Review of arithmetic mod \( p \)

Throughout this handout, \( p \) will denote an odd prime \( p \geq 3 \). First we review some basic facts about arithmetic mod \( p \).

**Theorem 1.** If \( a \) and \( b \) are relatively prime positive integers, then there exist integers \( s \) and \( t \) such that \( as + bt = 1 \).

**Exercise 1.** Prove that if \( a \not\equiv 0 \mod p \), then \( a \) has a multiplicative inverse mod \( p \), i.e. there exists an integer \( b \) such that \( ab \equiv 1 \mod p \).

**Exercise 2.**

(a) Calculate the inverse of 4 mod 5.

(b) Calculate the inverse of 3 mod 11.

(c) Calculate the inverse of 2 mod 7.

**Exercise 3.**

(a) Prove that \( x^2 \equiv 1 \mod p \) if and only if \( x \equiv \pm 1 \mod p \). (Hint: \( p \) divides \( x^2 - 1 \). Factor and use a property of prime numbers).

(b) Prove that \( x^2 \equiv y^2 \mod p \) if and only if \( x \equiv \pm y \mod p \). (Hint: Exercise 1).

**Exercise 4** (CHALLENGE). Prove Theorem 1. More generally, prove that if \( a \) and \( b \) are any two positive integers, then there are integers \( s \) and \( t \) such that \( as + bt = \gcd(a, b) \).

Also, recall our favorite theorem from the Gaussian integers unit:

**Theorem 2** (Fermat’s Little Theorem). If \( a \not\equiv 0 \mod p \), then \( a^{p-1} \equiv 1 \mod p \).

**Quadratic residues modulo \( p \) and the Legendre symbol**

**Definition 1.** If \( a \not\equiv 0 \mod p \), we say \( a \) is a quadratic residue modulo \( p \) if there is some \( b \) such that \( b^2 \equiv a \mod p \). If there is no such \( b \), then we say \( a \) is a quadratic nonresidue modulo \( p \).

**Exercise 5.**

(a) List all the quadratic residues modulo 5.

(b) List all the quadratic residues modulo 11.

Note that we can determine the quadratic residues modulo \( p \) by squaring each of \( \{1, 2, \ldots, p - 1\} \).

**Exercise 6.** Prove that exactly half of the elements \( \{1, 2, \ldots, p - 1\} \) are quadratic residues modulo \( p \) (Hint: square the values and figure out how many of these are distinct).

**Definition 2.** If \( p \) is an odd prime, the Legendre symbol is defined as

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue mod } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue mod } p \\
0 & \text{if } a \equiv 0 \mod p.
\end{cases}
\]

**Exercise 7.** Calculate the following Legendre symbols

(a) \( \left( \frac{2}{7} \right) \) and \( \left( \frac{3}{7} \right) \)

(b) \( \left( \frac{3}{13} \right) \) and \( \left( \frac{-3}{13} \right) \)

**Exercise 8.** Let \( a \) be any integer. Prove that the number of integers \( x \in \{0, 1, \ldots, p - 1\} \) such that \( x^2 \equiv a \mod p \) is exactly \( 1 + \left( \frac{a}{p} \right) \).
Euler’s Criterion

We will now introduce a way of calculating the Legendre symbol in general.

**Theorem 3** (Euler’s Criterion). If $p$ is an odd prime, then for any residue class $a$, \( \left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p} \).

**Exercise 9.** Prove Euler’s Criterion.

(a) Prove Euler’s Criterion in the case \( \left( \frac{a}{p} \right) = 0 \).

(b) Let $a \neq 0 \pmod{p}$ and let $u$ be a primitive root mod $p$. Then recall that there is a unique integer $k \in \{0, 1, \ldots, p-1\}$ such that $u^k \equiv a \pmod{p}$. Prove that $a$ is a quadratic residue mod $p$ if and only if $k$ is even.

(c) Prove Euler’s Criterion in the case \( \left( \frac{a}{p} \right) = 1 \). (Hint: Fermat’s Little Theorem).

(d) Finally, consider the case \( \left( \frac{a}{p} \right) = -1 \). Let $u$ be the primitive root mod $p$ from part (b). Prove that $a^{(p-1)/2} \equiv u^{(p-1)/2} \pmod{p}$.

(e) Prove that $a^{(p-1)/2} \equiv -1 \pmod{p}$, completing the proof. (Hint: Fermat’s Little Theorem and Exercise 3).

In proving which integers are the sum of two squares, we showed that $-1$ is a square modulo $p$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. We can restate this problem in terms of quadratic residues.

**Exercise 10.** Prove that $-1$ is a quadratic residue modulo $p$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$ (Hint: use Euler’s Criterion).

**Exercise 11.** (a) Prove that \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \) for any integers $a, b$.

(b) Explain what the Legendre symbol being multiplicative means in terms of quadratic residues.

**Quadratic Reciprocity**

We are almost ready to state the core theorem of the handout.

**Exercise 12.** (a) Compute \( \left( \frac{5}{13} \right) \) and \( \left( \frac{13}{5} \right) \).

(b) Compute \( \left( \frac{3}{11} \right) \) and \( \left( \frac{11}{3} \right) \).

(c) Compute \( \left( \frac{7}{2} \right) \) and \( \left( \frac{2}{7} \right) \).

(d) Do you notice any patterns?

**Theorem 4** (Quadratic Reciprocity). Let $p$ and $q$ be distinct odd primes.

\[
\begin{cases}
\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\
\left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right) & \text{if } p \equiv q \equiv 3 \pmod{4}
\end{cases}
\]

**Exercise 13.** An equivalent formulation of quadratic reciprocity is if $p$ and $q$ are distinct odd primes, then

\[ \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}. \]

Show that this gives the same result.

**Exercise 14.** (a) Is 149 a quadratic residue mod 197? (you may assume these are both prime)

(b) Is 47 a quadratic residue mod 349? (same assumption)