THE LAW OF QUADRATIC RECIPROCITY

RONAN O'GORMAN

1. Introduction

Definition 1.1 (Quadratic residue)**.** Let $a, b \in \mathbb{Z}$. We say that a is a quadratic residue modulo b iff a is co-prime to b and there exists some $n \in \mathbb{Z}$ such that $a \equiv n^2 \pmod{b}$.

In this note, we discuss some aspects of the theory of these quadratic residues, and present two proofs of a delightful result known as the Law of Quadratic Reciprocity. This is one of the most-loved (and most-proved) results in mathematics - in 2000 Franz Lemmermeyer counted fully 196 distinct published proofs. The result is most commonly stated as follows:

Theorem 1.2 (Law of Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

where $(\frac{p}{q})$ denotes the Legendre symbol:

Definition 1.3 (Legendre symbol)**.** For any odd prime p, and $a \in \mathbb{Z}$, define

$$(\frac{a}{p}) = \begin{cases} 0 & a \equiv 0 \pmod{p} \\ 1 & (a,p) = 1,\ a \equiv n^2 \pmod{p} \text{ for some } n \in \mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$

This law was conjectured by Euler and (as the notation may suggest) Legendre, but the first complete proof is attributed to Gauss in 1801. He alone produced eight different proofs, and Ferdinand Eisenstein followed up soon after with another five (one of which is presented here). The list of proofs has been growing ever since, and generalizing the statement remains a central problem in modern number theory which has led to the development of vast swathes of new mathematics.

Here, we follow Flynn-Conolly's presentation of one of Eisenstein's more elegant proofs, and outline an additional proof from [1, Ch. 5]. The latter is based on Gauss's sixth proof and makes use of concepts which are central to the further development of the theory.

2. Euler's criterion

We first establish some basic facts about quadratic residues, including a neat test for quadratic reciprocity. In what follows, let p be an odd prime, $\mathbb{Z}_p$ denote the field of integers modulo p, and $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ the corresponding multiplicative group.

Date: October 17, 2018.

Lemma 2.1. *The quadratic residues modulo p are precisely*

$$\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}.$$

Proof. There can certainly be no quadratic residues other than these, since for any $a \in \mathbb{Z}$, $a^2 \equiv (p-a)^2 \pmod p$. To see that all of them are different, observe that for any $i, j \in \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$,

$$\begin{aligned} i^2 \equiv j^2 \pmod p &\implies p \mid i^2 - j^2 \\ &\implies p \mid (i+j)(i-j) \end{aligned}$$

so $i \neq j$ implies $p \mid (i+j)$, which is impossible since both are less than $\frac{p-1}{2}$. □

Next, recall the following result from elementary group theory:

Lemma 2.2 (Fermat's little theorem)**.** *For any prime p, and any $a \in \mathbb{Z}$ coprime to p,*

$$a^{p-1} \equiv 1 \pmod p.$$

Proof. Observe that since $\mathbb{Z}_p^*$ is a group under multiplication, the map

$$x \to ax$$

is bijective on this group, so it acts as a permutation of the elements $1, \cdots, p-1$ modulo p. Hence

$$(a)(2a)(3a)\cdots((p-1)a) \equiv (1)(2)\cdots(p-1) \pmod p)$$

and we can divide both sides by $(p-1)!$ to get the result.

Alternatively, this can be deduced immediately from Lagrange's theorem applied to the multiplicative group $\mathbb{Z}_p^*$. □

From this lemma, we see that every $a \in \mathbb{Z}_p^*$ is a root of the polynomial $x^{p-1} - 1$. If p is an odd prime, we can factorize this polynomial to get $(x^{\frac{p-1}{2}} + 1)(x^{\frac{p-1}{2}} - 1)$. Since Z_p is a field (and more specifically in this case an integral domain), each of these polynomials can have at most $\frac{p-1}{2}$ roots, so every element $a \in \mathbb{Z}_p^*$ is a root of exactly one of them.

Suppose a is a quadratic residue modulo some prime p (say $a \equiv n^2 \pmod p$). Then $a^{\frac{p-1}{2}} = n^{p-1} = 1$ by Fermat's little theorem. Therefore every quadratic residue is a root of $x^{\frac{p-1}{2}} - 1$. By lemma 2.1, there are $\frac{p-1}{2}$ quadratic residues, so we see that the quadratic residues modulo p are precicely the roots of $x^{\frac{p-1}{2}} - 1$, and the quadratic nonresidues modulo p are the roots of $x^{\frac{p-1}{2}} + 1$. Comparing this to the definition of the Legendre symbol, we immediately get the following:

Theorem 2.3 (Euler's Criterion)**.** *For any odd prime p, and any $a \in \mathbb{Z}$,*

$$(\frac{a}{p}) = a^{\frac{p-1}{2}}.$$

From this it easily follows that the Legendre symbol is multiplicative; i.e. for any $a, b \in \mathbb{Z}$ and odd prime p, we have

$$(\frac{a}{p})(\frac{b}{p}) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} = (\frac{ab}{p}).$$

3. The Lemma of Gauss

Euler's criterion and its immediate corollary give a simple way to test whether an integer is a quadratic residue modulo some prime p - namely, by first writing the number as a product of primes and -1, and then computing the Legendre symbol for each of the factors. In order to characterize quadratic residues more generally, then, it is enough to understand $(\frac{-1}{p}), (\frac{2}{p})$ and $(\frac{q}{p})$ for odd primes q, p (the case $p = 2$ will be left as an exercise for the enthusiastic reader).

The first of these is easy. Since $\frac{p-1}{2}$ is even if and only if $p \equiv 1 \pmod 4$, then we have by Euler's criterion that

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv -1 \pmod 4. \end{cases}$$

To deal with the other two, we will need some more machinery:

Lemma 3.1 (Lemma of Gauss)**.** *Let p be an odd prime and a be co-prime to p. Consider the set $\left\{a, 2a, \cdots, \frac{p-1}{2}a\right\}$ reduced modulo p to the residue system of smallest absolute value, i.e. $ia \equiv r_i$ with $-\frac{p-1}{2} \leq r_i \leq \frac{p-1}{2}$ for each $i = 1, \cdots, \frac{p-1}{2}$.*

Let S denote the set $\{r_i \colon r_i < 0\}$, and $s = \#S$. Then

$$(\frac{a}{p}) = (-1)^s.$$

Proof. First, re-label the r_i so that $u_1, \cdots, u_s$ are in S and $v_{s+1}, \cdots, v_{\frac{p-1}{2}}$ are not in S. The key here is to realize that $\{-u_1, \cdots, -u_s, v_{s+1}, \cdots v_{\frac{p-1}{2}}\} = \{1, 2, \cdots, \frac{p-1}{2}\}$.

To see this, first observe that, as in 2.1, the map $x \to ax$ is a bijection on the group $\mathbb{Z}_p^*$, so the elements $r_i, i = 1, \cdots, \frac{p-1}{2}$ are all distinct. Then, if $u_i = ka$ and $v_j = la$, then $-u_i \equiv v_j \pmod p$ for any i, j implies $p \mid u_i + v_i$, so $p \mid (k+l)a$. Since a and p are co-prime, this implies $p \mid k + l$ which is impossible since both are less than or equal to $\frac{p-1}{2}$.

Once we have this, the rest follows easily, since

$$\begin{aligned} \frac{p-1}{2}! &\equiv (-1)^s \prod_{i=1}^{s} u_i \prod_{j=s+1}^{\frac{p-1}{2}} v_j && \pmod p \\ &\equiv (-1)^s \prod_{i=1}^{\frac{p-1}{2}} ia && \pmod p \\ &\equiv (-1)^s a^{\frac{p-1}{2}} \frac{p-1}{2}! && \pmod p \end{aligned}$$

(applying Euler's criterion)

$$\equiv (-1)^s (\frac{a}{p}) \frac{p-1}{2}! \qquad \pmod p$$

and we can divide across by $(-1)^s \frac{p-1}{2}!$ to get the result. □

This result is important in its own right - it is the main ingredient in many proofs of the reciprocity law (including the first one presented here). More immediately for us, however, it makes short work of the term $(\frac{2}{p})$. Setting $a = 2$ in the lemma, we can easily see that

$$s = \#\left\{i\colon \frac{p-1}{2} < 2i \leq p-1\right\} = \#\left\{i\colon \frac{p-1}{4} < i \leq \frac{p-1}{2}\right\} = \left\lceil \frac{p-1}{4} \right\rceil.$$

Observe that

$$p = 8x+n \implies \frac{p-1}{4} = 2a + \frac{n-1}{2}$$

so $\lceil \frac{p-1}{4} \rceil$ is even iff $p = \pm 1 \pmod 8$, and we get

$$(\frac{2}{p}) = \begin{cases} 1 & p = \pm 1 \pmod 8 \\ -1 & p = \pm 3 \pmod 8. \end{cases}$$

4. First proof

We can now finally present our first proof of the reciprocity law. This proof is based on Gauss's third, though the precise formulation is due to Ferdinand Eisenstein, and is a very clever application of the Lemma of Gauss. We restate the theorem for reference:

Theorem (Law of Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

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

Proof. The idea is to use of the Lemma of Gauss to reduce the problem to counting points in a lattice.

Consider the set $\left\{a, 2a, \cdots, \frac{p-1}{2}a\right\}$ reduced modulo p to the residue system of smallest absolute value, as in the Lemma of Gauss. If iq reduces to r_i in this system, then there is a unique integer j such that $iq - jp = r_i$. Necessarily, $0 < j < \frac{q}{2}$. In other words, for any $i \in \mathbb{N}$, there exists some j, $0 < j < \frac{q}{2}$ with $\frac{-p}{2} < iq - jp < 0$ iff iq reduces to $r_i < 0$, and such a j is always unique. Hence, by the Lemma of Gauss, $(\frac{q}{p}) = (-1)^s$, where s is the number of points (i,j) satisfying

$$0 < pj - qi < \frac{p}{2}, \text{ with } 0 < i < \frac{q}{2},\ 0 < j < \frac{p}{2}.$$

Similarly, $(\frac{p}{q}) = (-1)^t$, where t is the number of points (i,j) satisfying

$$0 < qi - pj < \frac{q}{2}, \text{ with } 0 < i < \frac{q}{2},\ 0 < j < \frac{p}{2}.$$

We represent the points $\{(i,j) \in \mathbb{Z} \times \mathbb{Z}\colon 0 < i < \frac{q}{2},\ 0 < j < \frac{p}{2}\}$ in a lattice L, and superimpose the parallel lines $qi - pj = \frac{q}{2}$, $qi - pj = 0$, $qi - pj = -\frac{p}{2}$ on this lattice. Then s is the number of lattice points between the upper and middle diagonals, and t the number of points between the middle and lower diagonals (see figure 1), so the number of points between the upper and lower diagonals is $s + t$.

Label the outer regions above and below the diagonals B and R (colored blue and red in the figure), and let $|B|$ and $|R|$ respectively denote the number of lattice points they contain. We now make two observations about this lattice:

(1) There are no lattice points on any of the diagonal lines.

There are no points on the center diagonal since if $qi = pj$ then $i = \frac{pj}{q}$ which can't be an integer since both p and j are co-prime to q. Also, if i and j are integers then $qi - pj$ is also an integer, but $\frac{p}{2}$ and $\frac{q}{2}$ are not integers, so can be no points on the upper or lower diagonals.

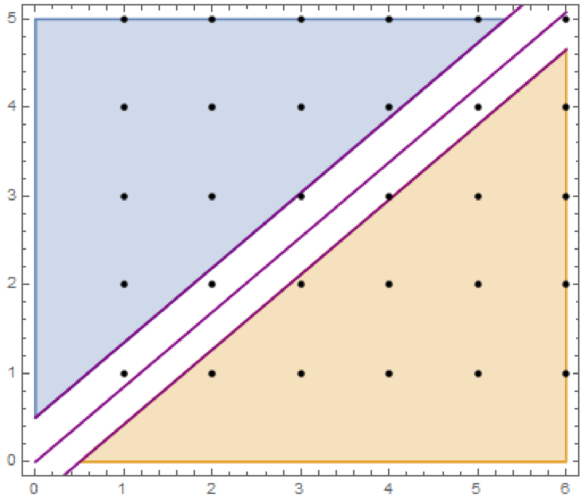

FIGURE 1. Example with $p = 11, q = 13$.

(2) $|B| + |R|$ is even.

To see this, let $\phi : L \to L;\ (x, y) \mapsto \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$. One can easily verify that ϕ is an involution which maps R to B and B to R, so we conclude that R and B contain the same number of elements.

Then, since the total number of points in the lattice is $\frac{p-1}{2}\frac{q-1}{2} = s+t+|B|+|R|$, we see that $\frac{p-1}{2}\frac{q-1}{2}$ and $s + t$ have the same parity. Hence

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{s+t} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

5. SECOND PROOF

We now briefly outline an alternative proof of the result, which is based on Gauss's sixth. This proof deduces the result from the properties of so-called "Gauss Sums" in finite fields. Gauss Sums are very important tools used throughout number theory, and the proof here can be taken as a starting point for results much more general than the reciprocity law.

We will need some facts about finite fields, which we recall here without proof. In what follows, let p and q be distinct odd primes and $\mathbb{F} = \mathbb{F}_{q^{p-1}}$ denote the field with q^{p-1} elements. For any $a \in \mathbb{F}, n \in \mathbb{Z}$, define

$$n \cdot q = \underbrace{a + \cdots + a}_{\text{n times}}.$$

(1) $\mathbb{F}$ has characteristic q - i.e., for any $a \in \mathbb{F}$, $q \cdot a = 0$.

In particular, for for any $b, c \in \mathbb{F}$,

$$(c + b)^q = \sum_{i=0}^{q} \binom{q}{i} \cdot b^i b^{c-i} = b^q + c^q$$

since all binomial co-efficients $\binom{q}{i}$ with $i \notin \{0, q\}$ are multiples of q.

(2) The multiplicative group $\mathbb{F}^*$ of $\mathbb{F}$ is cyclic of order $q^{p-1}-1$.
We know that p divides $q^{p-1}-1$ by Fermat's Little theorem, so using this we can find an element $\zeta \in \mathbb{F}^*$ of order p.

We can now proceed with the proof:

Proof. Let $\mathbb{F}, p, q, \zeta$ be as above. Consider the "Gauss Sum"

$$G := \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^i.$$

The result will be a simple corollary of the following lemma:

Lemma 5.1.

$$G^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. By multiplicity of the Legendre symbol, we have

$$G^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} (\frac{ij}{p}) \zeta^{i+j}$$

Set $k = j(i)^{-1} \pmod{p}$. Then, for fixed i, j and k run over the same indices, and hence

$$\begin{aligned} G^2 &= \sum_{k=1}^{p-1} \sum_{i=1}^{p-1} (\frac{k}{p}) \zeta^{i(1+k)} \\ &= \sum_{k=1}^{p-1} (\frac{k}{p}) \sum_{i=1}^{p-1} \zeta^{i(1+k)} \\ &= (\frac{-1}{p})(p-1) + \sum_{k=1}^{p-2} (\frac{k}{p}) \sum_{i=1}^{p-1} \zeta^{i(1+k)} \end{aligned}$$

(bringing out the terms where $k = -1 \pmod{p}$).

We now use the fact that for any p^{th} root of unity $\eta \neq 1$, $\sum_{i=1}^{p-1} \eta^i = -1$. Since for any $k \not\equiv -1 \pmod{p}$, $\zeta^{1+k} \neq 1$ and is also a p^{th} root, the inner summand in the above expression becomes -1 and we get

$$G^2 = (\frac{-1}{p})(p-1) - \sum_{k=1}^{p-2} (\frac{k}{p}).$$

Finally, since the number of quadratic residues and quadratic non-residues modulo p is equal, we know that

$$\sum_{k=1}^{p-1} (\frac{k}{p}) = 0$$

and hence

$$\sum_{k=1}^{p-2} (\frac{k}{p}) = -(\frac{-1}{p})$$

so substituting this into the formula for G^2 we get

$$G^2 = (\frac{-1}{p}) p = (-1)^{\frac{p-1}{2}} p$$

by Euler's Criterion. □

By the lemma, we have

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

However, we also have

$$\begin{aligned} G^q &= \sum_{i=1}^{p-1} (\frac{i}{p})^q \zeta^{iq} && \text{(by property 1 above)} \\ &= \sum_{i=1}^{p-1} (\frac{i}{p}) \zeta^{iq} && \text{(since q is odd)} \\ &= \sum_{i=1}^{p-1} (\frac{i}{p})(\frac{q^2}{p}) \zeta^{iq}. \end{aligned}$$

By multiplicity of the Legendre symbol, we can re-write this to get

$$G^2 = (\frac{q}{p}) \sum_{i=1}^{p-1} (\frac{iq}{p}) \zeta^{iq}.$$

All that remains is to see that i and iq run over the same indices, and then, recalling the definition of G, we get

$$G^2 = (\frac{q}{p}) G. \tag{2}$$

The result follows on dividing equations (1) and (2) by G, which we know is non-zero by the above lemma. □

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from The Book*. Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann.