Proof of Quadratic Reciprocity

Reading

- Section 11.5
- Section 11.6

Practice Problems

11.5 1-12
11.5 (Challenge, optional) 22
11.6 1-6

Notes

Eisenstein's Lemma

A key component of the proof of quadratic reciprocity is Eisenstein's Lemma, which is a rather surprising:

> **Eisenstein's Lemma**
>
> Let $p > 2$ be prime and a be an *odd* number that is not a multiple of p. Let q_k be the quotient when dividing $a \cdot k$ by p. Then we define the quantity:
>
> $$T(a,p) = q_1 + q_2 + \cdots + q_{\frac{k-1}{2}}$$
>
> Then:
>
> $$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

Eisenstein's Lemma offers us yet another way to compute the Legendre Symbol. Let us look at an example, before discussing the proof.

Consider $p = 13$ and $a = 3$. We have:

- $3 \cdot 1 = 3 = 0 \cdot 13 + 3$. $q_1 = 0$.
- $3 \cdot 2 = 6 = 0 \cdot 13 + 6$. $q_2 = 0$.
- $3 \cdot 3 = 9 = 0 \cdot 13 + 9$. $q_3 = 0$.
- $3 \cdot 4 = 12 = 0 \cdot 13 + 12$. $q_4 = 0$.
- $3 \cdot 5 = 15 = 1 \cdot 13 + 2$. $q_5 = 1$.
- $3 \cdot 6 = 18 = 1 \cdot 13 + 5$. $q_6 = 1$.
- $T(3, 13) = 0 + 0 + 0 + 0 + 1 + 1 = 2$.

According to Eisenstein's Lemma, this means that 3 is a quadratic residue modulo 13.

Let us try the same with 5:

- $5 \cdot 1 = 5 = 0 \cdot 13 + 5$. $q_1 = 0$.
- $5 \cdot 2 = 10 = 0 \cdot 13 + 10$. $q_2 = 0$.
- $5 \cdot 3 = 15 = 1 \cdot 13 + 2$. $q_3 = 1$.
- $5 \cdot 4 = 20 = 1 \cdot 13 + 7$. $q_4 = 1$.
- $5 \cdot 5 = 25 = 1 \cdot 13 + 12$. $q_5 = 1$.
- $5 \cdot 6 = 30 = 2 \cdot 13 + 4$. $q_6 = 2$.
- $T(5, 13) = 0 + 0 + 1 + 1 + 1 + 2 = 5$.

According to Eisenstein's Lemma, this would mean that 5 is a quadratic nonresidue modulo 13.

Proof of Eisenstein's Lemma

It is time to prove Eisenstein's Lemma, not the easiest of proofs:

We start with carrying out the divisions for $k = 1, \ldots, h = \frac{p-1}{2}$:

$$a \cdot k = q_k p + r_k$$

Where the r_k are the remainders. In accordance to what we looked at earlier, we will define the "signed" remainders:

$$s_k = \begin{cases} r_k - p & \text{if } r_k > \frac{p-1}{2} \\ r_k & \text{if } r_k \leq \frac{p-1}{2} \end{cases}$$

So s_k are the positive/negative residues we looked at previously. Notice:

$$r_1 + r_2 + \cdots + r_h = (s_1 + s_2 + \cdots + s_h) + g \cdot p$$

where g is as defined previously.

We then add all those formulas up:

$$a(1 + 2 + \cdots + h) = T(a, p) \cdot p + (s_1 + s_2 + \cdots + s_h) + g \cdot p$$

We will examine this relation modulo 2, as we are only interested at the end of the day in raising -1 to those powers. Because a and p are both odd, the above formula becomes:

$$1 + 2 + \cdots + h = T(a, p) + (s_1 + s_2 + \cdots + s_h) + g$$

Recall that the s_k are just a permutation of the $1, 2, \ldots, h$, with some signs thrown in. Since we are computing modulo 2, the signs do not matter. Therefore the sum $s_1 + s_2 + \cdots + s_h$ will cancel out the sum $1 + 2 + \cdots + h$. Therefore we get:

$$T(a, p) = -g = g \bmod 2$$

This completes the proof of Eisenstein's Lemma.

Visualizing Eisenstein's Lemma

A key aspect of using Eisenstein's Lemma for the proof of Quadratic Reciprocity is a visualization of the lemma.

> Consider the triangle defined by the lines $y = \frac{q}{p}$, $y = 0$ and $x = \frac{p}{2}$.
>
> Then $T(q, p)$ is equal to the number of "lattice points" in the triangle. Lattice points are points with integer coordinates.

To see this, consider an k between 1 and h. Then the lattice points under discussion are points (k, y) where $y \leq \frac{q}{p}k$. The largest one of those values y would be what we previously denoted as q_k. So there are exactly q_k such values. Adding over all k from 1 to h results in $T(q, p)$.

Proof of Quadratic Reciprocity

Finally it is time to finish the proof of our quadratic reciprocity law. It will boil down to the following:

> If $p \neq q$ are odd primes, then:
>
> $$T(p, q) + T(q, p) = \frac{p-1}{2} \times \frac{q-1}{2}$$

If we take this for granted for the moment, let us review how this relates to the law of quadratic reciprocity:

- Quadratic Reciprocity was restated equivalently as $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$.
- We showed in steps that $\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}} = (-1)^g = (-1)^{T(q,p)}$.
- We now show that $T(p, q) + T(q, p) = \frac{p-1}{2} \times \frac{q-1}{2}$.

- We will now be able to say:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{T(q,p)+T(p,q)} = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$$

  And this completes the proof.

Now what is left is to prove the formula for $T(p,q)$. There is a very elegant argument to it.

Consider the rectangle with opposing vertices at $(0,0)$ and $\left(\frac{p}{2},\frac{q}{2}\right)$. The diagonal through those vertices has equation $y = \frac{q}{p}x$ and splits it in 2 triangles.

We now examine the points with integer coordinates (starting at 1) that lie in that rectangle. There are $\frac{p-1}{2} \times \frac{q-1}{2}$ such points. They are split between the two triangles. Those triangles are what we examined earlier. The points in the lower right one are $T(q,p)$, those in the upper left are $T(p,q)$. This gives us the desired property.