Tour 11 - Quadratic Residues

We say that a is a *quadratic residue modulo* m if there exists an integer x for which $x^2 \equiv a \pmod{m}$.

For example, let us determine the set of quadratic residues modulo 4.

If n is even, say $n = 2k$, then $n^2 = 4k^2 \equiv 0 \pmod{4}$.
If n is odd, say $n = 2k+1$, then $n^2 = 4k^2 + 4k + 1 \equiv 0 + 0 + 1 \equiv 1 \pmod{4}$.
So every perfect square must be congruent to either 0 or 1 modulo 4. In other words, the set of quadratic residues modulo 4 is $\{0, 1\}$. In other words, we know that *no* perfect square is congruent to either 2 or 3 modulo 4. Often this idea helps us in difficult problems.

Here are some useful facts to remember:

The set of quadratic residues modulo 3 is $\{0, 1\}$.
The set of quadratic residues modulo 4 is $\{0, 1\}$.
The set of quadratic residues modulo 5 is $\{0, 1, 4\}$.
The set of quadratic residues modulo 8 is $\{0, 1, 4\}$.
The set of quadratic residues modulo 10 is $\{0, 1, 4, 5, 6, 9\}$.

To determine the set of quadratic residues modulo m, how many perfect squares will we need to check? Clearly we don't have to check infinitely many of them, because $1^2 \equiv (m+1)^2 \pmod{m}$, $2^2 \equiv (m+2)^2 \pmod{m}$, etc. So we will need to check at *most* m perfect squares, from 0^2 to $(m-1)^2$. See if you can convince yourself that we can do far better – that we only need to check at most $\left\lfloor \frac{m}{2} \right\rfloor + 1$ perfect squares!

Here are some problems.

1. Determine all solutions in integers x and y to the equation $x^2 + y^2 = 2003$.
2. Prove that the sequence $\{11, 111, 1111, 11111, \ldots\}$ contains no perfect squares.
3. If $a^2 + b^2$ is a multiple of 7, prove that a and b must both be multiples of 7.
4. Find all solutions in positive integers to the equation $x^2 - 2y^2 = 3$.
5. If $2n + 1$ and $3n + 1$ are both perfect squares, show that n must be divisible by 40.
6. If a, b, and c are odd integers, prove that the polynomial $ax^2 + bx + c$ has no *rational* roots.

   We solved this question in Tour 1 *using parity. Use quadratic residues to solve this problem*
7. Find all solutions in integers to the equation $x^2 + y^2 = 3z^2$.