1 First Quadratic Reciprocity Theorem

Recall that we were exploring the Legendre Symbol \( \left( \frac{-1}{p} \right) \) at the end of last week’s worksheet. For different odd values of \( p \), we get different values. For \( \{5, 13, 17, 29, 37, \ldots \} \) we can calculate \( \left( \frac{-1}{p} \right) = 1 \) and for \( \{3, 7, 11, 19, 23, 31, \ldots \} \) we can calculate \( \left( \frac{-1}{p} \right) = -1 \). Notice that the difference between the primes in the same lists are multiples of 4. Thus, we can conjecture the following:

\[
\left( \frac{-1}{p} \right) = \begin{cases} 
1 & p \equiv 1 \mod 4 \\
-1 & p \equiv 3 \mod 4 
\end{cases}
\]

It turns out that this is true. We will prove it below.

**Problem 1** Let \( p \) be an odd prime, and \( A = a^{(p-1)/2} \). What is the value of \( A^2 \mod p \)?

**Problem 2** Using the previously calculated value of \( A^2 \mod p \), conclude that \( p \mid A - 1 \) or \( p \mid A + 1 \). What are the only 2 possible values of \( A \mod p \)?

**Problem 3** Let \( p \) an odd prime, a a QR mod \( p \). Show that \( a^{(p-1)/2} \equiv 1 \mod p \). Thus, what is the set of roots to the equation \( x^{(p-1)/2} - 1 \equiv 0 \mod p \). Recall there are exactly \( \frac{p-1}{2} \) QR’s.
Problem 4 Let $p$ an odd prime, $a$ a NR mod $p$. Consider the equation $x^{p-1} \equiv 1 \mod p$. Show that $a^{(p-1)/2} + 1 \equiv 0 \mod p$. (Hint: Use problem 3)

Problem 5 Using problems 3 and 4, conclude that $a^{(p-1)/2} \equiv (\frac{-1}{p}) \mod p$. This is known as Euler’s criterion
Problem 6 Calculate, using problem 5, the following Legendre Symbols given the denominators are all prime: \((\frac{-1}{53})\), \((\frac{-1}{6911})\), \((\frac{-1}{7817})\).

Problem 7 (Quadratic Reciprocity part I) Let \(p\) be an odd prime. Show that
\[
(\frac{-1}{p}) = \begin{cases} 
1 & p \equiv 1 \mod 4 \\
-1 & p \equiv 3 \mod 4
\end{cases}
\]
Problem 8 (CHALLENGE) Show there are infinitely many primes $p$ such that $p \equiv 1 \mod 4$. (Hint: Start with a list of primes, $p_1, p_2, \ldots, p_n$ all congruent to 1 mod 4. Consider $A = q_1 q_2 \ldots q_m$ prime factorization. Show some factor is congruent to 1 mod 4.)
2 Second Quadratic Reciprocity Theorem

Example 1 We could do a similar thing as we did previously to calculate values of \( \left( \frac{2}{p} \right) \), and eventually we could conjecture that

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & p \equiv 1, 7 \mod 8 \\
-1 & p \equiv 3, 5 \mod 8 
\end{cases}
\]

Let’s try to outline a way we could prove this. Consider \( p = 13 \). Then, by Euler’s Criterion we know that \( 2^{(p-1)/2} = \left( \frac{2}{p} \right) \). Now, consider the numbers 1, 2, 3, 4, 5, 6 the first half of the nonzero numbers up to \( p = 13 \), the first \( \frac{p-1}{2} \) numbers. Let’s multiply each of these numbers by 2: 2, 4, 6, 8, 10, 12. Notice that the product of these are:

\[
2 \times 4 \times 6 \times 8 \times 10 \times 12 = (2 \times 1)(2 \times 2)(2 \times 3)(2 \times 4)(2 \times 5)(2 \times 6) = 2^6 \times 6!
\]

We can see that \( 2^6 \) appears on the RHS which is exactly what we want to calculate. Now, instead of multiplying 2, 4, 6, 8, 10, 12 directly, let’s try to reduce these each to an integer between \( -\frac{p-1}{2} \) and \( \frac{p-1}{2} \), i.e. \(-6, 6\). We get:

2, 4, 6, -5, -3, -1. Thus, we can conclude that

\[
2 \times 4 \times 6 \times 8 \times 10 \times 12 = 2 \times 4 \times 6 \times (-5) \times (-3) \times (-1) = (-1)^3 \times 6!
\]

Problem 9 In the above example, can we conclude \( 2^6 \equiv (-1)^3 \mod 13? \) Equivalently, can we conclude \( (-1)^3 \equiv \left( \frac{2}{p} \right) \mod 13? \) Why or why not?

Notice that the numbers that we had to reduce to the range were exactly the numbers strictly larger than \( \frac{p-1}{2} \). Thus, all we have to do is count the number of integers in the list (after multiplication by 2) that are larger than \( \frac{p-1}{2} \).
Problem 10 Suppose $p \equiv 1 \mod 8$. Show that $\left(\frac{2}{p}\right) = 1$. (HINT: Rewrite $p = 8k + 1$, and repeat the process on page 5)
**Problem 11 (OPTIONAL)** Prove the rest of the Second Quadratic Reciprocity Theorem using similar techniques as in problem 10 i.e. show that

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & p \equiv 1, 7 \mod 8 \\
-1 & p \equiv 3, 5 \mod 8 
\end{cases}
\]
3 Third Quadratic Reciprocity Theorem

Theorem 1 (THIRD QUADRATIC RECIPROCITY THEOREM) Suppose $p, q$ are odd primes. Then

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

Equivalently, $\left( \frac{p}{q} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left( \frac{q}{p} \right)$

Problem 12 Using everything from this worksheet, compute the following values: $\left( \frac{85}{101} \right), \left( \frac{29}{541} \right), \left( \frac{101}{1987} \right)$