Worksheet 10: Quadratic Residues

1. Make a list of all quadratic residues mod 2, 3, 5, 7, and 11.

2. In this exercise, we'll prove another one of Euler's theorems: If p is an odd prime, then a is a quadratic residue mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

   (a) Prove the "$\Longrightarrow$" direction, e.g., by recalling another theorem by Euler.

   (b) For the "$\Longleftarrow$" direction, you may assume that there exits a primitive root r mod p (which is true, although we haven't prove it). Assuming $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, use the fact that $a \equiv r^n$ for some n, and show that n is even.

3. Use Euler's theorem to prove, given a primitive root r mod p (as above, an odd prime), that g^n is a quadratic residue mod p if and only if n is even. Conclude that, for an odd prime p, exactly half the integers between 1 and $p-1$ are quadratic residues mod p.

4. Let p be and odd prime not dividing a and b. Show that:

   (a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

   (b) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$

5. Andrews 9.2.2.

6. Write down a precise statement for each definition we have given this week. For each definition, give an example and a non-example.