A PROOF OF QUADRATIC RECIPROCITY (MATH 4573)

INSTRUCTOR: TYLER GENAO

In this note, we will prove the classical theorem of quadratic reciprocity, which relates the Legendre symbols of two odd primes with respect to one another. There are 332 known proofs of quadratic reciprocity, see here. We've opted to go with a proof that's a balance of being "minimally technical" and not too long. However, since we are not using higher-level results from algebraic number theory to prove this, we will have to get quite involved with calculations!

Theorem. [NZM91, Theorem 3.4] *If $p, q \in \mathbb{Z}^+$ are distinct odd primes, then*

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

i.e.,

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

In other words,

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

Quadratic reciprocity can be very useful when calculating Legendre symbols. For example, at first glance calculating $\left(\frac{3}{101}\right)$ may seem tough, but since $101 \equiv 1 \pmod 4$, we have by quadratic reciprocity that

$$\left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1;$$

thus, we know that 3 is not a square modulo 101.

Proof of quadratic reciprocity. This proof is credited to George Rousseau [Rou91]. This proof only uses the Chinese remainder theorem, Wilson's Theorem and Euler's Criterion. In this proof, for $n \in \mathbb{Z}^+$ we will write $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. Thus, our unit groups are written as $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$. We will sometimes use brackets, such as $[k]$, to denote a congruence class (where the modulus should be clear from context).

The plan of this proof is to split $\mathbb{Z}_{pq}^\times$ into two halves (one half being denoted H_1), where every element $[k] \in \mathbb{Z}_{pq}^\times$ is such that either $[k] \in H_1$ or $[-k] \in H_1$. We will also split $\mathbb{Z}_q^\times$ into halves in $\mathbb{Z}_{pq}^\times$ (one half being denoted H_2), and produce an equality which relates the product of elements in H_1 and H_2 (this is Equation (1)). Finally, we'll simplify these product and the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ will appear, and we'll deduce quadratic reciprocity from this.

Let us define our halves,

$$H_1 := \left\{ [k] \in \mathbb{Z}_{pq}^\times : 1 \leq k < \frac{pq}{2} \right\}$$

and

$$H_2 := \left\{ (a,b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times : 1 \leq b < \frac{q}{2} \right\}.$$

By the CRT, we have a natural group isomorphism

$$\Phi \colon \mathbb{Z}_{pq}^\times \xrightarrow{\sim} \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times.$$

Thus, for all $(a,b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$, there exists a *unique* $1 \leq k < pq$ with $k \equiv a \pmod{p}$ and $k \equiv b \pmod{q}$, i.e., $\Phi([k]) = (a,b)$.

(1) If $1 \leq k < \frac{pq}{2}$, then
$$\Phi([k]) = (a,b)$$
and there's nothing to note.

(2) If $\frac{pq}{2} \leq k < pq$, then $1 \leq pq - k < \frac{pq}{2}$, and $\Phi([pq-k]) = \Phi([-k]) = -\Phi([k]) = -(a,b)$. (Note that $[pq-k]$ is in H_1.)

Thus, for every element $(a,b) \in H_2$, there exists unique $1 \leq k < pq$ such that either $k \in H_1$ or $pq - k \in H_1$. Therefore, **as a product of elements in** $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$**,** we have

$$\prod_{(a,b) \in H_2} (a,b) = \epsilon \cdot \prod_{k \in H_1} (k,k), \tag{1}$$

where $\epsilon \in \{\pm 1\}$ (ϵ is a product of the negative signs for the pairs $(a,b) \in H_2$ which which correspond to $1 \leq k < pq$ with $pq - k \in H_1$); keep in mind that in these pairs (a,b) and (k,k), the first coordinate is mod p, and the second coordinate is mod q. Thus, we've split up H_2 in $\mathbb{Z}_{pq}^\times$ using H_1.

We will simplify each side of (1) individually, and then equate them to deduce quadratic reciprocity. We'll first simplify the left hand side.

Before we begin, let us set $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$. After each step of our calculation, we will make a comment explaining it. We calculate

$$\prod_{(a,b) \in H_2} (a,b) = \prod_{\substack{1 \leq a < p, \\ 1 \leq b < \frac{q}{2}}} (a,b) = ((p-1)!^Q, Q!^{p-1}),$$

noting that $Q = \frac{q-1}{2}$ is the greatest positive integer below $\frac{q}{2}$ (the exponents come from the number of choices for b and a);

$$= ((p-1)!^Q, Q!^{2P}),$$

by definition of $P = \frac{p-1}{2}$;

$$= ((-1)^Q, Q!^{2P}),$$

by Wilson's theorem modulo p;

$$= ((-1)^Q, ((q-1)!(-1)^Q)^P)),$$

by the claim that $(\left(\frac{q-1}{2}\right)!)^2 \equiv (-1)^{\frac{q-1}{2}} \cdot (q-1)! \pmod q$ (this will be a homework problem);

$$= ((-1)^Q, ((-1)^{Q+1})^P),$$

by Wilson's theorem modulo q;

$$= ((-1)^Q, (-1)^{PQ+P}).$$

Thus, we've shown that

$$\prod_{(a,b)\in H_2} (a,b) \equiv ((-1)^Q, (-1)^{PQ+P}). \tag{2}$$

Next we will simplify the right hand side of (1), namely

$$\epsilon \cdot \prod_{k\in H_1} (k,k).$$

We we will do this one coordinate at a time. **Modulo p,** we check that

$$\prod_{k\in H_1} k = \prod_{\substack{1\le k<\frac{pq}{2}:\\ \gcd(k,pq)=1}} k = \left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ p\nmid k}} k\right)\cdot\left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ q\mid k}} k\right)^{-1},$$

the latter equality coming from the fact that we can divide by the integers divisible by q, to be left with a product of integers coprime to q;

$$= \left(\prod_{0<k<p} k \cdot \prod_{p<k<2p} k \cdot \prod_{2p<k<3p} k \cdots \prod_{(Q-1)p<k<Qp} k \cdot \prod_{Qp<k<\frac{pq}{2}} k\right)\cdot\left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ q\mid k}} k\right)^{-1},$$

where we've explicitly written out our product of integers coprime to p (which are the non-multiples of p) – note that the blue product might have less terms involved, and only goes up to $\frac{pq}{2}$);

$$= \left(\underbrace{(p-1)!\cdot(p-1)!\cdot(p-1)!\cdots(p-1)!}_{Q \text{ times}}\cdot \prod_{Qp<k<\frac{pq}{2}} k\right)\cdot\left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ q\mid k}} k\right)^{-1},$$

since each product $\prod_{jp<k<(j+1)p} k$ in the numerator for $0 \le j < Q$ is congruent to $(p-1)!$ mod p;

$$\left((p-1)!^Q \cdot \prod_{Qp<k<\frac{pq}{2}} k\right)\cdot\left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ q\mid k}} k\right)^{-1} = \left((p-1)!^Q \cdot P!\right)\cdot\left(\prod_{\substack{1\le k<\frac{pq}{2}:\\ q\mid k}} k\right)^{-1},$$

which follows from the fact that every integer $Qp < k < \frac{pq}{2}$ has the form $k = \ell + Qp$, with $1 \leq \ell \leq \frac{p-1}{2}$ – this is also a HW problem;

$$= \frac{(p-1)!^Q \cdot P!}{q \cdot 2q \cdot 3q \cdots Pq},$$

since $\prod_{\substack{1 \leq k < \frac{pq}{2}: \\ q|k}} k \equiv q \cdot 2q \cdot 3q \cdots Pq \pmod{p}$ – part of this is also a HW problem;

$$= \frac{(p-1)!^Q \cdot P!}{q^P \cdot P!} = \frac{(p-1)!^Q}{q^P} \equiv \frac{(-1)^Q}{q^P},$$

by Wilson's theorem modulo p;

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

by Euler's criterion for the Legendre symbol, see [NZM91, Theorem 3.1];

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

Thus, we conclude by our work above that

$$\prod_{k \in H_1} k \equiv (-1)^Q \cdot \left(\frac{q}{p}\right) \pmod{p}.$$

By a symmetric argument (where we switch the p's and q's in our work above, as well as the P's and Q's), we can also conclude that

$$\prod_{k \in H_1} k \equiv (-1)^P \cdot \left(\frac{p}{q}\right) \pmod{q}.$$

We can now substitute our conclusions above into (1): this equation

$$\prod_{(a,b) \in H_2} (a,b) = \epsilon \cdot \prod_{k \in H_1} (k,k)$$

now becomes

$$((-1)^Q, (-1)^{PQ+P}) = \left(\epsilon \cdot (-1)^Q \cdot \left(\frac{q}{p}\right), \epsilon \cdot (-1)^P \cdot \left(\frac{p}{q}\right)\right).$$

From the first coordinate equality, we have

$$(-1)^Q \equiv \epsilon \cdot (-1)^Q \cdot \left(\frac{q}{p}\right) \pmod{p},$$

i.e.,

$$1 \equiv \epsilon \cdot \left(\frac{q}{p}\right) \pmod{p}.$$

Thus,

$$p \mid \left(1 - \epsilon \cdot \left(\frac{q}{p}\right)\right);$$

since $\left|1 - \epsilon \cdot \left(\frac{q}{p}\right)\right| \leq 2 < p$, this forces $1 - \epsilon \cdot \left(\frac{q}{p}\right) = 0$ (by e.g. [NZM91, Theorem 1.1.(5)]) and thus

$$1 = \epsilon \cdot \left(\frac{q}{p}\right),$$

so that

$$\epsilon = \left(\frac{q}{p}\right).$$

A similar argument on the second coordinate equality shows that

$$(-1)^{PQ+P} = \epsilon \cdot (-1)^P \cdot \left(\frac{p}{q}\right),$$

so that

$$\epsilon = (-1)^{PQ} \cdot \left(\frac{p}{q}\right).$$

Equating these two expressions for ϵ, we conclude that

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

i.e.,

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

This proves quadratic reciprocity. □

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).

[Rou91] G. Rousseau, *On the quadratic reciprocity law*, J. Austral. Math. Soc. Ser. A (1991), no. 3, 423–425.