Quadratic Reciprocity I

Matthew Gherman and Adam Lott

High School I – 10/28/18

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 $a \not\equiv 0 \bmod p$, then a has a multiplicative inverse mod p, i.e. there exists an integer b such that $ab \equiv 1 \bmod p$.

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

(b) Prove that $x^2 \equiv y^2 \bmod p$ if and only if $x \equiv \pm y \bmod p$. (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 $a \neq 0 \bmod p$, then $a^{p-1} \equiv 1 \bmod p$.

Quadratic residues modulo p and the Legendre symbol

Definition 1. If $a \not\equiv 0 \bmod p$, we say a is a *quadratic residue* modulo p if there is some b such that $b^2 \equiv a \pmod p$. 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

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

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 $x^2 \equiv a \bmod p$ 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 $a \neq 0 \bmod p$ 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 $u^k \equiv a \bmod p$. 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 $a^{(p-1)/2} \equiv u^{(p-1)/2} \bmod p$.

(e) Prove that $a^{(p-1)/2} \equiv -1 \bmod p$, 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 $p \equiv 1 \pmod p$ (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 $\left(\frac{5}{7}\right)$ and $\left(\frac{7}{5}\right)$.

(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)

Quadratic Reciprocity II

Matthew Gherman and Adam Lott

High School I – 11/4/18

Quadratic Reciprocity

To review last week's handout, we state the main theorem and work through a few difficult examples.

Theorem 1 (Quadratic Reciprocity)**.** Let p and q be distinct odd primes.

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

An equivalent formulation of quadratic reciprocity is if p and q are distinct odd primes, then

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

Exercise 1. (a) Is 357 a quadratic residue mod 661? (note only 661 is prime)

(b) Is 243 a quadratic residue mod 419? (note only 419 is prime)

Applications of Quadratic Reciprocity

Given some integer a, we can now determine for which values of an odd prime p is a a quadratic residue modulo p.

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

Exercise 3. Characterize the primes for which 3 is a quadratic residue. (Hint: break into cases)

As we saw in the worksheet last week, computing Legendre symbols with 2 is not trivial. The following more difficult theorem shows us when 2 is a quadratic residue modulo an odd prime p.

Theorem 2. If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Exercise 4 (CHALLENGE)**.** Prove Theorem 2.

Exercise 5. Show that Theorem 2 is equivalent to $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3, 5 \pmod 8$.

Exercise 6. Is 173 a quadratic residue mod 197? (You may assume these are both prime)

Exercise 7. Characterize the primes for which 6 is a quadratic residue. (Hint: Exercise 3 and Theorem 2)

More applications

Another surprising application of quadratic reciprocity is that it can give us information about which primes divide the values taken by certain polynomials. For example, are there any defining characteristics of primes that divide numbers of the form $n^2 + n + 7$? Let's find out.

Exercise 8. (a) Prove that $n^2 + n + 7$ is odd for any integer n.

(b) Suppose that p is a prime dividing a number of the form $n^2 + n + 7$. Show that $(2n + 1)^2 \equiv -27 \bmod p$. Conclude that if p divides $n^2 + n + 7$, then -27 is a square mod p.

(c) If $p = 3$, clearly -27 is a square mod p. Assume $p \geq 5$. Prove that if p divides $n^2 + n + 7$, then $p \equiv 1 \bmod 6$. (Hint: use the previous section).

(d) Conclude that any prime divisor p of a number of the form $n^2 + n + 7$ satisfies either $p = 3$ or $p \equiv 1 \bmod 6$.

Exercise 9. Prove that there are infinitely many primes p such that $p \equiv 1 \bmod 6$.

(a) Suppose there are only finitely many. Let $\{7, p_1, p_2, \ldots, p_N\}$ be a list of them all and let $m = 3 \cdot p_1 \cdots p_N$. Show that $m^2 + m + 7$ is not divisible by 3 or by any of the p_j.

(b) Conclude that there are infinitely many primes $\equiv 1 \bmod 6$. (Hint: prime factorization).

A third application

Exercise 10. Suppose that n is odd, $a \not\equiv 0 \bmod p$, and p divides $a^n - 1$.

(a) Show that $a^{n+1} \equiv a \bmod p$.

(b) Prove $\left(\frac{a}{p}\right) = 1$.

Exercise 11. Let $m, n \geq 2$ and suppose $2^m - 1$ divides $3^n - 1$. Prove that n is even.

(a) Suppose that n is odd. Let p be any prime dividing $2^m - 1$. Show that $\left(\frac{3}{p}\right) = 1$. (Hint: Exercise 10).

(b) If $p \equiv 1 \bmod 4$, show that also $p \equiv 1 \bmod 12$. (Hint: use quadratic reciprocity and knowledge about squares mod 3).

(c) If $p \equiv 3 \bmod 4$, show that $p \equiv -1 \bmod 12$.

(d) Conclude that every prime divisor of $2^m - 1$ is either $\pm 1 \bmod 12$. Use this to arrive at a contradiction.