GROUP THEORY PROOF OF THE LAW OF QUADRATIC RECIPROCITY

YUENAN HUANG

Abstract. We present a proof of the celebrated quadratic reciprocity law given by George Rousseau in 1991. The proof is based on group theory and does not rely on Gauss's Lemma.

1. Introduction

The law of quadratic reciprocity is a fundamental result in number theory. It provides a way to determine whether the congruence equation $x^2 = a \pmod{p}$ is solvable, though it does not give a way of finding the specific solution. Like the Pythagorean theorem, the law of quadratic reciprocity has lent itself to an unusually large number of proofs. Carl Friedrich Gauss, who was often regarded as one of the greatest mathematicians of all time, gave the first complete proof in 1801 and followed up with seven more. In this paper we present a proof given by George Rousseau in 1991, which relies on nothing more than simple group theory, Wilson's theorem, and the Chinese remainder theorem.

2. Background on Quadratic Reciprocity

Definition 2.1. If p is an odd prime, and $\gcd(a, p) = 1$, then a is a *quadratic residue mod* p if the congruence equation $x^2 \equiv a \pmod{p}$ is solvable. If this is not solvable, then we call a is a *quadratic non-residue mod* p.

Theorem 2.2 (Euler's Criterion)**.** *If p is an odd prime and $\gcd(a, p) = 1$, then*

$$a^{\frac{p-1}{2}} = \begin{cases} 1 \pmod{p}, & \text{if and only if } a \text{ is a quadratic residue mod } p; \\ -1 \pmod{p}, & \text{if and only if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Proof. By Fermat's Little Theorem, we have $a^{p-1} = (a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$, and hence

$$0 \equiv (a^{\frac{p-1}{2}})^2 - 1 = (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \pmod{p}.$$

By Euclidean's lemma, we have either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence it suffices to prove only one of the cases. Suppose that a is a quadratic residue, then there exists an x_0 such that $x_0^2 \equiv a \pmod{p}$. Since $p \nmid a$, we have $p \nmid x_0$. It follows that

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem.
Conversely, suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Let g be a primitive root mod p. Then $a = g^k$ for some k such that $1 \leq k \leq p - 1$. We have

$$a^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^k \equiv (g^{\frac{k}{2}})^{p-1} \equiv 1 \pmod{p}.$$

Date: March 8, 2022.

Since $\text{ord}_p(g) = p-1$, we have $p-1|\frac{k(p-1)}{2}$. Therefore, $k = 2l$ for some $l \in \mathbb{Z}$. It then follows that

$$g^k = (g^l)^2 \equiv a \pmod{p}.$$

Therefore, g^l is a solution to $x^2 a \pmod{p}$ and a is a quadratic residue. ■

To help express the law of quadratic reciprocity, we will introduce the Legendre symbol, which named after the French mathematician Adrien-Marie Legendre in the course of his attempts to prove the theorem.

Definition 2.3. Let a be an integer and p be an odd prime number. The *Legendre symbol* is a function of a and p defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Euler's criterion can be concisely reformulated using the Legendre symbol as

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Now we can state the law of quadratic reciprocity.

Theorem 2.4 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes, then*

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

3. Proof of the Law of Quadratic Reciprocity

We will first prove two results that are needed for the proof of the law of quadratic reciprocity.

Theorem 3.1 (Wilson)**.** *Let p be a prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Note that the theorem holds when $p = 2$ and 3. Now suppose $p \geq 5$. Notice that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a field for prime p. Thus each $a \in (\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \cdots, p-1\}$ has an unique inverse $a^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$. If $a = a^{-1}$, then we must have $1 \equiv aa^{-1} = a^2 \pmod{p}$, which necessitates $a \equiv \pm 1 \pmod{p}$ and thus $a = 1$ or $p-1$. In the product $(p-1)! = 1 \times 2 \times \cdots \times (p-2)(p-1)$, we pair off each term, except 1 and $p-1$, with its inverse modulo p. We thus get $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. ■

Lemma 3.2. *Let p be a prime, then*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \pmod{p}.$$

Proof. Notice that for any $x \in \mathbb{Z}$ where $1 \leq x \leq \frac{p-1}{2}$, we have $p - x \equiv x \pmod{p}$. It follows that

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\ &\equiv \left(\frac{p-1}{2}\right)!\left((-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!\right) = (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.\end{aligned}$$

Multiply $(-1)^{\frac{p-1}{2}}$ on both sides, we get

$$(-1)^{\frac{p-1}{2}}(p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p},$$

as desired. ■

Now we will provide a proof of the quadratic reciprocity.

Proof. Let p and q be distinct odd primes. By Chinese Remainder Theorem, we have

$$G = (\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times,$$

or equivalently, $G = \{(a,b)\}$ where $a \in \{1,2,\cdots,p-1\}$ and $b \in \{1,2,\cdots,q-1\}$. We will determine the product π of the elements of the group $M = G/H$, where $H = \{(1,1),(-1,-1)\}$ is a subgroup of G.
Note that $\{(a,b) : a = 1,2,\cdots,p-1; b = 1,2,\cdots,(q-1)/2\}$ is a system of representatives for the cosets of H. We will use two approaches to find the produce of the (a,b). ■

(1) The list of representatives of G/H is

$$\{(a,b) : 1 \le a \le p-1, 1 \le b \le (q-1)/2\}.$$

Since each a component is repeated $\frac{q-1}{2}$ times, the a-component of pi is

$$(p-1)!^{\frac{p-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \pmod{p}.$$

Similarly, each b-component is repeated $p-1$ times, so the b component of π is

$$\begin{aligned}\left(\left(\frac{q-1}{2}\right)!\right)^{p-1} &= \left(\left(\frac{q-1}{2}\right)!^2\right)^{\frac{p-1}{2}} \\ &\equiv \left((-1)^{\frac{q-1}{2}}(q-1)!\right)^{\frac{p-1}{2}} \pmod{q} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (q-1)!^{\frac{p-1}{2}} \\ &\equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \pmod{q}.\end{aligned}$$

Hence the product of the representatives is

$$\pi = \left((-1)^{\frac{q-1}{2}} \pmod{p},\ (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod{q}\right) H. \tag{3.1}$$

(2) We will choose the representatives on $(\mathbb{Z}/pq\mathbb{Z})^\times = \{1,2,\cdots,pq-1\}$, by taking the first half of $(\mathbb{Z}/pq\mathbb{Z})^\times$. To find π, we shall multiply all the integers between 1 and $\frac{pq-1}{2}$ that are not divisible by p or q.
Let A be the set of integers in $\{1,2,\cdots,\frac{pq-1}{2}\}$ that are not divisible by p. Then we have

$$\begin{aligned}A = &\{1,2,\cdots,p-1\} \cup \{p+1,p+2,\cdots,2p-1\} \cup \{2p+1,2p+2,\cdots,3p-1\} \\ &\cup \cdots \cup \{\frac{q-1}{2}\cdot p+1, \frac{q-1}{2}\cdot p+2,\cdots,\frac{pq-1}{2}\},\end{aligned}$$

and

$$B = \{q, 2q, \cdots, \frac{p-1}{2}q\}$$

is the set of all integers in A that are divisible by B.
Thus the a-component of π is

$$\begin{aligned}\prod_{(m\in A)\cap(m\notin B)} m &= \frac{\prod_{m\in A} m}{\prod_{m\in B} m}\\ &\equiv \frac{(p-1)!^{(q-1)/2}\cdot\left(\frac{p-1}{2}\right)!}{q\cdot(2q)\cdots\left(\frac{p-1}{2}\right)q} \pmod p\\ &= \frac{(p-1)!^{(q-1)/2}\cdot\left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{2}\right)!\cdot q^{(p-1)/2}}\\ &= \frac{(p-1)^{(q-1)/2}}{q^{(p-1)/2}}\\ &\equiv \frac{(-1)^{(q-1)/2}}{q^{(p-1)/2}} \pmod p\\ &\equiv \frac{(-1)^{(q-1)/2}}{\left(\frac{q}{p}\right)} \pmod p\\ &= (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p.\end{aligned}$$

For modulo q, through similar calculation we find that the b-component of π is equivalent to

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

Hence the product of representatives is

$$\pi = \left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p,\ (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q\right) H. \tag{3.2}$$

Compare two expressions of π ((3.1) and (3.2)) gives

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

and hence the reciprocity law,

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

References

[1] G. Rousseau. On the quadratic reciprocity law. *J. Austral. Math. Soc. Ser. A*, 51(3):423-425, 1991.

Email address: yuenanhuang265@gmail.com