Quadratic Reciprocity

Jocelyn Wang, Stephanie Yao

Contents

1. Introduction

The law of quadratic reciprocity is a remarkably important theorem in number theory about modular arithmetic that provides conditions for the solvability of quadratic equations modulo prime numbers. Specifically, it provides criterion for determining whether a quadratic equation of the form $x^2 \equiv a \pmod{p}$ has a solution x for given integers a and p even without computing the exact value of x.

Quadratic reciprocity was conjectured by Leonhard Euler and Adrien-Marie Legendre. Having a total of more than 240 proofs provided in published papers, the quadratic reciprocity law can be viewed as one of the most complex laws in fundamental number theory. Carl Friedrich Gauss conjectured in 1795 that the theorem was correct, and later on, provided a complete proof in 1801. In total, he provided 8 rigorous proofs of quadratic reciprocity.

In this paper, we present a proof inspired by Set $\#25^+$, Podasip 2, which is based on half-systems and Wilson's Theorem, initially sketched by Rousseau. The recent proof by applying the isomorphism of rings given out in 1991 is quite simple compared to the intuitive proof by Gauss.

First, we introduce the definition of Legendre symbol, which is the most widely-used symbol to present the statement of Law of Quadratic Reciprocity.

Definition 1.1 (Legendre Symbol)**.** *For an odd prime p and some $a \in \mathbb{Z}$, we define the Legendre Symbol as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue in } \mathbb{U}_p \\ -1, & \text{if } a \text{ is not a quadratic residue in } \mathbb{U}_p \\ 0, & \text{if } p \mid a \end{cases}$$

Then, using this definition, we state the Law of Quadratic Reciprocity as the following:

Theorem 1.2 (Law of Quadratic Reciprocity)**.** *If p and q are distinct odd prime numbers, then*

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

This theorem is important for the powerful and efficient criterion for determining whether a given integer a is a quadratic residue modulo a prime p. Beyond its practical utility, quadratic reciprocity embodies the intrinsic beauty of mathematics, illustrating how simple yet surprising relationships can emerge from the fundamental properties of numbers, demonstrating the harmony underlying the structure of the integers.

2. Motivation

Imagine being a number theorist centuries ago: you are interested in finding all the squares mod p for all elements in $\mathbb{Z}_p$. For example, when $p = 3, 5, 7$, you list the following table:

x	$p = 5$ $x^2 \pmod 5$	$p = 7$ $x^2 \pmod 7$	$p = 11$ $x^2 \pmod{11}$
1	1	1	1
2	4	4	4
3	4	2	9
4	1	2	5
5	0	4	3
6	1	1	3
7	4	0	5
8	4	1	9
9	1	4	4
10	0	2	1
⋮	⋮	⋮	⋮

Then, observe the results of the table. For example, look at 5 and 7. When we have $p = 5$, $7 \equiv 2 \pmod 5$ does not exist in $x^2 \equiv 0, 1, 4 \pmod 5$. Similarly, when we have $p = 7$, twe ry to look for 5 in the $x^2 \pmod 7$ entry: 5 does not show up in the entries either.

Next, try to find 5 in the $x^2 \pmod{11}$ entries and 11 in the $x^2 \pmod 5$ entries: we know that $4^2 \equiv 5 \pmod{11}$, and $1^2, 4^2, 6^2, 9^2, \ldots \equiv 1 \equiv 11 \pmod 5$.

Note that for the cases where we can find neither or both of $x^2 \equiv p \pmod q$ and $y^2 \equiv q \pmod p$,

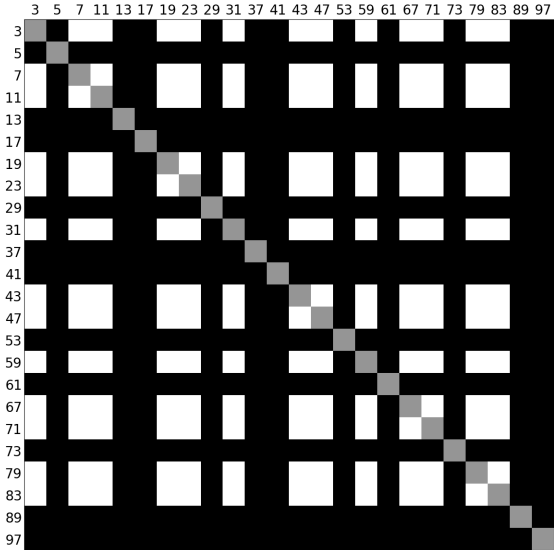
where $p = 5$, $q = 11$ and $p = 5$, $q = 7$, we have $\frac{5-1}{2}\frac{11-1}{2} = 10$, $\frac{5-1}{2}\frac{7-1}{2} = 6$. Both results of $\frac{p-1}{2}\frac{q-1}{2}$ are divisible by 2.

What about the cases with $2 \nmid \frac{p-1}{2}\frac{q-1}{2}$?

For example, if we have $p = 7$, $q = 11$, then we can find $11 \equiv 4 \equiv 2^2, 5^2, 9^2, \ldots \pmod 7$. However, we cannot find such x satisfying $x^2 \pmod{11} \equiv 7$.

This question also arose in number theorists' minds. They drew a table with both p and q as odd primes. If they could find $x \in \mathbb{Z}_q$ such that $x^2 \equiv p \pmod q$, they colored the entry (p, q) black, and if such x did not exist, the entry was uncolored (and if $p = q$, the grid is colored grey). The table drawn is shown below:

This seems to be a little bit messed up. What if we colored all the grids (p, q) when both or neither of x, y such that $x^2 \equiv p \pmod q, y^2 \equiv q \pmod p$ exist, and the uncolored grids are automatically the condition when only one of x, y exists? Here is the resulting table:



If we calculate $\frac{p-1}{2}\frac{q-1}{2}$ for any of the (p,q) grids that are colored black, we have $2 \mid \frac{p-1}{2}\frac{q-1}{2}$. In contrast, any of the (p,q) grids that are uncolored have $2 \nmid \frac{p-1}{2}\frac{q-1}{2}$. Referring to the definition of the Legendre Symbol, we know that it implies that when $2 \mid \frac{p-1}{2}\frac{q-1}{2}$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, and when $2 \nmid \frac{p-1}{2}\frac{q-1}{2}$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, which is equivalent to the law of quadratic reciprocity:

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

In the rest of the paper, we will present a rigorous proof of Theorem 1.2 (Quadratic Reciprocity).

3. Legendre Symbol

In this section, we try to map the Legendre symbol to a quantified value with meaning, instead of using the plain definition as stated in Definition 1.1. Then, we prove a few properties of the Legendre symbol, which are useful to our proof of quadratic reciprocity.

We will start by proving a theorem crucial to the Legendre symbol: Fermat's little Theorem (FℓT).

Theorem 3.1 (Fermat's little Theorem (FℓT))**.** *If p is prime, $a^{p-1} \equiv 1 \pmod{p}$ for $a \in \mathbb{Z}$ such that $p \nmid a$.*

Proof. We begin by taking the set $\mathbb{U}_p = \{1, 2, \ldots, p-1\}$. Then, we multiply every element in $\mathbb{U}_p$ by some constant a where $\gcd(a,p) = 1$ so that we have the new set $\{a, 2a, \ldots, (p-1)a\}$. Call this set S. Now, we will show that $S = \mathbb{U}_p$.

Note that each element in S equals some element in $\mathbb{U}_p$. Thus, we just have to show that no elements in S repeat. Now, for the sake of contradiction, assume that some $ai = aj$ where $i \neq j$. Then, $ai \equiv aj \pmod{p}$, and $\gcd(a,p) = 1$ implies that $i \equiv j \pmod{p}$. This means that $i = j$, and we have a contradiction. Thus, all elements in S must be distinct, and $\mathbb{U}_p = S$. Multiplying together all elements in both sets and equation gives:

$$a^{p-1} \cdot (p-1)! = (p-1)!$$

Cancelling out $(p-1)!$ on both sides gives $a^{p-1} \equiv 1 \pmod{p}$. □

Lemma 3.2 (Euler's Criterion)**.** *If p is prime and $a \in \mathbb{U}_p$, then $a^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if a is a quadratic residue.*

Proof. First we prove that $a^{(p-1)/2}$ must be 1 or -1 in mod p.

Suppose $x = a^{(p-1)/2}$,

$$\begin{aligned} x^2 &= (a^{\frac{p-1}{2}})^2 \\ &= a^{p-1} \end{aligned}$$

Since p is a prime number and $\varphi(p) = p - 1$, then

$$\begin{aligned} x^2 &= a^{p-1} \\ &\equiv 1 \pmod{p} \\ x^2 - 1 &\equiv 0 \pmod{p} \\ (x+1)(x-1) &\equiv 0 \pmod{p} \end{aligned}$$

Therefore, the solutions to x should be 1 or -1, which implies $a^{(p-1)/2} = \pm 1$.

Now, assume for the sake of contradiction, there exists $x \in \mathbb{U}_p$ such that $a \equiv x^2 \pmod{p}$ when $a^{(p-1)/2} = -1$, we have $(x^2)^{(p-1)/2} = a^{2\cdot(p-1)/2} = a^{p-1} = -1$, which contradicts Euler's Totient Function. Since there does not exist $a \equiv x^2 \pmod{p}$ when $a^{(p-1)/2} = -1$, we have proven that $a^{(p-1)/2} = 1$ implies that a is a square modulo p.

Next, we prove the opposite direction – when a is a square modulo p, $a^{(p-1)/2} = 1$. Since a is a square modulo p, $x^2 \equiv a \pmod{p}, x \in \mathbb{U}_p$. Therefore, $a^{(p-1)/2} = (x^2)^{(p-1)/2} = x^{p-1}$. According to Theorem 3.1 (FℓT), for $x \in \mathbb{U}_p$, $x^{p-1} \equiv 1 \pmod{p}$. Therefore, $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Thus, we have proved that $a^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if a is a quadratic residue. □

Euler's Criterion implies that $\left(\frac{a}{p}\right)$ is equivalent to $a^{(p-1)/2} \pmod{p}$.

Given the true quantitative meaning of $\left(\frac{a}{p}\right)$, we can prove its multiplicativity:

Lemma 3.3. *For all $a, b \in \mathbb{U}_p$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. According to the transferred definition of the Legendre symbol proved in Euler's Criterion,

$$\begin{aligned} \left(\frac{ab}{p}\right) &= (ab)^{(p-1)/2} \\ &= a^{(p-1)/2} \cdot b^{(p-1)/2} \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \end{aligned}$$

□

Lemma 3.4. *If $a \geq p$, $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$, such that $r \equiv a \pmod{p}$, and $r < p$.*

Proof. Based on Lemma 3.2, we have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Now, since $a \geq p$, we can say that $a \equiv r \pmod{p}$ for some $r < p$. Furthermore, since we know that $ab \pmod{m} = (a \pmod{m}) \cdot (b \pmod{m}) \pmod{m}$ for all $a, b, m \in \mathbb{Z}$, we can say that:

$$a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \pmod{p}$$

Thus, for any $a \geq p$, $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$ for $r < p$. □

4. Proof of Quadratic Reciprocity

This proof, as mentioned in the introduction, was yielded by Rousseau in the late 20th century, with a better application in modern mathematics. In this proof of quadratic reciprocity law, we introduce a new definition – *half-system*.

4.1. Introducing Half-Systems

We focus on introducing what a half-system H of R and the product of half-system $\mathbf{P}(H)$ are, which are the only two concepts we need to prove quadratic reciprocity by this method:

Definition 4.1 (Half-System)**.** *If R is a ring with finitely many elements, a subset H of the units of R is called a half-system if for all units $u \in R$, exactly one of u or $-u$ belongs to H.*

Definition 4.2 ($\mathbf{P}(H)$)**.** *Given a half-system H, we let $\mathbf{P}(H)$ denote the product of all elements of H.*

Here we also provide the proof of a lemma that declares the relationship between different half-systems, H and H', of the same set R. This is crucial to the proof of quadratic reciprocity we are constructing.

Lemma 4.3. *If H and H' are two half-systems for the same ring R, then $\mathbf{P}(H) = \pm\mathbf{P}(H')$.*

Proof. We will begin by taking all units u in R and constructing a possible half-system H. For each u, either $u \in H$ or $-u \in H$, so taking the product gives $|\mathbf{P}(H)| = |\mathbf{P}(H')|$ for any half-systems H and H'. From this, $\mathbf{P}(H) = \pm\mathbf{P}(H')$ directly follows.

□

4.2. Constructing Half-Systems

In this section, we enter the main purpose of the exposition of proving the quadratic reciprocity, by constructing the half-systems that are useful to our proof:

Let $R = \mathbb{Z}_p \times \mathbb{Z}_q$ where p, q are distinct odd primes. Construct the following subset of R:

$$H = \left\{(a, b) : 1 \le a \le \frac{p-1}{2}, 1 \le b \le q-1\right\},$$
$$H' = \left\{(a, a) : 1 \le a \le \frac{pq-1}{2}, \gcd(a, pq) = 1\right\}.$$

Note that R is a ring under component-wise addition and multiplication, that is, for $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$, we have

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{4.1}$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) \tag{4.2}$$

Lemma 4.4. *There is an isomorphism from the ring $\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$.*

Proof. To prove an isomorphism, we want to show that there is a map $\phi : \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$ that is both a homomorphism and bijection. Now, we will define ϕ as follows. For some $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$, $\phi((a, b)) \to c$ for $c \in \mathbb{Z}_{pq}$ is the c that satisfies both:

$$c \equiv a \pmod{p}$$
$$c \equiv b \pmod{q}$$

Now, we will prove that ϕ is both a homomorphism and a bijection. Note that the homomorphism is already proven above in Equation 4.1 and Equation 4.2. Thus, we just need to prove a bijection.

To show a bijection, we must prove both injectivity and surjectivity. We will start by proving surjectivity: namely, that every $c \in \mathbb{Z}_{pq}$ has a corresponding $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$. We can show this by noting that since $\gcd(p, q) = 1$, by the Chinese Remainder Theorem , every element $c \in \mathbb{Z}_{pq}$ can be taken separately mod p and mod q, so that $c \equiv a_1 \pmod{p}$ and $c \equiv b_1 \pmod{q}$ for some $a_1 \in \mathbb{Z}_p, b_1 \in \mathbb{Z}_q$, and ϕ is surjective.

Next, we will show injectivity. We need to show that for some some $c_1 = c_2$, the corresponding $(a_1, b_1) = (a_2, b_2)$, respectively. For the sake of contradiction, assume that $c_1 = c_2$, but $(a_1, b_1) \neq (a_2, b_2)$. Then, taking c_1 and c_2 mod p and mod q separately, we get that:

$$c_1 \equiv c_2 \equiv a \pmod{p}$$
$$c_1 \equiv c_2 \equiv b \pmod{q}$$

for some $a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$. However, this means that

$$(a_1, b_1) = (a_2, b_2) = (a, b)$$

and this is a contradiction. Thus, ϕ must also be injective, and ϕ is a bijection. We have now shown that ϕ is both a homomorphism and bijection, so it is an isomorphism. □

Lemma 4.5. *The subsets H and H' are both half-systems for R.*

Proof. We first prove that $H = \{(a, b) : 1 \leq a \leq \frac{p-1}{2}, 1 \leq b \leq q - 1\}$ is a half-system. According to the definition of a half-system, we need to prove that for all $u = (a, b) \in H$, $-u \notin H$. Assume for the sake of contradiction that $-u = (-a, -b) \in H$, so $-a \equiv kp - a \in [1, \frac{p-1}{2}]$ for some $k \in \mathbb{Z}$ where $a \in [1, \frac{p-1}{2}]$. Then we have $(kp - a) + a = kp \in [2, p - 1]$. Such $k \in \mathbb{Z}$ does not exist, leading to a contradiction. Therefore, H is a half-system for R.

Then, we will prove that $H' = \{(a, a) : 1 \leq a \leq \frac{pq-1}{2}, \gcd(a, pq) = 1\}$ is also a half-system in R. Similarly, we want to prove that for $u \in H'$, $-u \notin H'$. If $u = (a, a) \in H'$, then $-u = (-a, -a)$. According to the Chinese Remainder Theorem, $H' = \{(a, a) : 1 \leq a \leq \frac{pq-1}{2}, \gcd(a, pq) = 1\} \cong \mathbb{Z}_{pq} \cap [1, \frac{pq-1}{2}]$.

As we have proved for H, similarly, $a \in [1, \frac{pq-1}{2}]$, then $-a \notin [1, \frac{pq-1}{2}]$. Therefore, $\mathbb{Z}_{pq} \cap [1, \frac{pq-1}{2}]$ is a half-system in the ring $\mathbb{Z}_{pq}$.

In Lemma 4.4, we showed that there exists an isomorphism from $\mathbb{Z}_p \times \mathbb{Z}_q$ to $\mathbb{Z}_{pq}$. Thus, H' is also a half-system for $R : \mathbb{Z}_p \times \mathbb{Z}_q$. □

Since we already proved that two half-systems H and H' for the same ring R satisfy $\mathbf{P}(H) = \mathbf{P}(H')$, we are interested in calculating the product of H and H' and trying to connect it with quadratic reciprocity.

To start calculating the product of all elements of H, a frequently used theorem is Wilson's Theorem.

Theorem 4.6 (Wilson's Theorem)**.** *If p is prime, $(p-1)! \equiv -1 \pmod{p}$.*

Proof. We begin with the set $\mathbb{U}_p$. For all distinct $a \in \mathbb{U}_p$, we can find some distinct $b \in \mathbb{U}_p$ such that $ab \equiv 1 \pmod{p}$ and $a \neq b$, except for the elements 1 and -1, since $1 \cdot 1 \equiv (-1) \cdot (-1) \equiv 1 \pmod{p}$. In other words, every element in $\mathbb{U}_p$ has a distinct multiplicative inverse except for 1 and -1. Then, if we pair the multiplicative inverses and take the product of all elements in $\mathbb{U}_p$, we will get:

$$(p-1)! \equiv 1^{(p-1)/2} \cdot 1 \cdot -1 = -1. \pmod{p}.$$

Thus, $(p-1)! \equiv -1 \pmod{p}$. □

Then we apply Wilson's Theorem to help calculating the product of all elements in H.

Lemma 4.7. *The product of all elements of H, $\mathbf{P}(H) = \left((-1)^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}}\right)$.*

Proof. Denote the result of component-wise multiplication as $\mathbf{P}(H) = (A, B)$, for $A \in \mathbb{Z}_p$, $B \in \mathbb{Z}_q$. First, we will find A. For each possible b, we have $1 \leq a \leq \frac{p-1}{2}$, so the product of the possible a would be $\left(\frac{p-1}{2}\right)!$. Furthermore, there are $q-1$ possible b, so we want to find $\left(\left(\frac{p-1}{2}\right)!\right)^{q-1} \mod p$.

Now, note by Theorem 4.6 (Wilson's Theorem) that $(p-1)! \equiv -1 \pmod{p}$, and that $\prod_{i=\frac{p+1}{2}}^{p-1} i$. Namely

$$\prod_{i=\frac{p+1}{2}}^{p-1} i = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$$

Then, taking the product of possible a when $q = 1$ and $q = 2$, we get

$$\left(\frac{p-1}{2}\right)! \cdot \prod_{i=\frac{p+1}{2}}^{p-1} i = (p-1)! = -1.$$

However,

$$\left(\frac{p-1}{2}\right)! \cdot \prod_{i=\frac{p+1}{2}}^{p-1} i = \left(\frac{p-1}{2}\right)^2 \cdot (-1)^{\frac{p-1}{2}}$$

Thus, we finally end up with

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

Next, multiplying both sides by $(-1)^{(p-1)/2}$ gives

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

Finally, to get $((\frac{p-1}{2})!)^{q-1}$, we raise both sides of the equation to the $\frac{q-1}{2}$ power to get:

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

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

Now, we will find B. For each possible a, we have $1 \leq b \leq q-1$, so the product of the possible b would be $(q-1)! \equiv -1 \pmod{q}$ by Theorem 4.6 (Wilson's Theorem). Furthermore, since there are $\frac{p-1}{2}$ possible a, we raise -1 to the $\frac{p-1}{2}$ power to get:

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

Thus, we have:

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

□

Then, similarly, we calculate the product of all elements in H'.

Lemma 4.8. *The product of all elements of H', $\mathbf{P}(H') = \left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)$.*

Proof. Because $\gcd(a, pq) = 1$, since p and q are distinct odd primes, $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$, implying a is not divisible by p and q.

Denote the result of component-wise multiplication as $\mathbf{P}(H') = (A', B')$, $A' \in \mathbb{Z}_p, B' \in \mathbb{Z}_q$. First consider A'. We will multiply all the integers $a \in [1, \frac{pq-1}{2}]$ not divisible by p or q:

$$A' = \prod_{p,q \nmid a} a, \qquad a \in \left[0, \frac{pq-1}{2}\right].$$

Consider $a \in [1, \frac{pq-1}{2}]$. The elements not divisible by wp are listed below:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & p-1 \\ p+1 & p+2 & p+3 & \cdots & p+(p-1) \\ 2p+1 & 2p+2 & 2p+3 & \cdots & 2p+(p-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{q-3}{2}p+1 & \frac{q-3}{2}p+2 & \frac{q-3}{2}p+3 & \cdots & \frac{q-3}{2}p+(p-1) \\ \frac{q-1}{2}p+1 & \frac{q-1}{2}p+2 & \cdots & \frac{q-1}{2}p+\frac{p-1}{2}=\frac{pq-1}{2} & \end{array}$$

Calculate the product of elements in the same complete row k,

$$\begin{aligned} &(kp+1)(kp+2)(kp+3)\cdots(kp+p-1) \\ \equiv &1\cdot 2\cdot 3\cdots(p-1)=(p-1)! \end{aligned}$$

for $k \in [0, \frac{q-3}{2}]$. Consider Theorem 4.6 (Wilson's Theorem), the product of elements in the same row $= (p-1)! \equiv -1 \pmod{p}$. Note that there are $\frac{q-1}{2}$ complete rows in total, so the product of all the elements in the complete rows not divisible by p is $(-1)^{(q-1)/2}$.

Some elements are on the last row where $k = \frac{q-1}{2}$. We calculate their product separately:

$$\left(\frac{q-1}{2}p+1\right)\left(\frac{q-1}{2}p+2\right)\cdots\left(\frac{q-1}{2}p+\frac{p-1}{2}\right) \equiv 1\cdot 2\cdots\frac{p-1}{2}=\left(\frac{p-1}{2}\right)! \pmod{p}$$

Therefore, the product of elements that do not divide p is

$$\prod_{p\nmid a} a = (-1)^{\frac{q-1}{2}}\cdot\left(\frac{p-1}{2}\right)!, \qquad a \in \left[1, \frac{pq-1}{2}\right].$$

Then, consider excluding elements $a \in [1, \frac{pq-1}{2}]$ that are divisible by q. We claim that there do not exist any elements $a \in [1, \frac{pq-1}{2}]$ that divide p and q at the same time.

For the sake of contradiction, assume that there exists such an a satisfying $p \mid a, q \mid a$ at the same time. Then, $a \geq \operatorname{lcm}(p,q)$. Since p, q are odd primes, $\operatorname{lcm}(p,q) = pq$, so $a \geq pq$, contradicting with the construction of the half-system that $a \leq \frac{pq-1}{2} < pq$. Therefore, to divide out all the elements divisible by q, we calculate the number of a such that $q \mid a$

$$\#a \text{ such that } q \mid a = \left\lfloor \frac{(pq-1)/2}{q} \right\rfloor = \frac{p-1}{2}.$$

These a are $q, 2q, \ldots, \frac{p-1}{2}q$. Therefore, the product of all elements divisible by q is:

$$\prod_{q\mid a} a = q\cdot 2q\cdots\frac{p-1}{2}q = \left(\frac{p-1}{2}\right)!\cdot q^{\frac{p-1}{2}}, \qquad a \in \left[1, \frac{pq-1}{2}\right].$$

Therefore, the product A' is

$$\begin{aligned} A' = \prod_{p,q\nmid a} a &= \frac{\prod_{p\nmid a} a}{\prod_{q\mid a} a} \\ &\equiv \frac{(-1)^{\frac{q-1}{2}} \cdot (\frac{p-1}{2})!}{(\frac{p-1}{2})! \cdot q^{\frac{p-1}{2}}} \\ &\equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \pmod{p}. \end{aligned}$$

Considering Theorem 3.1 (FℓT), we have $q^{p-1} \equiv 1 \pmod{p}$, so we multiply by 1:

$$\begin{aligned} A' = \prod_{p,q\nmid a} a &\equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \\ &= \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \cdot q^{p-1} \\ &= (-1)^{\frac{q-1}{2}} \cdot q^{\frac{p-1}{2}} \\ &= (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}. \end{aligned}$$

Similarly, for $B' \in \mathbb{Z}_q$, we can do the exact same procedure and derive that

$$B' = \prod_{p,q\nmid a} a \equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \pmod{q}.$$

Therefore, we have proved that $\mathbf{P}(H') = \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right), \frac{p-1}{2} \left(\frac{p}{q}\right)\right)$. □

Reaching here, we can finally combine what we have proven about the lemmas for half-systems and use these to yield the proof of Theorem 1.2, the quadratic reciprocity law.

Theorem 1.2. *If p, q are positive odd primes, then*

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

Proof. According to Lemma 4.5, we know that both H and H' constructed are half-systems in $R = \mathbb{Z}_p \times \mathbb{Z}_q$. As Lemma 4.3 stated, $\mathbf{P}(H) = \pm\mathbf{P}(H')$. Denote the result of component-wise multiplication for H and H' as

$$\mathbf{P}(H) = (A, B), \mathbf{P}(H') = (A', B').$$

Respectively, we have,

$$A = \pm A'$$
$$B = \pm B'.$$

Regardless of whether it is $A = A', B = B'$ or $A = -A', B = -B'$, the equation

$$AB = A'B'$$

always holds. Therefore, plugging in the values of A, B, A', B' calculated in Lemma 4.7 and 4.8, we have

$$\begin{aligned} AB &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ A'B' &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\ \implies (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \end{aligned}$$

Since $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \neq 0$, canceling $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ on both sides, we have

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

Therefore, we have proved that for distinct odd prime numbers p and q,

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

□

5. Applications of Quadratic Reciprocity

Observe what we discovered from the law of quadratic reciprocity, as the equation

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

holds, if $2 \mid \frac{p-1}{2}\frac{q-1}{2}$, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \implies \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

If instead, $2 \nmid \frac{p-1}{2}\frac{q-1}{2}$, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \implies \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

The law of quadratic reciprocity gives us a efficient method to compute whether a number is a perfect square modulo a prime. It is often useful in simplifying large calculations, as demonstrated by the examples below.

Example 5.1. *Check if 17 is a square in $\mathbb{Z}_{509}$.*

Solution. Since 17 and 509 are both odd primes, we apply quadratic reciprocity as follows:

$$2 \mid \frac{17-1}{2}\frac{509-1}{2}, \qquad \left(\frac{17}{509}\right) = \left(\frac{509}{17}\right).$$

By applying Lemma 3.4, we have

$$\left(\frac{17}{509}\right) = \left(\frac{509}{17}\right) = \left(\frac{16}{17}\right).$$

Clearly, $\left(\frac{16}{17}\right) = 1$, since $16 = 4^2$ is a square in $\mathbb{Z}$. Therefore, we have $\left(\frac{17}{509}\right) = 1$, implying that 17 is a square in $\mathbb{Z}_{509}$.

Now, we have used quadratic reciprocity to confirm that 17 is a square mod 509, greatly improving efficiency compared to if we had to manually check each residue. □

Example 5.2. *Check if 57 is a square in $\mathbb{Z}_{73}$.*

Solution. Note that 57 is not a prime, so we cannot directly plug into the quadratic reciprocity law. Instead, recall that Lemma 3.3 implies that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

we can factorize 57 as the product of 2 primes, changing $\left(\frac{57}{73}\right)$ to

$$\left(\frac{57}{73}\right) = \left(\frac{3}{73}\right)\left(\frac{19}{73}\right).$$

Then, we check $\left(\frac{3}{73}\right)$ and $\left(\frac{19}{73}\right)$ separately.

$$2 \mid \frac{73-1}{2}\frac{3-1}{2}, \qquad \left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$$
$$2 \mid \frac{19-1}{2}\frac{73-1}{2}, \qquad \left(\frac{19}{73}\right) = \left(\frac{73}{19}\right) = \left(\frac{16}{19}\right)$$

Since 16 is a square in $\mathbb{Z}$, it is definitely a quadratic residue in $\mathbb{Z}_{19}$. Therefore, $\left(\frac{19}{73}\right) = \left(\frac{16}{19}\right) = 1$.

Therefore, $\left(\frac{57}{73}\right) = \left(\frac{19}{73}\right)\left(\frac{3}{73}\right) = 1 \cdot 1 = 1$, showing that there exists an element such that its square is equivalent to 57 in $\mathbb{Z}_{73}$. □

Example 5.3. *Check if the equation $x^2 = 5$ has solutions in $\mathbb{Z}_{119}$.*

Solution. Consider $x^2 \equiv 5 \pmod{119} \Rightarrow x^2 = 119k + 5$, implying that $x^2 \equiv 5 \pmod{7}, x^2 \equiv 5 \pmod{17}$. So we check $\left(\frac{5}{7}\right)$ and $\left(\frac{5}{17}\right)$,

$$2 \mid \frac{5-1}{2}\frac{7-1}{2}, \qquad \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Since in modulo 7, 5 is not a quadratic residue, 5 is not a quadratic residue in modulo 119. Therefore, the equation $x^2 = 5$ has no solutions in $\mathbb{Z}_{119}$. □

6. Conclusion

The uses of quadratic reciprocity have extended past number theory, with applications in both other mathematical fields, as well as more modern real world applications. Its further applications in the field of mathematics include its relations to class field theory, a important branch of algebraic number theory. In fact, class field theory can be viewed as a generalization of quadratic reciprocity.

Furthermore, it also has applications in the area of cryptography. The first public-key encryption (a form of encryption involving the usage of a public key for encryption and a private key for decryption, often involving modular arithmetic) scheme requires calculations that can be made much more efficient using quadratic reciprocity. Overall, quadratic reciprocity has played a crucial role in the field of number theory as it stands today, and continues to play a part in the path for future discovery.