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.