17 Sums of two squares

$$n = a^2 + b^2;\ a, b \geq 0,\ n \geq 1$$

Note:

$1 = 1^2 + 0^2$		$16 = 4^2 + 0^2$		$\underline{31 = --}$	$\leftarrow$
$\underline{2 = 1^2 + 1^2}$		$\underline{17 = 4^2 + 1^2}$		$32 = 4^2 + 4^2$	
$\underline{3 = --}$	$\leftarrow$	$18 = 3^2 + 3^2$		$33 = -$	
$4 = 2^2 + 0^2$		$\underline{19 = --}$	$\leftarrow$	$34 = 5^2 + 3^2$	
$\underline{5 = 2^2 + 1^2}$		$20 = 4^2 + 2^2$		$35 = -$	$\leftarrow$
$6 = -$		$21 = -$		$36 = 6^2 + 0^2$	
$\underline{7 = --}$	$\leftarrow$	$22 = -$		$\underline{37 = 6^2 + 1^2}$	
$8 = 2^2 + 2^2$		$\underline{23 = --}$	$\leftarrow$	$38 = -$	
$9 = 3^2 + 0^2$		$24 = -$		$39 = -$	$\leftarrow$
$10 = 3^2 + 1^2$		$25 = 5^2 + 0^2 = 4^2 + 3^2$		$40 = 6^2 + 2^2$	
$\underline{11 = --}$	$\leftarrow$	$26 = 5^2 + 1^2$		$\underline{41 = 5^2 + 4^2}$	
$12 = -$		$27 = -$	$\leftarrow$	$42 = -$	
$\underline{13 = 3^2 + 2^2}$		$28 = -$		$\underline{43 = --}$	$\leftarrow$
$14 = -$		$\underline{29 = 5^2 + 2^2}$			
$15 = -$	$\leftarrow$	$30 = -$			

For all integers a, b, we have

$$a^2 + b^2 \equiv 0, 1 \text{ or } 2 \pmod 4$$

Indeed, $a, b = 0, 1, 2, 3 \pmod 4 \ \Rightarrow a^2, b^2 \equiv 0, 1 \pmod 4 \ \Rightarrow a^2 + b^2 \equiv 0, 1, 2 \pmod 4$. So the numbers congruent to 3 mod 4 *cannot* be written as sums of 2 squares. It appears from this table that if p is an odd prime, we may write $p = a^2 + b^2$ iff $p \not\equiv 3$ mod 4.

Lemma A: If m, n are sums of 2 squares, then so is their product mn.

Proof: Use the identity $(A^2 + B^2)(x^2 + y^2) = (Ax + By)^2 + (Ay - Bx)^2$

Proposition A. Let p be a prime congruent to 1 mod 4. Then p is a sum of two squares in $\mathbb{Z}$.

Proof of Proposition A. First we claim that there exists integers A, B, m, with $1 \leq m < p$, such that

$$mp = A^2 + B^2 \tag{1}$$

Indeed, since $p \equiv 1 \pmod 4$, $(\frac{-1}{p}) = 1$ and so we can find $n \in \mathbb{Z}$ such that $n^2 \equiv -1 \pmod p$. It was proved earlier that the set $T : \{1, 2, \dots, \frac{p-1}{2}\}$ is a set of representatives for the **squares** in $(\mathbb{Z}/p)^*$. Hence we may choose $n \in T$ such that

$$n^2 + 1 = mp,$$

for some integer $m \geq 1$. Since $n < \frac{p}{2}$, we have:

$$m = \frac{1}{p}(n^2+1) < \frac{1}{p}\left(\frac{p^2}{4} + 1\right) < p,$$

which proves the claim.

Now there may be more than one m for which (1) holds. (Of course (A, B) will depend on m.). So we may, and we will, choose m to be the **smallest** integer ≥ 1 for which (1) holds. Of course, $m < p$. We are done if $m = 1$, so we will assume that $m > 1$ and derive a contradiction.

Find $x, y \in \mathbb{Z} \cap [-\frac{m}{2}, \frac{m}{2}]$ such that $x \equiv A \bmod m$, $y \equiv B \bmod m$.

Then

$$x^2 + y^2 = km, \text{ for some integer } k \geq 1, \tag{2}$$

$$\text{since } A^2 + B^2 \equiv \ 0 \bmod m.$$

By construction,

$$x^2 + y^2 \leq \frac{m^2}{4} + \frac{m^2}{4} = \frac{m^2}{2} = \frac{m}{2} \cdot m.$$

So $k < m$. Applying the identity proving Lemma 1, we obtain

$$(x^2+y^2)(A^2+B^2) = km \cdot mp = m^2 kp$$

$$= (Ax+By)^2 + (Ay-Bx)^2.$$

Notice that

$$Ay \equiv xy \equiv xB \pmod m.$$

So

$$m^2 | (Ay - Bx)^2,$$

and this gives

$$m^2 | (Ax + By)^2.$$

Hence $m|(Ax+By)$, and

$$\left(\frac{Ax+By}{m}\right)^2 + \left(\frac{Ay-Bx}{m}\right)^2 = kp. \tag{3}$$

Since $k < m$, and (3) gives a contradiction to the minimality of m.

Example: $p = 41$, $9^2 = 81 \equiv -1 \pmod p$

Start with $9^2 + 1^2 = 2 \cdot 41$, $x, y \in \mathbb{Z} \cap [-1, 1]$ such that $x \equiv 9 \pmod 2$, $y \equiv 1 \pmod 2$. Pick $x = y = 1$,

$$\frac{Ax+By}{m} = \frac{9 \cdot 1 + 1 \cdot 1}{2} = 5$$
$$\frac{Ay-Bx}{m} = \frac{9 \cdot 1 - 1}{2} = 4$$

This gives:

$$41 = 5^2 + 4^2.$$

Proposition C. Let p be a prime $\equiv 3 \bmod 4$. Then no integer n divisible precisely by an **odd** power of p can be written as a sum of two squares.

Theorem Let $n \geq 1$ be an integer. Then n can be written as a sum of two squares **iff** every prime $\equiv 3 \pmod 4$ occurs to a even power in its prime factorization.

Proof of Theorem (modulo Proposition C)
($\Rightarrow$): This is because Proposition C says that any prime congruent to 3 mod 4 has to occur to an even power r in n.
($\Leftarrow$): Let $r = p_1 p_2 \ldots p_m q_1^{2n} \ldots q_\ell^{2n_\ell}$, with $p_i \equiv 1 \bmod 4$, $q_j \equiv 3 \bmod 4$. By Prop. B, p_i is an sum of two squares, and $q_j^{2n_j} = (q_j^{n_1})^2 + 0^2$. Thus n is a product of numbers which are sums of two squares, and we are done by applying Lemma A.

Proof of Proposition C: Let $p \equiv 3 \pmod 4$ be a prime. Suppose

$$n = a^2 + b^2, \text{ with } p^{2s+1} \| n.$$

Let $d = (a, b)$, so that $d^2 | (a^2 + b^2) = n$. Hence

$$\left(\frac{n}{d}\right)^2 = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2, \text{ if } m = \frac{n}{d},\ x = \frac{a}{d},\ y = \frac{b}{d}.$$

So we get
$$m = x^2 + y^2, \text{ with } \gcd(x, y) = 1,$$
and
$$p^{2s+1} \| m.$$
In particular, $p|m$, but p does not divide both x and y. But if $p|x$, as $m = x^2 + y^2$, $p|y^2$, and so $p|y$. Consequently, $p \not| xy$.

It follows, since $(p, x) = 1$, that
$$Ax - Bp = t$$
is solvable in $\mathbb{Z}$ for all t. Take $t = y$ to get $Ax \equiv y \pmod p$.

Then
$$0 \equiv x^2 + y^2 \equiv x^2(A^2 + 1) \pmod p.$$
Since $p \not| x$, get:
$$A^2 + 1 \equiv 0 \pmod p.$$
But $(\frac{-1}{p}) = -1$ as $p \equiv 3 \bmod 4$, giving a contradiction.

Questions:

1. What if one considers sums of k squares with $k > 2$, e.g., $7 = 2^2 + 1^2 + 1^2 + 1^2$.

   In Section 19, we will prove that any positive integer can be written as a sum of four squares.

2. If $n = a^2 + b^2$, in how many ways can one write n as a sum of two squares?

   Example: $25 = 5^2 + 0^2 = 4^2 + 3^2$

   $65 = 8^2 + 1^2 = 7^2 + 4^2$

   Note in general that
$$\begin{aligned}(x^2 + y^2)(A^2 + B^2) &= (xA + yB)^2 + (xB - yA)^2 \\ &= (xA - yB)^2 + (xB + yA)^2\end{aligned}$$

   Example:
$$\begin{aligned}25 = 5 \cdot 5 &= +(2^2 + 1)(2^2 + 1) \\ &= (x \cdot 2 + 1 \cdot 1)^2 + (2 \cdot 1 - 1 \cdot 2)^2 = 5^2 + 0^2 \\ &= (2 \cdot 2 - 1 \cdot 1)^2 + (2 \cdot 1 - 1 \cdot 2)^2 = 3^2 + 4^2\end{aligned}$$

   When do these two ways of writing it coincide?

They do iff we have

$$(xA + yB)^2 = (xA - yB)^2$$

or

$$(xA + yB)^2 = (xB + yA)^2$$

First case:

Square both sides to get

$$xyAB = 0 \text{ i.e., at least one of } x, y, A, B \text{ is zero..}$$

Second case: Here we get

$$x^2A^2 + y^2B^2 = y^2A^2 + x^2B^2$$

$$\Leftrightarrow x^2(A^2 - B^2) + y^2(B^2 - A^2) = 0$$
$$\Leftrightarrow (x^2 - y^2)(A^2 - B^2) = 0$$
$$\Leftrightarrow x = y \text{ or } A = B$$

Claim: If $p \equiv 1 \pmod 4$ is a prime, then $p = a^2 + b^2$ uniquely.

Indeed, suppose $p = a^2 + b^2 = c^2 + d^2$, for $a, b, c, d \in \mathbb{Z}$. Then

$$a^2d^2 - b^2c^2 = (a^2 + b^2)d^2 - (c^2 + d^2)b^2 = p(d^2 - b^2)$$

$\Rightarrow ad \equiv bc \pmod p$, or $ad \equiv -bc \pmod p$.

Clearly $0 < a, b, c, d < \sqrt{p}$. So

$$ad \equiv bc, \text{ or } ad = p - bc.$$

If $ad = p - bc$

$$\begin{aligned} p^2 &= (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 \\ &= p^2 + (ac - bd)^2 \Rightarrow ac = bd \end{aligned}$$

Hence $a|bd$, and $\gcd(a, b) = 1$. $\Rightarrow a|d$. Also $d|ac$, and $\gcd(c, d) = 1$, so $d|a$. So $a = \pm d$, so $a = d$. $\Rightarrow b = c$.

If $ad = bc$, we find that $a = c$, $b = c$, and also $c = d$. Now the uniqueness assertion follows.