Math 40520 Theory of Number
Homework 8

Due Wednesday 10/21

Do 4.

1. Let a be a nonzero integer.

   (a) Show that there exists at least one prime p such that $\left(\frac{a}{p}\right) = 1$. [Hint: You seek a prime p such that $a \equiv b^2 \pmod{p}$ for some integer b.]

   (b) Show that there are infinitely many primes p such that $\left(\frac{a}{p}\right) = 1$. [Hint: We did this in class for $a = -1$ and $a = -3$.]

2. Compute, using quadratic reciprocity, the Legendre symbol $\left(\frac{-123}{2017}\right)$.

3. Let $p > 5$ be a prime number and write $P = \{1, 2, \ldots, (p-1)/2\}$. Show that $x \in P$ is such that

$$5x \in 5P \cap (-P)$$

   if and only if

$$\left\lceil \frac{p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{5} \right\rfloor \quad \text{or} \quad \left\lceil \frac{3p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{2p-1}{5} \right\rfloor$$

   and conclude that for $p > 5$,

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 9 \pmod{20} \\ -1 & \text{if } p \equiv \pm 3, \pm 7 \pmod{20} \end{cases}$$

   and remark that this is equivalent to the simpler statement

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{5} \\ -1 & \text{if } p \equiv \pm 2 \pmod{5} \end{cases}$$

4. Let p be an odd prime. Suppose that $a \neq 0$ is a square mod p. Show that a is a square mod p^n for every $n \geq 1$.

5. Let $p > 3$ be a prime. What is the sum modulo p of all the quadratic residues mod p?

6. Show that $(x^2 - 13)(x^2 - 17)(x^2 - 13 \cdot 17) = 0$ has no rational solutions but has solutions modulo n for every positive integer n.

7. Determine all the rational solutions to the equation $x^2 + 2y^2 = 11$. [Hint: Parametrize these rational points with rational points along a line, as we did in class with Pythagorean triples.]