Math 370 Number Theory
Assignment # 10

1. For each of the following compute using i) the definition of quadratic residue ii) Euler's criterion (don't use online calculator) iii) Gauss's lemma iv) Eisenstein's Lemma (you have to wait until Tuesday for this)
   (a) $\left(\frac{3}{17}\right)$
   (b) $\left(\frac{5}{19}\right)$
   (c) $\left(\frac{9}{23}\right)$

2. (a) Let $n \in \mathbb{N}$ and $2 \leq a \leq n-2$. Show that if $a^3 \equiv a \pmod{n}$ then n is composite.
   (b) Let $a = 4739$ and $n = 8137$. Show that $a^3 \equiv a \pmod{n}$.
   (c) Is 8137 prime?

3. Let $p = 430113052620387572818669480533792426437631539710120391948802752968893868700640$
   $715121307573968744295199849494507677481572439566746330961863524112255985786120131219 66$
   $528441617544859650531431981027153706490087457636040754627102526646106541689834082438 10$
   $544457419057677762320558784133388955060049213295 53$

   and

   $q = 906984389687163078170449573416033716843255342786706657245842498930305145891622421 6$
   $894956268010549462452760313599163404782288157616471459222436868505726048097597875166 66$
   $672528892667552879094663197574176268088206860636347791797403638828113305131599659382 01$
   $881664095471620166198790366446884239682174984 1.$

   Calculate the following (don't use online calculator):
   (a) $\left(\frac{p-1}{p}\right)$
   (b) $\left(\frac{q-1}{q}\right)$
   (c) $\left(\frac{2}{p}\right)$
   (d) $\left(\frac{2}{q}\right)$

4. Let p be an odd prime. Find a formula for $\left(\frac{-2}{p}\right)$ that involves what p is congruent to mod 8.

5. Suppose that $p \geq 11$, show that there are two consecutive quadratic residues of p. (Hint think about $2, 5$ and 10).

6. Suppose that p is prime. Find the smallest positive $k \in \mathbb{Z}$ such that $a^k \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}$ such that $p \not| a$. Make sure to prove your answer.