 0 \pmod{t}$, hence $\sum y_i^2 = st$ for some integer s . Not all the x_i are divisible by t , otherwise (2) would imply $t|p$, which is impossible; hence some $y_i \neq 0$, hence $s > 0$. Also since $|y_i| < t/2$ we get $\sum y_i^2 < 4(t^2/4) = t^2$, hence $s < t$.

Now write $(\sum x_i^2)(\sum y_i^2) = \sum z_i^2$ as in the previous lemma. Since $x_i \equiv y_i \pmod{t}$ we get $z_1 \equiv \sum x_i^2 \equiv 0 \pmod{t}$. Also $z_2 \equiv (x_1x_2 - x_2x_1) + (x_3x_4 - x_4x_3) \equiv 0 \pmod{t}$, and similarly $z_3, z_4 \equiv 0 \pmod{t}$. Thus we may define integers $w_i = z_i/t$ for $i = 1, 2, 3, 4$ and then we have

$$\sum w_i^2 = \left(\sum z_i^2\right)/t^2 = \left(\sum x_i^2\right) \left(\sum y_i^2\right)/t^2 = (tp)(st)/t^2 = sp.$$

Since $0 < s < t$, once again we contradict the minimality of $\sum x_i^2$. ■