Math 465 - Spring 2021 April 8th, 2021
Group Discussion 7

---

(1) Make a list of all quadratic residues mod 2, 3, 5, and 7.
(2) Prove our corollary from class: given a primitive root g mod p (an odd prime), that $a = g^n$ 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.
(3) Let p be and odd prime not dividing a and b. Using Euler's criterion, show that:
   (a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
   (b) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ (Think about the roots of $x^2 \equiv 1 \pmod{p}$...)
(4) Fill out the following table:

$\left(\frac{q}{p}\right)$	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
$q=3$					
$q=5$					
$q=7$					
$q=11$					
$q=13$					

Compare the rows and columns (e.g. how does $\left(\frac{p}{5}\right)$ compare to $\left(\frac{5}{p}\right)$)? Can you make any conjectures as to how these two values relate?