Investigating Proofs of the Quadratic Reciprocity Law

Cuyler Warnock

December 2, 2016

Abstract

For over 300 years, number theorists have investigated quadratic residues and their properties. A quadratic residue modulo p is an integer a such that $x^2 \equiv a \pmod{p}$ for some $x \in \mathbb{Z}_p$. Number theorists such as Fermat, Euler, Legendre, and Gauss were interested in finding conditions for distinct primes p and q so that p would be a quadratic residue modulo q and q would be a quadratic residue modulo p. Through the contributions of these mathematicians, a surprisingly eloquent relationship was discovered: the quadratic nature of p modulo q is the same as the quadratic nature of q modulo p if and only if $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$. This result, first proved by Gauss in the late 1790's, has become known as the Quadratic Reciprocity Law. Since that time, there have been hundreds of different proofs published. These proofs exhibit an astounding variety of methods derived from various branches of mathematics. We will investigate three different proofs, each varying in proof technique and complexity.

1 Introduction

First stated by Euler, the Quadratic Reciprocity Law was discovered because of the need to determine whether p is a quadratic residue modulo q where p and q are distinct primes. In other words, Euler was interested in determining conditions for the solvability of the congruence

$$x^2 \equiv p \pmod{q},$$

where p and q are distinct primes. A century before Euler, Fermat had also attempted to discover a realtionship among these distinct primes p and q. In 1658, Fermat wrote in a letter to Kenelm Digby that he already knew the conditions for which odd primes q and the numbers $\pm 1, \pm 2, \pm 3, 5$ are quadratic residues or nonresidues modulo q. The results of Fermat, Euler, and others were conjectured based on empirical evidence, but were given without any proofs. Eventually, Euler was able to prove the case for -1 and ± 3, and Lagrange proved the case for ± 2 and ± 5.

By further examining these cases, Euler was able to formulate the Quadratic Reciprocity

Law in full generality. He gives the following four theorems that completely contain the Quadratic Reciprocity Law. Let p and q be distinct primes.

1. If $p \equiv 1 \pmod 4$ and $p \equiv x^2 \pmod q$ for some integer x, then $\pm q \equiv y^2 \pmod p$ for some integer y.

2. If $p \equiv 3 \pmod 4$ and $-p \equiv x^2 \pmod q$ for some integer x, then $q \equiv y^2 \pmod p$ for some integer y and $-q \not\equiv z^2 \pmod p$ for all integers z.

3. If $p \equiv 3 \pmod 4$ and $-p \not\equiv x^2 \pmod q$ for all integers x, then $-q \equiv y^2 \pmod p$ for some integer y and $q \not\equiv z^2 \pmod p$ for all integers z.

4. If $p \equiv 1 \pmod 4$ and $p \not\equiv x^2 \pmod q$ for all integers x, then $\pm q \not\equiv y^2 \pmod p$ for all integers y.

Gauss, unknowing that Euler had formulated a version of the Quadratic Reciprocity Law, credits Legendre with the discovery of this law. In 1785, Legendre explicitly stated the theorem using formulas and gave several proofs, each of which contained serious gaps pointed out by Gauss. Since Legendre noticed that the solvability of $x^2 \equiv p \pmod q$ where p and q are distinct primes and x is an integer depends on whether $p^{\frac{q-1}{2}} \equiv 1 \pmod q$ or $p^{\frac{q-1}{2}} \equiv -1 \pmod q$, Legendre developed a useful shorthand notation to represent whether an integer is a quadratic residue modulo p where p is prime. In [7] on page 186, Legendre states,

> "Since the analogous quantities $N^{\frac{c-1}{2}}$ will occur often in our researches, we shall employ the abbreviation $\left(\frac{N}{c}\right)$ for expressing the residue that $N^{\frac{c-1}{2}}$ gives upon division by c, and which, according to what we just have seen, only assumes the values $+1$ or -1."

Also, in [7] on page 214, Legendre gives the Quadratic Reciprocity Law in its commonly written form. He writes

> "Whatever the prime numbers m and n are, if they are not both of the form $4x-1$, one always has $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$; and if both are of the form $4x-1$, one has $\left(\frac{n}{m}\right) = -\left(\frac{m}{n}\right)$. These two general cases are contained in the formula
>
> $$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{m}{n}\right)."$$

Even though Legendre states the theorem using two distinct primes, the Legendre symbol $\left(\frac{a}{p}\right)$ makes sense for composite values of a. Legendre never provided a complete and accurate proof of this theorem. However, in 1796 at the age of eighteen, Gauss was able to provide the first complete proof by using induction (see [4] p. 92-97). The proof took Gauss an entire year to complete. Gauss wrote,

> "For a whole year this theorem tormented me and absorbed my greatest efforts until, at last, I obtained the proof explained in the fourth section of the *Disquisitiones Arithmeticae*".

Providing just one proof of the Quadratic Reciprocity Law was not enough for Gauss. By 1818, he had published five other proofs of the theorem and two more were found in his unpublished papers after his death.

Since Gauss' first complete proof of the Quadratic Reciprocity Law, more than 300 proofs have been published ([2] p. 131-138). These proofs exhibit an astounding variety of methods derived from various branches of mathematics, such as quaternion algebras, group theory, geometry, and complex analysis. We will analyze three proofs, each varying in proof technique and complexity.

2 Essential Definitions and Theorems

Before analyzing the proofs, we give some definitions and theorems that we will use in the proofs of the Quadratic Reciprocity Law.

Definition 1 (quadratic residue)**.** *Let p be a prime, and let $a \in \mathbb{Z}$ such that $p \nmid a$. If a is a square modulo p, then a is a* **quadratic residue modulo p**. *If a is not a square modulo p, then a is a* **quadratic nonresidue modulo p**.

In other words, a quadratic residue modulo p is a nonzero square modulo p. Determining whether an integer is a quadratic residue modulo p can be very tedious and time consuming when p becomes large. However, Euler provided a useful method for determining if a is a quadratic residue modulo p by performing modular exponentiation.

Theorem 1 (Euler's Criterion)**.** *Let p be an odd prime, and let a be an integer not divisible by p. If a is a quadratic residue mod p, then*

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

If a is a quadratic nonresidue mod p, then

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

A proof of Euler's Criterion can be found in [3] on pages 171-172. Using Euler's Criterion to determine if an integer a is a quadratic residue modulo p can still take be tedious; however, it is a better technique than squaring each positive integer less than $(p/2)$ and checking if it is congruent to a modulo p. We will show the usefulness of Euler's Criterion with an example.

Example: Is -74 is a quadratic residue modulo 167.

Solution. Since 167 is prime, we will use Euler's Criterion. Note that $\frac{167-1}{2} = 83$. Therefore, we will calculate $(-74)^{83} \pmod{167}$. Note the following:

$$\begin{aligned}
(-74)^{83} &\equiv (-74)^{64} \cdot (-74)^{16} \cdot (-74)^{2} \cdot (-74) \pmod{167} \\
&\equiv 5476^{32} \cdot 5476^{8} \cdot 5476 \cdot (-74) \pmod{167} \\
&\equiv 132^{32} \cdot 132^{8} \cdot (-9768) \pmod{167} \\
&\equiv 17424^{16} \cdot 17424^{4} \cdot (-82) \pmod{167} \\
&\equiv 56^{16} \cdot 56^{4} \cdot (-82) \pmod{167} \\
&\equiv 3136^{8} \cdot 3136^{2} \cdot (-82) \pmod{167} \\
&\equiv 130^{8} \cdot 130^{2} \cdot (-82) \pmod{167} \\
&\equiv 16900^{4} \cdot 16900 \cdot (-82) \pmod{167} \\
&\equiv 33^{4} \cdot (-34) \pmod{167} \\
&\equiv 1089^{2} \cdot (-34) \pmod{167} \\
&\equiv 87^{2} \cdot (-34) \pmod{167} \\
&\equiv 7569 \cdot (-34) \pmod{167} \\
&\equiv 1 \pmod{167}.
\end{aligned}$$

Therefore, we have $(-74)^{83} \equiv 1 \pmod{83}$. Thus, by Euler's Criterion we have that -74 is a quadratic residue modulo 167. □

As stated in the introduction, Legendre developed a useful shorthand notation to represent whether an integer a is a quadratic residue modulo p.

Definition 2 (Legendre symbol)**.** *Let p be a prime, and let $a \in \mathbb{Z}$. The* **Legendre symbol** $\left(\frac{a}{p}\right)$ *is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & \text{if } \ p|a \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

In one of the proofs we will analyze, we are concerned with finding a solution to a system of linear congruences. Therefore, the following theorem will be useful.

Theorem 2 (Chinese Remainder Theorem)**.** *Let k be a positive integer and let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers. Let $b_1, b_2, \ldots, b_k$ be arbitrary integers. Then the system*

$$\begin{aligned}
x &\equiv b_1 \pmod{m_1} \\
x &\equiv b_k \pmod{m_k} \\
&\vdots \\
x &\equiv b_k \pmod{m_k}
\end{aligned}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

A proof of the Chinese Remainder Theorem can be found in [3] on pages 79-80. In this proof of the Chinese Remainder Theorem, a formula for the solution to such a system of linear congruences is constructed; and such a solution is of the form

$$x \equiv b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_k M_k M_k' \pmod{m_1 m_2 \cdots m_k},$$

where $M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$ for each $i \in \{1, 2, \cdots, k\}$ and M_i' is an integer such that $M_i M_i' \equiv 1 \pmod{m_i}$.

Wilson's Theorem will also be important in one of the proofs of the Quadratic Reciprocity Law.

Theorem 3 (Wilson's Theorem)**.** *If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

A proof of Wilson's Theorem can be found in [10] on page 186.

3 Importance of the Quadratic Reciprocity Law

As previously mentioned, the Quadratic Reciprocity Law provides a very useful method in determining whether an integer a is a quadratic residue modulo p, or equivalently, determining whether $\left(\frac{a}{p}\right) = \pm 1$. We first present some useful theorems in helping to determine the value of $\left(\frac{a}{p}\right)$.

Theorem 4. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, and let p be a prime. Then the following hold.*

1. *If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *If $a \not\equiv 0 \pmod{p}$, then $\left(\frac{a^2}{p}\right) = 1$.*
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Theorem 5. *For p an odd prime,*

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

Theorem 6. *For p an odd prime,*

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

A proof of Theorem 4 can be found in [3] on page 176. A proof of Theorems 5 and 6 can be found in [10] on pages 335 and 337-338 respectively. Using the results stated above, we are able to determine the value of $\left(\frac{a}{p}\right)$ relatively quickly. However, the Quadratic Reciprocity Law provides even faster techniques for determining the value of $\left(\frac{a}{p}\right)$.

Theorem 7 (Quadratic Reciprocity Law)**.** *If p and q are odd primes, then*

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

Note that if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $(\frac{p-1}{2})(\frac{q-1}{2})$ is even. Thus, $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$. However, if $p \equiv q \equiv 3 \pmod 4$, then $(\frac{p-1}{2})(\frac{q-1}{2})$ is odd. Therefore $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$. Thus, we have an alternate form of the Quadratic Reciprocity Law.

Theorem 8 (Quadratic Reciprocity Law)**.** *If p and q are odd primes, then*

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

We will now rework the earlier example to show the ease with which $\left(\frac{a}{p}\right)$ can be calculated by using the above theorems.

Example: Is -74 is a quadratic residue modulo 167.

Solution. Note that 167 is prime. Consider the following:

$$\begin{aligned}
\left(\frac{-74}{167}\right) &= \left(\frac{-1}{167}\right)\left(\frac{2}{167}\right)\left(\frac{37}{167}\right) && \text{By Theorem 4 (4) since } -74 = (-1)(2)(37) \\
&= (-1)\left(\frac{2}{167}\right)\left(\frac{37}{167}\right) && \text{By Theorem 5 since } 167 \equiv -1 \pmod 4 \\
&= -(1)\left(\frac{37}{167}\right) && \text{By Theorem 6 since } 167 \equiv -1 \pmod 8 \\
&= -\left(\frac{167}{37}\right) && \text{By QRL since } 37 \equiv 1 \pmod 4 \\
&= -\left(\frac{19}{37}\right) && \text{By Theorem 4 (1) since } 167 \equiv 19 \pmod{37} \\
&= -\left(\frac{37}{19}\right) && \text{By QRL since } 37 \equiv 1 \pmod 4 \\
&= -\left(\frac{-1}{19}\right) && \text{By Theorem 4 (1) since } 37 \equiv -1 \pmod{19} \\
&= -(-1) && \text{By Theorem 5 since } 19 \equiv -1 \pmod 4 \\
&= 1.
\end{aligned}$$

Therefore, we have that $\left(\frac{-74}{167}\right) = 1$. Hence, -74 is a quadratic residue modulo 167. □

4 Proofs

4.1 Classical Proof by Gauss

The first proof we will analyze is a variation of Gauss' third proof which was simplified by Eisenstein. In this proof, Gauss uses what is now known as Gauss' Lemma, which is used in more than 50 proofs of the Quadratic Reciprocity Law.

Lemma 1 (Gauss' Lemma)**.** *Let p be an odd prime and let a be an integer such that $p \nmid a$. Let n denote the number of least positive residues of the integers $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ that exceed $p/2$. Then $\left(\frac{a}{p}\right) = (-1)^n$.*

Proof. Let p be an odd prime and let a be an integer such that $p \nmid a$. Let n denote the number of least positive residues of the integers $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ that exceed $\frac{p}{2}$. Since $\gcd(a, p) = 1$, we have that each of the elements $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ are unique modulo p. Since $p \nmid a$, we know that $ak \not\equiv 0 \pmod p$ for each $k \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Let m and n be integers and let $r_1, r_2, \ldots, r_m$ denote the least positive residues of $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ such that $0 < r_i < p/2$ and let $s_1, s_2, \ldots, s_n$ denote the least positive residues of $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ such that $p/2 < s_j < p$. Note that no least positive integer is equal to $p/2$ since p is an odd integer which implies that $p/2$ is not an integer. It follows that $m + n = (p-1)/2$ and that the integers

$$r_1, r_2, \ldots, r_m, p - s_1, p - s_2, \ldots, p - s_n$$

are all positive and less than $p/2$.

We will show that each of these above integers is distinct. Suppose to the contrary that $r_i = p - s_j$ for some $i, j \in \mathbb{Z}$ where $1 \leq i \leq m$ and $1 \leq j \leq n$. By definition of r_i and s_j, there exist integers $u, v \in \{1, 2, \ldots, \frac{p-1}{2}\}$ such that $r_i \equiv ua \pmod{p}$ and $s_j \equiv va \pmod{p}$. It follows that

$$(u+v)a = ua + va \equiv r_i + s_j \equiv p \equiv 0 \pmod{p}.$$

On the other hand, since $1 < u + v < p - 1$, we know that $(u+v)a \not\equiv 0 \pmod{p}$. Hence, each r_i and s_j are distinct. It follows that the $\frac{p-1}{2}$ numbers

$$r_1, r_2, \ldots, r_m, p - s_1, p - s_2, \ldots, p - s_n$$

are some rearrangement of the integers $1, 2, \ldots, \frac{p-1}{2}$. It follows that the product of the $\frac{p-1}{2}$ above numbers is $\left(\frac{p-1}{2}\right)!$. Note that

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \\
&\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod{p} \\
&\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p} \\
&\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \pmod{p} \\
&\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.
\end{aligned}$$

Thus $\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$. Since $\left(\frac{p-1}{2}\right)!$ is relatively prime to p, we know that $\left(\frac{p-1}{2}\right)!$ has an inverse modulo p. Multiplying both sides of the above congruence by the inverse of $\left(\frac{p-1}{2}\right)!$ yields $1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p}$. Multiplying both sides by $(-1)^n$ yields $(-1)^n \equiv a^{\frac{p-1}{2}} \pmod{p}$. By using Euler's criterion, we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. Therefore, we conclude that

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

□

Lemma 2 (Eisenstein's Lemma)**.** *If p is an odd prime and a is an odd integer with* $\gcd(a, p) = 1$*, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Proof. Let p be an odd prime and let a be an odd integer such that $\gcd(a, p) = 1$. Let $S = \{a, 2a, \ldots, \left(\frac{p-1}{2}\right)a\}$. Using the division algorithm, we obtain $ka = pq_k + b_k$ where $q_k \in \mathbb{Z}$, $k \in \{1, 2, \ldots, \frac{p-1}{2}\}$ and $b_k \in \{0, 1, \ldots, p-1\}$. It follows that $\frac{ka}{p} = q_k + \frac{b_k}{p}$. Hence, $\left\lfloor \frac{ka}{p} \right\rfloor = q_k$. Therefore, we have that

$$ka = \left\lfloor \frac{ka}{p} \right\rfloor p + b_k.$$

If $b_k < \frac{p}{2}$, then it is one of the integers r_i from the proof of Gauss' Lemma. If $b_k > \frac{p}{2}$, then it is one of the integers s_j from the proof of Gauss' Lemma. Therefore, we obtain the following:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k.$$

From the proof of Gauss' Lemma, we have that the $\frac{p-1}{2}$ numbers

$$r_1, r_2, \ldots, r_m, p - s_1, p - s_2, \ldots, p - s_n$$

are just a rearrangement of the integer $1, 2, \ldots, \frac{p-1}{2}$. Therefore, we have that

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k.$$

Note the following:

$$\begin{aligned}
(a-1)\sum_{k=1}^{\frac{p-1}{2}} k &= a\sum_{k=1}^{\frac{p-1}{2}} k - \sum_{k=1}^{\frac{p-1}{2}} k \\
&= \sum_{k=1}^{\frac{p-1}{2}} ka - \sum_{k=1}^{\frac{p-1}{2}} k \\
&= \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k - \left(pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \right) \\
&= p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \right) + 2\sum_{k=1}^{n} s_k.
\end{aligned}$$

Thus, $(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n\right) + 2\sum_{k=1}^{n} s_k$. Since a and p are odd integers, we know that $a - 1 \equiv 0 \pmod 2$ and $p \equiv 1 \pmod 2$. Therefore, considering the above equation modulo 2 yields $0 \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \pmod 2$ which implies that $n \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2$. Therefore, by Gauss' Lemma, we obtain the following:

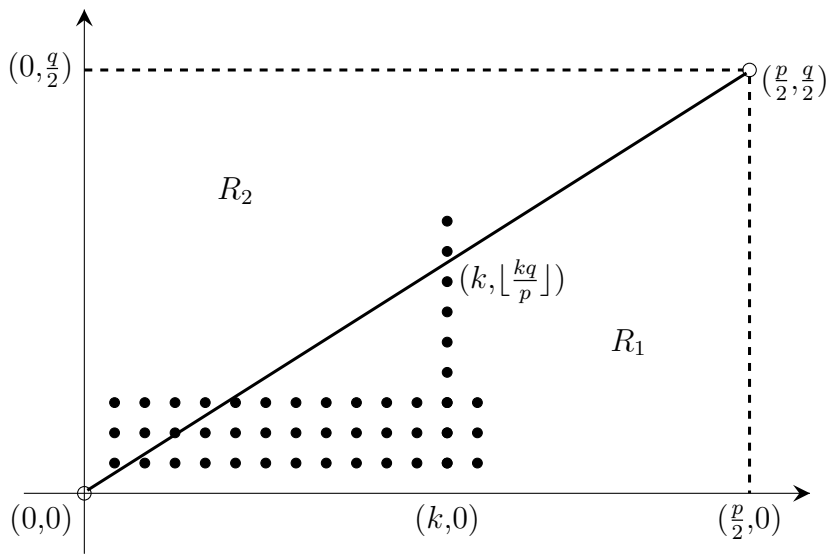
$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

□

Theorem 7. (Quadratic Reciprocity Law) *If p and q are distinct odd primes, then*

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

Proof. Let p and q be distinct odd primes. Consider the rectangle in the xy coordinate plane whose vertices are $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2})$, and $(\frac{p}{2}, \frac{q}{2})$. Let R denote the region within the rectangle not including the boundary lines. We will count the number of lattice points inside R in two different ways. Since p and q are odd, the lattice points in R consists of all point (m, n) where $m, n \in \mathbb{Z}$ with $1 \leq m \leq \frac{p-1}{2}$ and $1 \leq n \leq \frac{q-1}{2}$. It follows that the number of lattice points in R is $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Let D denote the diagonal from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ excluding the endpoints. It follows that D is a segment of the line with equation $y = (q/p)x$, or equivalently, $py = qx$. Suppose (a, b) is a lattice point on D. Then $pb = qa$ which implies that $p \mid a$. However, we know that $p \nmid a$ since $a \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Therefore, no lattice points lie on D. Let R_1 denote the region in R that is below D and let R_2 denote the region in R that is above D. We will now count the number of lattice points in both R_1 and R_2.



Let k be an integer such that $1 \leq k \leq \frac{p-1}{2}$. We have that the number of integers less than $\frac{kq}{p}$ is equal to $\lfloor \frac{kq}{p} \rfloor$. Therefore, we have that there are exactly $\lfloor \frac{kq}{p} \rfloor$ lattice points in R_1 on the line $x = k$. Consequently, we have that the total number of lattice points in R_1 is given by

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

We use a similar argument for counting the points in R_2. For each $k \in \{1, 2, \ldots, \frac{q-1}{2}\}$, there are $\lfloor \frac{kp}{q} \rfloor$ lattice points on the line $y = k$ in R_2. Hence, the total number of lattice points in R_2 is given by

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Since this accounts for all of the lattice points in R, we have that

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Using Lemma 2, we obtain the following:

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{kp}{q}\right\rfloor}(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor}\\ &= (-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{kp}{q}\right\rfloor+\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor}\\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.\end{aligned}$$

Therefore, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

4.2 Kim

In 2004, Sey Y. Kim published a proof of the Quadratic Reciprocity Law that uses elementary number theory results such as Wilson's Theorem and the Chinese Remainder Theorem. This proof is similar to a proof by George Rousseau in 1991.

Let p and q be distinct odd primes and let

$$\Phi = \left\{a \in \mathbb{Z} : 1 \leq a \leq \frac{pq-1}{2} \text{ and } \gcd(a, pq) = 1\right\},$$

and let $A = \prod_{a\in\Phi} a$. We will first prove the following lemma.

Lemma 3. *$A \equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod{p}$ and $A \equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod{q}$.*

Proof. Let

$$S = \left\{a \in \mathbb{Z} : 1 \leq a \leq \frac{pq-1}{2} \text{ and } \gcd(a, p) = 1\right\} \quad \text{and} \quad T = \left\{q \cdot 1, \ldots, q \cdot \frac{p-1}{2}\right\}.$$

We will show $T \subseteq S$. Let $t \in T$. It follows that $t = qb$ for some $b \in \mathbb{Z}$ such that $1 \leq b \leq \frac{p-1}{2}$. Since p and q are distinct prime, we know that $p \nmid q$. Also, since $b \leq \frac{p-1}{2}$, we know that $p \nmid b$. Therefore, $p \nmid t$. It follows that $\gcd(t, p) = 1$. We now show that $t \leq \frac{pq-1}{2}$. Since $q > 1$, we know that $pq - q < pq - 1$. It follows that $\frac{pq-q}{2} < \frac{pq-1}{2}$. Since $t \leq \frac{pq-q}{2}$ by definition of T, we know that $t < \frac{pq-1}{2}$. Therefore, we have that $\gcd(t, p) = 1$ and $1 \leq t \leq \frac{pq-1}{2}$. Hence, $t \in S$. It follows that $T \subseteq S$. Note that S and Φ contain the same elements except that Φ does not contain any multiples of q while S contains all positive multiples of q less than $\frac{pq-1}{2}$. Since $\frac{pq-1}{2} = \frac{p-1}{2} \cdot q + \frac{q-1}{2}$, we have that S contains $q \cdot 1, q \cdot 2, \ldots, q \cdot \frac{p-1}{2}$. Note that these multiples of q are precisely the elements in the set T. Therefore, we have that $S = \Phi \cup T$. Since Φ contains no multiples of q, we also have that $\Phi \cap T = \emptyset$. Thus, by Euler's criterion, we have

that

$$\begin{aligned}\prod_{a\in S} a &= \prod_{a\in T} a \cdot \prod_{a\in \Phi} a \\ &= (q\cdot 1)(q\cdot 2)\cdots(q\cdot \frac{p-1}{2})\cdot A \\ &= q^{\frac{p-1}{2}}\left[\frac{p-1}{2}\right]!\cdot A \\ &\equiv \left(\frac{q}{p}\right)\left[\frac{p-1}{2}\right]!\cdot A \pmod{p}.\end{aligned}$$

Hence,

$$\prod_{a\in S} a \equiv \left(\frac{q}{p}\right)\left[\frac{p-1}{2}\right]!\cdot A \pmod{p}. \tag{1}$$

Since we have that $\frac{pq-1}{2} = \frac{q-1}{2}\cdot p + \frac{p-1}{2}$ and since S contains no multiples of p, we obtain the following:

$$\begin{aligned}\prod_{a\in S} a &= (1)\cdots(p-1)(p+1)\cdots(2p-1)(2p+1)\cdots(3p-1)\cdots \\ &\quad \cdots\left(\frac{q-3}{2}p+1\right)\cdots\left(\frac{q-1}{2}p-1\right)\left(\frac{q-1}{2}p+1\right)\cdots\left(\frac{q-1}{2}p+\frac{p-1}{2}\right) \\ &\equiv [(p-1)!]^{\frac{q-1}{2}}\left[\frac{p-1}{2}\right]! \pmod{p} \\ &\equiv (-1)^{\frac{q-1}{2}}\left[\frac{p-1}{2}\right]! \pmod{p},\end{aligned}$$

where we have that $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem. Thus,

$$\prod_{a\in S} a \equiv (-1)^{\frac{q-1}{2}}\left[\frac{p-1}{2}\right]! \pmod{p}. \tag{2}$$

It follows from (1) and (2),

$$\left(\frac{q}{p}\right)\left[\frac{p-1}{2}\right]!\cdot A \equiv (-1)^{\frac{q-1}{2}}\left[\frac{p-1}{2}\right]! \pmod{p}.$$

Since $\left[\frac{p-1}{2}\right]!$ and p are relatively prime, we have that the inverse of $\left[\frac{p-1}{2}\right]!$ modulo p exists. Multiplying the above congruence by the inverse of $\left[\frac{p-1}{2}\right]!$ modulo p yields

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

Multiplying both sides of the congruence by $\left(\frac{q}{p}\right)$ yields $A \equiv (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod{p}$. By a similar argument, we deduce $A \equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod{q}$. $\square$

Note that $\pm 1 = (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \equiv A \pmod{p}$ and $\pm 1 = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \equiv A \pmod{q}$. If $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = 1 = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, then we have that $A \equiv 1 \pmod{p}$ and $A \equiv 1 \pmod{q}$ which implies that $A \equiv 1 \pmod{pq}$. Also, if $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = -1 = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$, then we have that $A \equiv -1 \pmod{p}$ and $A \equiv -1 \pmod{q}$ which implies that $A \equiv -1 \pmod{pq}$. Therefore, we have that $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ if and only if $A \equiv 1$ or $-1 \pmod{pq}$. We now present the following lemma.

Lemma 4. *$A \equiv 1$ or $-1 \pmod{pq}$ if and only if $p \equiv q \equiv 1 \pmod{4}$.*

Proof. Consider the congruence $x^2 \equiv 1 \pmod{pq}$. Since p and q are relatively prime, we know that x satisfies one of the following systems of congruences:

$$\begin{array}{cccc} x \equiv 1 \pmod{p} & x \equiv 1 \pmod{p} & x \equiv -1 \pmod{p} & x \equiv -1 \pmod{p} \\ x \equiv 1 \pmod{q} & x \equiv -1 \pmod{q} & x \equiv 1 \pmod{q} & x \equiv -1 \pmod{q} \end{array}$$

By the Chinese Remainder Theorem, we have that each of the systems of congruences has a unique solution modulo pq. Therefore, we have that $x \equiv 1, n, -n, -1 \pmod{pq}$ are the only solutions to $x^2 \equiv 1 \pmod{pq}$, where $n \in \mathbb{Z}_{pq}$ such that $n \equiv 1 \pmod{p}$ and $n \equiv -1 \pmod{q}$. Now consider the congruence $x^2 \equiv -1 \pmod{pq}$ and suppose there exists a solution. Therefore, we have that $pq \mid (x^2+1)$. Since p and q are relatively prime, we have that $p \mid (x^2+1)$ and $q \mid (x^2+1)$. It follows that $x^2 \equiv -1 \pmod{p}$ and $x^2 \equiv -1 \pmod{q}$. Since $x^2 \equiv -1 \pmod{pq}$ has a solution if and only if $x^2 \equiv -1 \pmod{p}$ and $x^2 \equiv -1 \pmod{q}$ have a solution which only occurs when $p \equiv q \equiv 1 \pmod{4}$, we deduce that $x^2 \equiv -1 \pmod{pq}$ has a solution if and only if $p \equiv q \equiv 1 \pmod{4}$. Therefore, if $p \equiv q \equiv 1 \pmod{pq}$, let ℓ be a solution to $x^2 \equiv -1 \pmod{pq}$. It follows that $\ell, -\ell, n\ell, -n\ell$ are all of the solutions to $x^2 \equiv -1 \pmod{pq}$.

We will now show that for each $a \in \Phi$, there exists an $a' \in \Phi$ such that $aa' \equiv \delta \pmod{pq}$ where $\delta \in \{-1, 1\}$. Let $a \in \Phi$. By definition of Φ, we have that $1 \leq a \leq \frac{pq-1}{2}$ and $\gcd(a, pq) = 1$. Since $\gcd(a, pq) = 1$, we have that there exists a nonzero $a' \in \mathbb{Z}_{pq}$ such that $aa' \equiv 1 \pmod{pq}$ and $\gcd(a', pq) = 1$. Since $a' \in \mathbb{Z}_{pq}$ and a' is nonzero, we have that either $1 \leq a' \leq \frac{pq-1}{2}$ or $\frac{pq+1}{2} \leq a' \leq pq - 1$. If $1 \leq a \leq \frac{pq-1}{2}$, we have that $a' \in \Phi$. If $\frac{pq+1}{2} \leq a' \leq pq - 1$, we have that $1 - pq \leq -a' \leq -\frac{pq+1}{2}$. It follows that $-a' \equiv b \pmod{pq}$ for some integer b with $1 \leq b \leq \frac{pq-1}{2}$. Since $\gcd(a', pq) = 1$ and since $-a' \equiv b \pmod{pq}$, we have that $\gcd(b, pq) = 1$. Therefore, $b \in \Phi$. Note that $ab \equiv a(-a') \equiv -aa' \equiv -1 \pmod{pq}$. Thus, we have that for every $a \in \Phi$, there exists $a' \in \Phi$ such that $aa' \equiv \delta \pmod{pq}$ where $\delta \in \{-1, 1\}$.

Let Ψ denote the set containing each $a \in \Phi$ such that $a = a'$, that is, let

$$\Psi = \left\{a^2 \equiv \pm 1 \pmod{pq} \mid a \in \Phi\right\}.$$

Note that for each $a \in \Phi - \Psi$ there exists $a' \in \Phi - \Psi$ with $a \neq a'$ such that $aa' \equiv \pm 1 \pmod{pq}$. However, for each $a \in \Psi$ there does not exist $a' \in \Phi$ with $a \neq a'$ such that $aa' \equiv \pm 1 \pmod{pq}$

since $a = a'$ for all $a \in \Psi$. It follows that

$$A \equiv \prod_{a \in \Phi} a \equiv \pm \prod_{a \in \Psi} a \pmod{pq}.$$

Note that each $a \in \Psi$ is a solution to either $x^2 \equiv 1 \pmod{pq}$ or $x^2 \equiv -1 \pmod{pq}$. Suppose $p \equiv q \equiv 1 \pmod 4$. It follows that

$$A \equiv \prod_{a \in \Phi} a \equiv \pm \prod_{a \in \Psi} a \equiv \pm(1 \cdot n \cdot \ell \cdot n\ell) \equiv \pm(n^2 \cdot \ell^2) \equiv \pm 1 \pmod{pq}.$$

Therefore, $A \equiv \pm 1 \pmod{pq}$ when $p \equiv q \equiv 1 \pmod 4$. Now suppose either $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. It follows that

$$A \equiv \prod_{a \in \Phi} a \equiv \pm \prod_{a \in \Psi} a \equiv \pm(1 \cdot n) \equiv \pm n \not\equiv \pm 1 \pmod{pq}.$$

Therefore, $A \not\equiv \pm 1 \pmod{pq}$ when $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. Consequently, we have that $A \equiv \pm 1 \pmod{pq}$ if and only if $p \equiv q \equiv 1 \pmod 4$. □

Combining Lemma 3 and Lemma 4 we obtain that $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ if and only if $p \equiv q \equiv 1 \pmod 4$. It follows that $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = -(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ if and only if $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. Note that $-(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = 1$ if $p \equiv q \equiv 1 \pmod 4$ but $-(-1)^{\frac{p+1}{2}\frac{q+1}{2}} = -1$ if $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. Therefore, we deduce that

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

or equivalently,

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

Note the following:

$$\begin{aligned}
\frac{p-1}{2}\frac{q-1}{2} &= \frac{pq-p-q+1}{4} \\
&= \frac{pq+p+q+1}{4} - \frac{p-1+q-1+2}{2} \\
&= \frac{p+1}{2}\frac{q+1}{2} - \left(\frac{p-1}{2} + \frac{q-1}{2} + 1\right) \\
&\equiv \frac{p+1}{2}\frac{q+1}{2} + \frac{p-1}{2} + \frac{q-1}{2} + 1 \pmod 2.
\end{aligned}$$

It follows that

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

Therefore, we have

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

4.3 Barnard

Virgil Barnard proves the Quadratic Reciprocity Law by using Euler's Criterion, primitive roots, and properties of the floor function. Upon presenting a modified version of Gauss' Lemma, he uses an argument similar to counting lattice points which we showed in the first proof we analyzed.

Let p be an odd prime and let a be an integer such that $\gcd(a,p) = 1$. We have by Euler's Criterion that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Since p is an odd prime, we know that there exists an integer b which is a primitive root modulo p; that is, there is an integer b such that $b^1, b^2, \ldots, b^{p-1}$ are each distinct modulo p. It follows that there exists a positive integer j with $0 \leq j < p$ such that $b^j \equiv a \pmod{p}$. Since b is a primitive root, we know that $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Thus, $\left(\frac{b}{p}\right) = -1$. Since the Legendre symbol is multiplicative we have that $\left(\frac{a}{p}\right) = \left(\frac{b^j}{p}\right) = \left(\frac{b}{p}\right)^j = (-1)^j$.

For convenience, we will let $\{a\}_p$ denote the least non-negative integer such that $a \equiv \{a\}_p \pmod{p}$. Let a, b, c be integers and let $p > 0$. Then we have the following results:

1. If $a \equiv b \pmod{p}$, then $\{a\}_p \equiv \{b\}_p \pmod{p}$.
2. If $p \nmid c$, then $\{-c\}_p = p - \{c\}_p$.
3. $\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor = \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p}$.
4. If $p \nmid c$ and $p \nmid a$, then $\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor + \left\lfloor \frac{a\{-c\}_p}{p} \right\rfloor = a - 1$.
5. For any function f we have the equality:

$$\sum_{n=1}^{j} f(n) + \sum_{n=1}^{k} f(j+n) = \sum_{n=1}^{k} f(n) + \sum_{n=1}^{j} f(k+n).$$

These results are given without proof in Barnard's paper, so we will provide a proof of each result.

Proof. (1) Let a, b be integers and let p be a positive integer. Suppose $a \equiv b \pmod{p}$. By the Division Algorithm, we know that $a = a_0 + pk_1$ and $b = b_0 + pk_2$ where $0 \leq a_0, b_0 < p$ and $k_1, k_2 \in \mathbb{Z}$. It follows that $a_0 + pk_1 \equiv b_0 + pk_2 \pmod{p}$. Consequently, $a_0 \equiv b_0 \pmod{p}$. Since $0 \leq a_0, b_0 < p$, we have that $a_0 = b_0$. Therefore, $\{a\}_p = \{b\}_p$.

(2) Let $p > 0$ be an integer and let c be an integer such that $p \nmid c$. It follows that $c \neq 0$. By the Division Algorithm, we have that $c = c_0 + pk_0$ and $-c = c_1 + pk_1$ where $k_0, k_1 \in \mathbb{Z}$ and $0 < c_0, c_1 < p$ since $c \neq 0$. It follows that $c_0 + c_1 = -p(k_0 + k_1)$. Since $0 < c_0, c_1 < p$, we

know that $0 < c_0 + c_1 < 2p$. Thus, $k_0 + k_1 = -1$. It follows that $c_1 = p - c_0$. Since $c_0 = \{c\}_p$ and $c_1 = \{-c\}_p$, we deduce that $\{-c\}_p = p - \{c\}$.

(3) Let a, c be integers and let p be a positive integer. By the Division Algorithm we have that $a\{c\}_p = \left\lfloor \frac{a\{c\}_p}{p} \right\rfloor p + r$, where $r \in \mathbb{Z}$ such that $0 \leq r < p$. Considering the equation modulo p yields $r \equiv a\{c\}_p \equiv ac \equiv \{ac\}_p \pmod{p}$. Since $0 \leq r < p$ and $0 \leq \{ac\}_p < p$, we deduce that $r = \{ac\}_p$. Therefore, we have that $a\{c\}_p = \left\lfloor \frac{a\{c\}_p}{p} \right\rfloor p + \{ac\}_p$. Dividing both sides by p and solving for $\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor$ yields

$$\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor = \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p}.$$

(4) Let $p > 0$ be an integer and let a, c be an integer such that $p \nmid a$ and $p \nmid c$. From (3) we know that $\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor = \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p}$ and $\left\lfloor \frac{a\{-c\}_p}{p} \right\rfloor = \frac{a\{-c\}_p}{p} - \frac{\{-ac\}_p}{p}$. Note the following:

$$\begin{aligned}
\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor + \left\lfloor \frac{a\{-c\}_p}{p} \right\rfloor &= \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p} + \frac{a\{-c\}_p}{p} - \frac{\{-ac\}_p}{p} \\
&= \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p} + \frac{a(p - \{c\}_p)}{p} - \frac{p - \{ac\}_p}{p} \\
&= \frac{a\{c\}_p}{p} - \frac{\{ac\}_p}{p} + \frac{ap}{p} - \frac{a\{c\}_p}{p} - \frac{p}{p} + \frac{\{ac\}_p}{p} \\
&= a - 1
\end{aligned}$$

Therefore, $\left\lfloor \frac{a\{c\}_p}{p} \right\rfloor + \left\lfloor \frac{a\{-c\}_p}{p} \right\rfloor = a - 1$.

(5) Let f be a function. Note that

$$\begin{aligned}
\sum_{n=1}^{j} f(n) + \sum_{n=1}^{k} f(j+n) &= f(1) + f(2) + \cdots + f(j) + f(j+1) + f(j+2) + \cdots + f(j+k) \\
&= f(1) + f(2) + \cdots + f(k) + f(k+1) + f(k+2) + \cdots + f(k+j) \\
&= \sum_{n=1}^{k} f(n) + \sum_{n=1}^{j} f(k+n).
\end{aligned}$$

Thus, $\sum_{n=1}^{j} f(n) + \sum_{n=1}^{k} f(j+n) = \sum_{n=1}^{k} f(n) + \sum_{n=1}^{j} f(k+n)$ $\square$

We will now begin to prove the Quadratic Reciprocity Theorem by first proving the following proposition.

Proposition 1. *Let p be an odd prime, a be an integer such that $p \nmid a$, and let θ denote a primitive root modulo p. If $a \equiv \theta^j \pmod{p}$ where j is an integer such that $1 \leq j < p$, then*

$$j = \frac{a-1}{p}\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \frac{2}{p}\sum_{n=1}^{j}\{\theta^n\}_p - \sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor.$$

Proof. Let p be an odd prime, a be an integer such that $p \nmid a$, and let θ denote a primitive root modulo p. Suppose $a \equiv \theta^j \pmod{p}$ where j is an integer such that $1 \leq j < p$. We first consider $\displaystyle\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor$. From (3) above, we have that

$$\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor = \sum_{n=1}^{\frac{p-1}{2}}\left(\frac{a\{\theta^n\}_p}{p} - \frac{\{a\theta^n\}_p}{p}\right).$$

Since $a \equiv \theta^j \pmod{p}$, we know theta $a\theta^n \equiv \theta^{j+n} \pmod{p}$. Thus, by (1) from above, we have that

$$\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor = \sum_{n=1}^{\frac{p-1}{2}}\left(\frac{a\{\theta^n\}_p}{p} - \frac{\{\theta^{j+n}\}_p}{p}\right) = \frac{1}{p}\left(\sum_{n=1}^{\frac{p-1}{2}} a\{\theta^n\}_p - \sum_{n=1}^{\frac{p-1}{2}}\{\theta^{j+n}\}_p\right).$$

Letting $k = \frac{p-1}{2}$ and $f(n) = \theta^n$ in (5), we obtain

$$\sum_{n=1}^{\frac{p-1}{2}}\{\theta^{j+n}\}_p = \sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p - \sum_{n=1}^{j}\{\theta^n\}_p + \sum_{n=1}^{j}\{\theta^{\frac{p-1}{2}+n}\}_p.$$

Since θ is a primitive root modulo p, we have that $\theta^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. It follows that $\theta^{\frac{p-1}{2}+n} \equiv -\theta^n \pmod{p}$. From (1) and (2) above, we obtain $\{\theta^{\frac{p-1}{2}+n}\}_p = \{-\theta^n\}_p = p - \{\theta^n\}_p$. It follows that $\displaystyle\sum_{n=1}^{j}\{\theta^{\frac{p-1}{2}+n}\}_p = pj - \sum_{n=1}^{j}\{\theta^n\}_p$. We now obtain the following equation:

$$\begin{aligned}
\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor &= \frac{1}{p}\left(\sum_{n=1}^{\frac{p-1}{2}} a\{\theta^n\}_p - \sum_{n=1}^{\frac{p-1}{2}}\{\theta^{j+n}\}_p\right)\\
&= \frac{1}{p}\left(\sum_{n=1}^{\frac{p-1}{2}} a\{\theta^n\}_p - \left(\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p - \sum_{n=1}^{j}\{\theta^n\}_p + \sum_{n=1}^{j}\{\theta^{\frac{p-1}{2}+n}\}_p\right)\right)\\
&= \frac{1}{p}\left(\sum_{n=1}^{\frac{p-1}{2}} a\{\theta^n\}_p - \left(\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p - \sum_{n=1}^{j}\{\theta^n\}_p + pj - \sum_{n=1}^{j}\{\theta^n\}_p\right)\right)\\
&= \frac{1}{p}\left((a-1)\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + 2\sum_{n=1}^{j}\{\theta^n\}_p - pj\right)\\
&= \frac{a-1}{p}\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \frac{2}{p}\sum_{n=1}^{j}\{\theta^n\}_p - j.
\end{aligned}$$

Therefore, $j = \dfrac{a-1}{p}\displaystyle\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \dfrac{2}{p}\sum_{n=1}^{j}\{\theta^n\}_p - \sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \dfrac{a\{\theta^n\}_p}{p}\right\rfloor.$ □

Proposition 2. *Let p be an odd prime, a be an odd integer with $p \nmid a$ and θ be a primitive root modulo p. Also let $j \in \{1, 2, \ldots, p-1\}$ such that $a \equiv \theta^j \pmod{p}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor}.$$

Proof. Let p be an odd prime, a be an odd integer with $p \nmid a$ and θ be a primitive root modulo p. Let $j \in \{1, 2, \ldots, p-1\}$ be such that $a \equiv \theta^j \pmod{p}$. Since a is odd, let $a - 1 = 2w$ for some integer w. It follows from Proposition 1 that

$$j = \frac{2w}{p}\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \frac{2}{p}\sum_{n=1}^{j}\{\theta^n\}_p - \sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor = \frac{2}{p}\left(w\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \sum_{n=1}^{j}\{\theta^n\}_p\right) - \sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor. \quad (3)$$

Let $x = w\sum_{n=1}^{\frac{p-1}{2}}\{\theta^n\}_p + \sum_{n=1}^{j}\{\theta^n\}_p$. Since $j \in \mathbb{Z}$ and $\displaystyle\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor \in \mathbb{Z}$, we deduce that $\dfrac{2x}{p} \in \mathbb{Z}$. Since p is odd and $p \nmid 2$, we have that $p \mid x$. Therefore, $\dfrac{2x}{p}$ is an even integer. Considering equation (3) modulo 2 yields the following:

$$j \equiv -\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor \equiv \sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor \pmod{2}.$$

Therefore,

$$\left(\frac{a}{p}\right) = (-1)^j = (-1)^{\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{a\{\theta^n\}_p}{p}\right\rfloor}.$$

□

The following proposition is a version of Gauss' Lemma.

Proposition 3 *Let p be an odd prime, a be an odd integer with $p \nmid a$ and θ be a primitive root modulo p. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}}\left\lfloor \frac{an}{p}\right\rfloor}.$$

Proof. Let p be an odd prime, a be an odd integer with $p \nmid a$ and θ be a primitive root modulo p. Since θ is a primitive root modulo p, we know that $p \nmid \theta$. Therefore, by (4)

we obtain $\left\lfloor \frac{a\{\theta^n\}_p}{p} \right\rfloor + \left\lfloor \frac{a\{-\theta^n\}_p}{p} \right\rfloor = a - 1$. Since a is odd, we know that $a - 1$ is even. Therefore, we have that $\left\lfloor \frac{a\{\theta^n\}_p}{p} \right\rfloor \equiv \left\lfloor \frac{a\{-\theta^n\}_p}{p} \right\rfloor \pmod 2$. It follows that

$$\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{a\{\theta^n\}_p}{p} \right\rfloor \equiv \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{a}{p} \min(\{\theta^n\}_p, \{-\theta^n\}_p) \right\rfloor \pmod 2.$$

From (2) we have that $\{-\theta\}_p = p - \{\theta\}_p$. Therefore, we deduce $1 \leq \min(\{\theta^n\}_p, \{-\theta^n\}_p) \leq \frac{p-1}{2}$. Since θ is a primitive root modulo p, we know that the sets

$$\left\{ \{\theta^1\}_p, \{\theta^2\}_p, \ldots, \{\theta^{\frac{p-1}{2}}\}_p \right\} \text{ and } \left\{ \{\theta^{\frac{p+1}{2}}\}_p, \{\theta^{\frac{p+3}{2}}\}_p, \ldots, \{\theta^{p-1}\}_p \right\}$$

are disjoint. By (1) from above and since $-\theta^n \equiv \theta^{\frac{p-1}{2}+n} \pmod p$, we know that

$$\left\{ \{-\theta^1\}_p, \{-\theta^2\}_p, \ldots, \{-\theta^{\frac{p-1}{2}}\}_p \right\} = \left\{ \{\theta^{\frac{p+1}{2}}\}_p, \{\theta^{\frac{p+3}{2}}\}_p, \ldots, \{\theta^{p-1}\}_p \right\}.$$

Since $1 \leq \min(\{\theta^n\}_p, \{-\theta^n\}_p) \leq \frac{p-1}{2}$, we deduce that $\left\{\min(\{\theta^n\}_p, \{-\theta^n\}_p)\right\}_{n=1}^{\frac{p-1}{2}}$ contains $\frac{p-1}{2}$ distinct integers that range in value between 1 and $\frac{p-1}{2}$. Therefore,

$$\left\{\min(\{\theta^n\}_p, \{-\theta^n\}_p)\right\}_{n=1}^{\frac{p-1}{2}} = \{1, 2, \ldots, \frac{p-1}{2}\}.$$

It follows that $\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{a}{p} \min(\{\theta^n\}_p, \{-\theta^n\}_p) \right\rfloor = \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p} \right\rfloor$. Therefore, by Proposition 2, we deduce

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{a\{\theta^n\}_p}{p} \right\rfloor} = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p} \right\rfloor}.$$

□

From here, Barnard uses the same argument as is used in the first proof we analyzed where we considered lattice points to complete the proof of the Quadratic Reciprocity Law.

5 Conclusion

The Quadratic Reciprocity Law continues to be a valuable theorem in number theory today. As has been shown previously, the theorem is useful in determining whether an integer a is quadratic residue modulo p where p is an odd prime and $p \nmid a$. The Quadratic Reciprocity Law has been implemented in several modern applications. The theorem is extremely useful in the Goldwasser-Micali public key cryptosystem, because the key chosen for this cryptosystem must be a quadratic nonresidue modulo p and q where p, q are very large distinct primes. The Quadratic Reciprocity Law has also been applied in several primality

tests, such as Euler's test.

The three proofs we have analyzed demonstrate the wide variety of techniques that have been implemented over the past 300 years to prove the Quadratic Reciprocity Law. There have been proofs published in many branch of mathematics. Gauss states that the reason he provided multiple proofs was to be able to prove the reciprocity law in general for powers higher than quadratic, for example, the cubic, quartic, and octic reciprocity laws. Gauss was successful in finding such a generalization in his sixth published proof of the theorem.

After 300 years, why are mathematicians still attempting to provide new proofs of this important theorem today? Mathematician Yuri Manin provides an answer to this question in [9] by saying

> "... one proof is sufficiently convincing. The point is, that proving is the way we are discovering new territories, new features of the mathematical landscape."

Mathematicians also continue to provide proofs of this theorem because many believe it is one of the most beautiful theorems in number theory. David Burton says about the Quadratic Reciprocity Law in [3] on page 169,

> "For those who consider the theory of number 'The Queen of Mathematics,' this (QRL) is one of the jewels in her crown."

References

[1] Barnard, Virgil, "A Proof of Quadratic Reciprocity." *The American Mathematical Monthly* 122.6 (2015): 588-592. Web.

[2] Baumgart, Oswald, *The Quadratic Reciprocity Law: A Collection of Classical Proofs,* Springer International Publishing, [c2015].

[3] Burton, David M., *Elementary Number Theory* 6th ed. New York, NY: McGraw-Hill, 2007.

[4] Gauss, C. F., *Disquisitiones Arithmeticae* (trans A. A. Clarke), Yale University Press, New Haven, 1966.

[5] Kim, Sey Y., "An Elementary Proof of the Quadratic Reciprocity Law." *The American Mathematical Monthly* 111.1 (2004): 48-50. Web.

[6] Koshy, Thomas, *Elementary Number Theory with Applications* 2nd ed. Academic Press, 2007.

[7] Legendre, A.M., *Essai sur la théorie des nombres*, Dprat, Paris (1798); cf. p.

[8] Lemmermeyer, F., *Reciprocity Laws,* Springer-Verlag, Berlin Heidelberg [c2000].

[9] Manin, Y. I., *Good proofs are proofs that make us wiser*, DMV-Mitteilungen 2 (1998), 40-44.

[10] Rosen, Kenneth H., *Elementary Number Theory and its Applications* 3rd ed. Murray Hill, NJ: AT&T Bell Laboratories, 1993.