*Proposition:* If $n = a^2 + b^2$ , $p|n$ , and $p \equiv 3 \pmod 4$ , then $p|a$ and $p|b$ .

If not, then either $p \not| a$ or $p \not| b$ , say $p \not| a$ . Then $(a,p) = 1$, so there is a $z$ with $az \equiv 1 \pmod p$ . But then since $p|n$, $p|a^2 + b^2$, so $a^2 + b^2 \equiv 0 \pmod p$ . Then $1 + (bz)^2 = (az)^2 + (bz)^2 = z^2(a^2 + b^2) \equiv z^2 0 = 0 \pmod p$ , so $x = bz$ satisfies $x^2 + 1 \equiv 0 \pmod p$ , i.e., $x^2 \equiv -1 \pmod p$ , a contradication. So $p|a$ and $p|b$ .

(*) This means that $p^2|a^2$ and $p^2|b^2$ , so $p^2|a^2 + b^2 = n$ , and $(n/p^2) = (a/p)^2 + (b/2p)^2$ . This will be very significant shortly! The final peice of the puzzle is:

*Proposition:* If $p \equiv 1 \pmod 4$ and $p$ is prime, then $p = a^2 + b^2$ for some integers $a$ , $b$ .

To see this, set $k = \lfloor \sqrt{p} \rfloor$ = the largest integer $\leq p$ . Since $p$ is prime, $\sqrt{p}$ is not an integer, so $k < \sqrt{p} < k + 1$ . Because $p \equiv 1 \pmod 4$ , there is an $x$ with $x^2 \equiv -1 \pmod p$ . Now look at the collection of integers $u + xv$ for $0 \leq u \leq k$ and $0 \leq v \leq k$ . Since there are $(k + 1)^2 > p$ of them, at least two of them are congruent mod $p$; $u_1 + xv_1 \equiv u_2 + xv_2$ . Then $u_1 - u_2 \equiv xv_2 - xv_1 = x(v_2 - v_1)$ , so $(u_1 - u_2)^2 \equiv x^2(v_2 - v_1)^2 = -(v_2 - v_1)^2$ . Setting $a = u_1 - u_2$ and $b = v_2 - v_1$ , this means $p|a^2 + b^2$ . But since either $u_1 \neq u_2$ or $v_1 \neq v_2$ , $a^2 + b^2 > 0$ . Also, since $0 \leq u_1, u_2, v_1, v_2 \leq k$ , $|u_1 - u_2|, |v_2 - v_1| \leq k$ , so $a^2 + b^2 \leq k^2 + k^2 = 2k^2 < 2p$ . So $0 < a^2 + b^2 < 2p$ and is divisible by $p$ ; so $a^2 + b^2 = p$ , as desired.

So now we know that (1) the product of two sums of two squares is a sum of two squares, (2) 2 and any prime $\equiv 1 \pmod 4$ is a sum of two squares, and (3) and prime $\equiv 3 \pmod 4$ which divides $a^2 + b^2$ divides both $a$ and $b$. Putting these together, we can completely characterize which numbers can be expressed as $a^2 + b^2$ :

*Theorem:* If $n = 2^k p_1^{k_1} \cdots p_r^{k_r} q_1^{m_1} \cdots q_s^{m_s}$ is the prime factorization of $n$, where $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$ for every $i$ , then $n = a^2 + b^2$ for some integers $a, b \Leftrightarrow m_i$ is even for every $i$ .

The idea: use (*) above to show that if $n = a^2 + b^2$ then each of the primes $q_i$ can be divided out two at a time as $(n/q_i^2) = (a/q_i)^2 + (b/q_i)^2$ , until there are none left, showing that their exponents are all even. Conversely, (by induction) $2^k p_1^{k_1} \cdots p_r^{k_r}$ is a sum of two squares, since each factor is, and then since the remaining factor $q_1^{m_1} \cdots q_s^{m_s} = q_1^{2u_1} \cdots q_s^{2u_s} = (q_1^{u_1} \cdots q_s^{u_s})^2 + 0^2$ is a sum of squares, the product, $n$ , is a sum of two squares.

So, for example, since we know $p = 61 \cdot 2^{285652} + 1$ is prime and (as one of our class members pointed out!) $4|2^{285652}$ so $p \equiv 1 \pmod 4$ , this number can be expressed as the sum of two squares. Care to figure out which ones?