Quadratic Reciprocity

Taylor Dupuy

Throughout this note p and q will denote distinct odd primes. The **Legendre Symbol** is given by

$$\left(\frac{n}{p}\right) = \left\{ \begin{array}{cc} 1, & n \text{ is a square modulo } p \\ 0, & p|n \\ -1, & \text{otherwise} \end{array} \right. . \tag{1}$$

Theorem 1 (Law of Quadratic Reciprocity)**.** *For p and q distinct odd primes we have*

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

The main point of this theorem is that p and q are "entangled" by this extra relation. Most of the time in number theory one can treat primes as uniformly distributed random variables (like in dirichlet's theorem about the equidistribution of the residue classes of primes p mod q). The Law of Quadratic Reciprocity is an exception to this Heuristic and shows that there is is hidden symmetry in the prime numbers.

The proof of the Law of Quadratic Reciprocity is interesting because we need to go beyond viewing $\mathbf{Z}/p$ as an abstract group — the proof uses the ordering of representatives of $\mathbf{Z}/p$. Throughout this proof we will fix representatives

$$\mathbf{Z}/p = \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\},$$

rather than the form $\{0, 1, \ldots, p-1\}$ because in the previous form, we consider the sign of certain numbers.

Lemma 1 (Euler)**.**

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \mod p \tag{3}$$

Proof. Our job is to show

$$n^{(p-1)/2} \mod p \equiv \begin{cases} 1, & n \text{ is a square modulo } p \\ 0, & p|n \\ -1, & \text{otherwise} \end{cases}$$

case 1 Suppose $p|n$. Then $n^{\frac{p-1}{2}} \equiv 0$ is trivial.

case 2 Suppose $n \equiv x^2 \mod p$. Then $n^{\frac{p-1}{2}} = x^{p-1} = 1$ from Fermat's Little Theorem.

case 3 Suppose n is not a square mod p. We need two facts.

1. $(p-1)! \equiv -1 \mod p$ (which holds generally)
2. $(p-1)! \equiv n^{(p-1)/2}$. (which holds when n is not a square)

First, $\mathbf{Z}/p$ is a field. We write out $(p-1)!$ and pairing inverses and get $(p-1)! \equiv \prod_{c \in \mathbf{F}_p^\times} c = -1$, Since the only elements left over at the ones which are there own inverses. But the only elements which are there own inverses are -1 and 1 (The two roots of $x^2 = 1$). [1]

Consider pairs c, d such that $cd = n \mod p$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, for every c there exists a unique d (since n is not a square mod p, there are exactly $(p-1)/2$ pairs $\{c, d\}$ such that $cd = n \mod p$, and that these pairs partition $\mathbf{Z}/p$. [2] This gives $(p-1)! = \prod_{cd=n} c \cdot d = n^{(p-1)/2} \mod p$.

□

Consider the sets $P = \{1, 2, \dots, \frac{p-1}{2}\}$ and $N = \{-1, -2, \dots, -\frac{p-1}{2}\}$ positive and negative representatives of $\mathbf{F}_p^\times$.

Let's let $u_p(n)$ denote the number of elements of P that are sent to negative representatives under multiplication by $n \in \mathbf{F}_p^\times$:

$$u_p(n) = \#(nP \cap N) = \# \text{ number of minus signs changes in } nP \tag{4}$$

We first claim that all the elements P appear in $n \cdot P$ up to sign. To see this note that two images under multiplication by n are equal up-to sign if and only if he quotient of their images under multiplication by n is ± 1 which will give a contradiction—we write this out now: for $x \neq y \in P$ we have

$$nx/ny \equiv \pm 1 \implies x/y \equiv \pm 1 \implies x \equiv \pm y$$

which is impossible.

Lemma 2 (Gauss)**.**

$$\left(\frac{n}{p}\right) = (-1)^{u_p(n)}. \tag{5}$$

Proof.
- Every element in P appears in nP up to sign.

[1] An alternative suggestion by someone in the class was to view $\mathbf{F}_p^\times$ as a cyclic group $\mathbf{F}_p^\times = \langle t \rangle$ so that the product can be written as $\prod_{j=0}^{p-1} t^j = t^{\sum_{j=0}^{p-1} j} = t^{p(p-1)/2} = (t^p)^{(p-1)/2} = t^{(p-1)/2}$. It is clear that $t^{(p-1)/2}$ is a root of the equation $x^2 \equiv 1 \mod p$. It is also clear that $t^{(p-1)/2} \neq 1 \mod p$ since t is the generator and $(p-1)/2$ is smaller than the group. — There should be some natural generalization of this theorem to field extensions of $\mathbf{F}_p$.

[2] If n is a square then there are *exactly two* numbers x such that $x^2 = n$—one positive, one negative.

- $\prod_{x\in nP} x \equiv (-1)^{u_p(n)} \prod_{x\in P} x$ and we also have $\prod_{x\in nP} x = \prod_{x\in P} nx \equiv n^{(p-1)/2} \prod_{x\in P} x$.

□

Lemma 3. *1. $u_p(q) = \#\{(x,y) \in P \times Q : -p/2 < qx - py < 0\}$*

2. $u_p(q)$ is the number of lattice points between the lines $y = (q/p)x$ and $y = (q/p)x + 1/2$.

Proof.

$$\begin{aligned} u_p(q) &= \#qP \cap N \\ &= \#\{x \in P : \exists n \in N, qx \equiv n \mod p\} \end{aligned}$$

$$\begin{aligned} \exists n \in N, qx \equiv n \mod p &\iff \exists y \in \mathbf{Z}, qx - py \in N \\ &\iff \exists y \in \mathbf{Z}, -p/2 < qx - py < 0 \end{aligned}$$

So we have

$$\#\{x \in P : \exists n \in N, qx \equiv n \mod p\} = \#\{x \in P : \exists y \in \mathbf{Z}, -p/2 < qx - py < 0\}$$

If we show that if a $y \in Q$ exists then it is unique (for a fixed x) we are done—but changing $y \to y \pm 1$ changes $qx - py$ by at least p which would violate the bounds (since we only have $p/2$ room to move). □

Since the line $qx - py = 0$ is equivalent to $y = (q/p)x$ the lemma really tells us that $u_p(q)$ is simply the number of lattice points in $P \times Q$ between the lines $y = qx/p$ and $y = qx/p + 1/2$.

We are now in a position to attack the proof of the Law of Quadratic Reciprocity.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{u_p(q)+u_q(p)}$$

by two applications of Gauss' theorem. We show that

$$u_p(q) + u_q(p) \equiv \#P \times Q - \text{ some even crap}$$

which will prove the theorem since $\#P \times Q = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

First note by symmetry we have

$$\begin{aligned} u_q(p) &= \#\{(y,x) \in Q \times P; -q/2 < py - qx < 0\} \\ &= \#\{(x,y) \in P \times Q; 0 \le qx - py < q/2\} \end{aligned}$$

Which tells us

$$\begin{aligned} u_p(q) + u_q(p) &= \#\{(x,y) \in P \times Q; -p/2 < qx - py < 0 \text{ or } 0 < qx - py < q/2\} \\ &= \#\{(x,y) \in P \times Q; -p/2 < qx - py < q/2\}. \end{aligned}$$

On the second line we used the fact that the line $y = (q/p)x$ has no lattice points since q and p are coprime. So we $u_p(q) + u_q(p)$ counts the number of lattice points between two parallel lines of slope q/p with y-intercepts $1/2$ and $-(q/p)/2$ respectively.

- Let $T = \{(x, y) \in P \times Q; -p/2 < qx - py < q/2\}$ be the region bounded by these two lines.
- Let A be the remaining portion of $P \times Q$ above the top line.
- Let B be the remaining portion of $P \times Q$ above the bottom line.

If $\#A = \#B$ we are done since

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{u_p(q)+u_q(p)} = (-1)^{\#T} = (-1)^{\#P\times Q-\#A-\#B} = (-1)^{\#P\times Q}$$

Lemma 4. *If $A = \{(x, y) \in P \times Q; qx - py < -p/2\}$ and $B = \{(x, y) \in P \times Q : qx - py > q/2\}$ then the map $\rho : \mathbf{Z}^2 \to \mathbf{Z}^2$ defined by*

$$\rho(x, y) = (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$$

induces a bijection between the sets A and B with $\rho(A) = B$ and $\rho(B) = A$. In particular we have $\#A = \#B$.

Proof. Suppose that $qx-py < -p/2$ (i.e. $(x, y) \in A$ then we claim that $\rho(x, y) = (x', y')$ is in B;

$$\begin{aligned} qx' - py' &= q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right) \\ &= q/2 - p/2 - (qx - py) \\ &> q/2 - p/2 + p/2 = q/2. \end{aligned}$$

This shows that $\rho(A) \subset B$. It is clear that $\rho \circ \rho$ is the identity. An argument similar to the one above shows that $\rho(x', y')$ is in A by showing $qx''-py'' < -p/2$ (if $\rho(x', y') = (x'', y'')$). This means that $\rho(\rho(x', y')) = (x', y')$ which shows every element of B is in the image of A and we have a bijection. □