GROUP THEORY AND THE LAW OF QUADRATIC RECIPROCITY

CHAOFAN CHEN

Abstract. This paper explores the role of group theory in providing a proof for the Law of Quadratic Reciprocity, which states that for distinct odd primes $p$and q, q is a quadratic residue mod p if and only if p is a quadratic residue mod q, unless p and q are both congruent to 3 mod 4. The Law of Quadratic Reciprocity is an important result in number theory; it provides us with a simple method to determine whether a number is a quadratic residue modulo an odd prime number.

Contents

1. Fundamentals of Group Theory

In this Section, we will state the definitions of some basic concepts in group theory.

Definition 1.1. Let G be a set, together with a binary operation $*$, satisfying the following axioms:

(a) for all a, b in G, $a * b$ is in G (closure);

(b) for all a, b, and c in G, $(a * b) * c = a * (b * c)$ (associativity);

(c) there is an identity element e in G such that for all a in G, $a * e = e * a = a$ (identity);

(d) for each a in G, there is an element b in G such that $a * b = b * a = e$, where e is the identity element in G (inverses).

Then we say that the set G forms a group under the binary operation $*$.

Definition 1.2. Let G be a group. A non-empty subset H of G is a subgroup if H is a group under the same operation as G.

Definition 1.3. We say that a group G is abelian if its elements commute, i.e. $g * h = h * g$ for all g, h in G.

Date: July 29, 2010.

Definition 1.4. The order of a group G, denoted by $|G|$, is the number of elements in G.

Definition 1.5. Let g be an element of the group G with the binary operation $*$. The order of the element g is the least positive integer i such that $g^i = e$, where g^i denotes the product $g * g * ... * g$ with i factors and e is the identity element in G.

Definition 1.6. A group G is cyclic if there exists an element c in G such that every element g in G has the form $g = c^i$ for some integer i. The element c is also called a generator for G.

Theorem 1.7. *The order of a generator for a finite cyclic group is equal to the order of the group. Conversely, if the order of an element is equal to the order of the group, that element must be a generator for the group.*

Proof. Let G be a finite cyclic group with the binary operation $*$, and c be the generator for G.
Let i be the order of c. By definition, we have $c^i = e$, where e is the identity element in G.
By division algorithm, each $j \in \mathbb{Z}$ can be written $j = qi + r$ for some unique pair of integers q and r where $0 < r \leq i$.
Thus, for each $j \in \mathbb{Z}$, we have $c^j = c^{qi+r} = c^{qi} * c^r = (c^i)^q * c^r = c^r$ for some unique integer r with $0 < r \leq i$.
This means that the value of c^j must come from the list $c, c^2, ..., c^i$.
Now, we will show that the above list contains i distinct elements.
Suppose that $c^m = c^n$ for some integers m, n with $0 < n \leq m \leq i$, so $0 \leq m-n < i$.
We have $c^{m-n} = e * c^{m-n} = c^{-n} * c^n * c^{m-n} = c^{-n} * (c^n * c^{m-n}) = c^{-n} * c^m = c^{-n} * c^n = e$.
If $m \neq n$, then $m-n$ would be a positive integer less than i and satisfying $c^{m-n} = e$, contradicting that i is the order of c.
Hence, we have $m = n$, which means that the list $c, c^2, ..., c^i$ contains i distinct values.
Now, since c is the generator for G, every element of G can be written c^j for some integer j. This means that every element of G can be found in the set $C = \{c, c^2, ..., c^i\}$, i.e. $G \subseteq C$.
At the same time, since G is a group, any product $c^j = c * c * ... * c$ with j factors must be in G, so $C \subseteq G$.
Thus, $G = C$, which means that $|G| = |C| = i$.
Conversely, suppose that c is any element in G such that the order of c (call it i) is equal to $|G|$. By the same argument, the list $c, c^2, ..., c^i$ contains i distinct values.
Let $C = \{c, c^2, ..., c^i\}$. Then $C \subseteq G$ because G is a group, and any product $c^j = c * c * ... * c$ with j factors must be in G.
Now, $|C| = i = |G|$ implies that $C = G$, so every element of G can be written as some power of c. □

2. The Group of Units

Now, we will apply the group theory to the study of units in $\mathbb{Z}_n$. The goal of this Section is to prove that the set of units in $\mathbb{Z}_p$ for some prime number p forms a cyclic group under multiplication mod p.

Before we proceed any further, we will first introduce the idea of congruence

classes, the number system $\mathbb{Z}_n$, and the operations defined in $\mathbb{Z}_n$.

For some fixed integer n, the division algorithm allows us to express each integer a as $a = qn+r$ for some unique pair of integers q and r with $0 \leq r < n$. The number r is known as the remainder of a when divided by n. Replacing each integer with its remainder when divided by n partitions the set $\mathbb{Z}$ into n congruence classes, namely $[0], [1], ..., [n-1]$, where $[a] = \{b \in \mathbb{Z} : b \equiv a \ mod \ n\}$ (we say that b is congruent to a modulo n and denote by $b \equiv a \ mod \ n$ if b and a leave the same remainder when divided by n), thereby forming a number system $\mathbb{Z}_n$ with the above n congruence classes as its elements. If $[a]$ and $[b]$ are elements of $\mathbb{Z}_n$, we can define their sum and product as

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

It is easy to show that the above operations are well-defined, and $[0]$ is the additive identity and $[1]$ is the multiplicative identity in $\mathbb{Z}_n$.

Definition 2.1. A congruence class $[a] \in \mathbb{Z}_n$ is a unit if it has a multiplicative inverse in $\mathbb{Z}_n$, that is, if there exists a class $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$.

The following lemma allows us to determine whether an integer is a unit mod n easily:

Lemma 2.2. *$[a]$ is a unit in $\mathbb{Z}_n$ if and only if a and n are coprime.*

Proof. If $[a]$ is a unit, then there exist some integers b and q such that $ab = 1 + qn$. This implies that any common divisor of a and n must divide 1, so $gcd(a, n) \mid 1$. Since the only integer which divides 1 is 1, we have $gcd(a, n) = 1$.
On the other hand, if a and n are coprime, i.e. $gcd(a, n) = 1$, by Bezout's identity, there exist some integers u and v such that $1 = gcd(a, n) = au + nv$, so $au \equiv 1$ mod n. This means that $[u]$ is the multiplicative inverse of $[a]$ in $\mathbb{Z}_n$. □

Let U_n denote the set of units in $\mathbb{Z}_n$. The following corollary is a direct consequence of the above lemma:

Corollary 2.3. $U_p = \{[1], [2], ..., [p-1]\} = \mathbb{Z}_p \setminus \{[0]\}$.

Proof. We know that the congruence classes in $\mathbb{Z}_p$ are [0], [1], [2], ..., $[p-1]$.
Since for all integers c with $1 \leq c \leq p-1$, c and p are coprime, it follows from Lemma 2.2 that [1], [2], ..., $[p-1]$ are units in $\mathbb{Z}_p$. ([0] is not a unit in $\mathbb{Z}_p$ because $gcd(0, p) = p \neq 1$.)
Thus, $U_p = \{[1], [2], ..., [p-1]\} = \mathbb{Z}_p \setminus \{[0]\}$. □

We will now show that the set U_n forms an abelian group under multiplication mod n.

Theorem 2.4. *For each positive integer n, the set U_n forms an abelian group under multiplication mod n, with identity element $[1]$.*

Proof. To prove commutativity, simply note that $[a][b] = [ab] = [ba] = [b][a]$ for all units $[a]$ and $[b]$.
Now, we will show that the set U_n satisfies the group axioms listed in Definition 1.1.
To prove closure, we need to show that if $[a]$ and $[b]$ are units, then $[a][b] = [ab]$ is also a unit.

If $[a]$ and $[b]$ are units, then there exist $[u]$ and $[v]$ such that $[a][u] = [au] = [1]$ and $[b][v] = [bv] = [1]$.
Thus, we have $[ab][uv] = [abuv] = [(au)(bv)] = [au][bv] = [1][1] = [1]$. This means that $[ab]$ has inverse $[uv]$, so $[ab]$ is a unit.
To prove associativity, we need to show that $([a][b])[c] = [a]([b][c])$ for all units $[a]$, $[b]$ and $[c]$.
It is clear that $([a][b])[c] = [ab][c] = [(ab)c)] = [a(bc)] = [a][bc] = [a]([b][c])$.
There exists the identity element $[1]$ in U_n, because $[1][a] = [a] = [a][1]$ for all $[a] \in U_n$.
If $[a]$ is a unit, then by definition there exists $[u] \in \mathbb{Z}_n$ such that $[a][u] = [1]$.
Now, $[u]$ is also a unit, because $[u][a] = [a][u] = [1]$. This means that $[u]$ is the inverse of $[a]$ in U_n.
Thus, U_n is an abelian group. □

The order of the group U_n is given by the Euler's function.

Definition 2.5. The Euler's function, $\phi : \mathbb{N} \to \mathbb{N}$, is defined as $\phi(n) = |U_n|$.

The value of $\phi(n)$ is given by the equation below, which we will not prove here:

$$\phi(n) = \prod_{i=1}^{k}({p_i}^{e_i} - {p_i}^{e_i-1}) = \prod_{i=1}^{k} {p_i}^{e_i-1}(p_i - 1) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}) \tag{2.6}$$

if n has prime-power factorization $n = {p_1}^{e_1}...{p_k}^{e_k}$.

Theorem 2.7. *If $n \geq 1$ then $\sum_{d|n} \phi(d) = n$.*

Proof. Let $S = \{1, 2, ..., n\}$, and for each d dividing n let $S_d = \{a \in S : gcd(a, n) = n/d\}$.
These sets S_d partitions the set S into disjoint subsets, because:
(i) For all $a \in S$, there exists some d dividing n such that $a \in S_d$:
If a shares some prime factors $p_1, ..., p_k$ with n, then $gcd(a, n) = p_1^{i_1}...p_k^{i_k}$ where $i_1, ...i_k$ are the smaller powers of $p_1, ..., p_k$ in the prime factorizations of a and n.
It is clear that $gcd(a, n) = p_1^{i_1}...p_k^{i_k}$ divides n, i.e. there exists some positive integer d dividing n such that $gcd(a, n) = n/d$, so a is in S_d for such d.
If a shares no prime factors with n , then $gcd(a, n) = 1 = n/n$, so a is in S_n.
(ii) No single $a \in S$ can be found in two distinct S_d because for each $a \in S$, $gcd(a, n)$ is unique.
Therefore, $\sum_{d|n} |S_d| = |S| = n$, so it is sufficient to show that $|S_d| = \phi(d)$ for each d.
Now, we know that

$$a \in S_d \text{ if and only if } a \in \mathbb{Z},\ 1 \leq a \leq n, \text{ and } gcd(a, n) = n/d. \ (*)$$

If we define $a' = a/(n/d)$ for each $a \in S_d$, then a' is an integer because $n/d = gcd(a, n)$ divides a, and the statement $(*)$ is equivalent to:
$a \in S_d$ if and only if $a = (n/d) \cdot a'$, where $a' \in \mathbb{Z}$, $1 \leq a' \leq d$ and $gcd(a', d) = 1$.
Thus, $|S_d|$ is the number of integers a' such that a' is between 1 and d inclusive, and a' is coprime to d.
It follows from Lemma 2.2 that $|S_d|$ is the number of units in $\mathbb{Z}_d$, which, by definition, is equal to $\phi(d)$. □

Both the theorem above and a corollary of Lagrange's Theorem are useful in proving that the group U_p for some prime number p is cyclic, a result which follows from the next theorem:

Theorem 2.8. *If p is prime, then the group U_p has $\phi(d)$ elements of order d for each d dividing $p-1$.*

Proof. For each d dividing $p-1$, let $\Omega_d = \{a \in U_p : a \text{ has order } d\}$ and $\omega(d) = |\Omega_d|$. We need to show that $\omega(d) = \phi(d)$ for all such d.
A corollary of Lagrange's Theorem states that the order of any element of a finite group divides the order of the group, so the order of each element of U_p divides $|U_p| = |\mathbb{Z}_p \setminus \{[0]\}| = p-1$.
Thus, the sets Ω_d form a partition of U_p, and

$$\sum_{d|p-1} \omega(d) = |U_p| = p-1.$$

By Theorem 2.7, we have

$$\sum_{d|p-1} \phi(d) = p-1,$$

so

$$\sum_{d|p-1} (\phi(d) - \omega(d)) = 0.$$

Now we are going to show that for each d dividing $p-1$, $\omega(d) \leq \phi(d)$.
The inequality $\omega(d) \leq \phi(d)$ is obvious if Ω_d is empty, so we may assume that Ω_d contains an element a.
It is clear that the powers $a^i = a, a^2, ..., a^d(= 1)$ are all distinct, and they satisfy $(a^i)^d = 1$ so they are the d distinct roots of the polynomial $f(x) = x^d - 1$ in $\mathbb{Z}_p$.
Since $f(x)$ has at most d distinct roots in $\mathbb{Z}_p$, the powers $a^i = a, a^2, ..., a^d(= 1)$ form a complete set of roots of $f(x)$.
We will now show that any element b of Ω_d can be written $b = a^i$ where i is an integer such that $1 \leq i \leq d$ and $gcd(i, d) = 1$.
If $b \in \Omega_d$, then b is a root of $f(x)$, so $b = a^i$ where i is an integer such that $1 \leq i \leq d$.
Let $j = gcd(i, d)$. Then $b^{d/j} = a^{id/j} = (a^d)^{i/j} = 1^{i/j} = 1$ in U_p.
Since d is the order of b, no lower power of b than b^d can be equal to 1, so $j = 1$.
Thus, every element b of Ω_d has the form a^i where i is an integer such that $1 \leq i \leq d$ and i is coprime to d.
The number of such integer i is $\phi(d)$, so the number of elements b in Ω_d, which is equal to $\omega(d)$, is at most $\phi(d)$, i.e. $\omega(d) \leq \phi(d)$ for each d dividing $p-1$.
This means that $\phi(d) - \omega(d) \geq 0$ for each d dividing $p-1$.
Thus, $\sum_{d|p-1} (\phi(d) - \omega(d)) = 0$ implies that $\phi(d) - \omega(d) = 0$ for each d dividing $p-1$, so $\omega(d) = \phi(d)$, and the proof is complete. □

Corollary 2.9. *If p is prime then the group U_p is cyclic.*

Proof. By Theorem 2.8, the group U_p has $\phi(p-1)$ elements of order $p-1$. Since $\phi(p-1) \geq 1$, the group U_p has at least one element (call it a) of order $p-1$. Now, $p-1 = |U_p|$, so the order of a is equal to the order of the group U_p. By Theorem 1.7, a is a generator for the group U_p, i.e. the group U_p is cyclic. □

If U_n is cyclic, any generator g for U_n is called a primitive root mod n.

3. The Group of Quadratic Residues and the Legendre Symbol

In this Section, we will discuss the group of quadratic residues and the Legendre symbol.

Definition 3.1. An element $a \in U_n$ is a quadratic residue mod n if $a = s^2$ for some $s \in U_n$. The set of such quadratic residues is denoted by Q_n.

For small n, we can find Q_n by squaring all the elements of U_n. For example, in $U_7 = \{1, 2, 3, 4, 5, 6\}$, we have $1^2 = 1, 2^2 = 4, 3^2 = 2, 4^2 = 2, 5^2 = 4, 6^2 = 1$; thus, 1, 2 and 4 are quadratic residues mod 7 and $Q_7 = \{1, 2, 4\} \subset U_7$.

Lemma 3.2. *Q_n is a subgroup of U_n.*

Proof. We need to show that Q_n contains the identity element of U_n, and is closed under taking products and inverses.
Firstly, $1 \in Q_n$ because $1 = 1^2$ with $1 \in U_n$.
If a, $b \in Q_n$, then $a = s^2$ and $b = t^2$ for some s, $t \in U_n$, so $ab = s^2t^2 = (st)^2$ with $st \in U_n$, i.e. $ab \in Q_n$.
Finally, if $a \in Q_n$, then $a = s^2$ for some $s \in U_n$. Since s is a unit mod n, it has inverse s^{-1} in U_n. Now, $a(s^{-1})^2 = s^2(s^{-1})^2 = (ss^{-1})^2 = 1^2 = 1$, i.e. a has inverse $a^{-1} = (s^{-1})^2$ with $s^{-1} \in U_n$, so $a^{-1} \in Q_n$. □

When U_n is cyclic, the following lemma describes Q_n:

Lemma 3.3. *Let $n > 2$, and suppose that there is a primitive root g mod n. Then Q_n is a cyclic group of order $\phi(n)/2$, generated by g^2, consisting of the even powers of g.*

Proof. We will first show that when $n > 2$, $\phi(n)$ is even. There are two cases:
(i) If n has some odd prime factor p, then $p-1$ is even. Hence, Equation 2.6 implies that $\phi(n)$ is even.
(ii) If n has no odd prime factors, we have $n = 2^m$ for some integer m; since $n > 2$, we have $m > 1$, i.e.$m - 1 > 0$. By Equation 2.6, $\phi(n) = 2^{m-1}(2-1) = 2^{m-1}$ must be even.
Now, any element $a \in U_n$ can be written $a = g^i$ for some integer i, and $U_n = \{g, g^2, ..., g^{\phi(n)}\}$, with $g^{\phi(n)} = 1$.
If i is even, then $a = g^i = (g^{i/2})^2 \in Q_n$.
If $a \in Q_n$, then $a = (g^j)^2 = g^{2j}$ for some j, so $i \equiv 2j \bmod \phi(n)$; since $\phi(n)$ is even, i must be even.
Hence, Q_n consists of even powers of g. This means that $Q_n = \{g^2, g^4, ..., g^{\phi(n)}\} = \{g^2, (g^2)^2, ..., (g^2)^{\phi(n)/2}\}$, with $|Q_n| = \phi(n)/2$. □

We will now introduce the Legendre symbol, a useful notation whose value denotes whether an integer is a quadratic residue mod p.

Definition 3.4. For an odd prime p, the Legendre symbol of any integer a is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \in Q_p \\ -1 & \text{if } a \in U_p \setminus Q_p \end{cases}$$

The Legendre symbol depends only on the congruence class of a mod p, and is clearly well-defined on $\mathbb{Z}$ or $\mathbb{Z}_p$.

We have proven that the group U_p is cyclic for any prime number p (See Corollary

2.9), and this guarantees the existence of a primitive root g mod p. The following corollary is a direct consequence of Lemma 3.3:

Corollary 3.5. *If p is an odd prime number, and g is a primitive root mod p, then $\left(\frac{g^i}{p}\right) = (-1)^i$.*

Proof. By Lemma 3.3, when i is even, g^i is in Q_p, so $\left(\frac{g^i}{p}\right) = 1 = (-1)^i$. When i is odd, g^i is in $U_p \backslash Q_p$, so $\left(\frac{g^i}{p}\right) = -1 = (-1)^i$. □

The following theorem is very useful for calculations involving the Legendre symbol:

Theorem 3.6. *If p is an odd prime, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all integers a and b.*

Proof. If p divides a or b, then $\left(\frac{a}{p}\right) = 0$ or $\left(\frac{b}{p}\right) = 0$, so $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$; at the same time, p divides ab, so $\left(\frac{ab}{p}\right) = 0$.
If p divides neither a nor b, then $a, b \in U_p$. Let g be a primitive root mod p. Then $a = g^i$ and $b = g^j$ for some integers i and j, so $ab = g^i g^j = g^{i+j}$. By Corollary 3.5, we have

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{i+j}}{p}\right) = (-1)^{i+j} = (-1)^i(-1)^j = \left(\frac{g^i}{p}\right)\left(\frac{g^j}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

4. Euler's Criterion and Gauss's Lemma

In this Section, we will introduce two more effective methods for determining quadratic residues. The first is known as Euler's Criterion:

Theorem 4.1. *(Euler's Criterion) If p is an odd prime, then for all integers a we have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.*

Proof. If p divides a, then $\left(\frac{a}{p}\right) = 0$; at the same time, p divides $a^{(p-1)/2}$, so $0 \equiv a^{(p-1)/2} \mod p$, i.e. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.
If p does not divide a, then $a \in U_p$. Let g be a primitive root mod p. It is clear that the order of g is equal to $|U_p| = p - 1$.
Now, $a = g^i$ for some integer i. Define $h = g^{(p-1)/2}$. Then $h^2 = g^{p-1} = 1$ in U_p, so $h^2 \equiv 1 \mod p$. This means that p divides $h^2 - 1 = (h+1)(h-1)$, so p divides $h+1$ or $h-1$. Thus, $h = \pm 1$ in U_p.
Since g has order $p - 1 > (p-1)/2$, so $h = g^{(p-1)/2} \neq 1$. Hence, we have $h = -1$.
By Corollary 3.5, we have

$$a^{(p-1)/2} = (g^i)^{(p-1)/2} = (g^{(p-1)/2})^i = h^i = (-1)^i = \left(\frac{g^i}{p}\right) = \left(\frac{a}{p}\right)$$

in $\mathbb{Z}_p$, and the proof is complete. □

Before stating the next result, let us use the set $\{\pm 1, \pm 2, ..., \pm(p-1)/2\}$ as a reduced set of residues mod p (a set of integers such that each integer is coprime to p, i.e. is a unit mod p, and no two are congruent mod p). Then we can partition

U_p into two subsets $P = \{1, 2, ..., (p-1)/2\}$ and $N = \{-1, -2, ..., -(p-1)/2\}$. For each $a \in U_p$, we define $aP = \{ax : x \in P\}$.

Theorem 4.2. *(Gauss's Lemma) If p is an odd prime and $a \in U_p$, then $\left(\frac{a}{p}\right) = (-1)^\mu$ where $\mu = |aP \cap N|$.*

Proof. If x and y are distinct elements of P, then $ax \neq \pm ay$ in U_p, because if $ax \equiv \pm ay \bmod p$, then p divides $ax \mp ay = a(x \mp y)$, so p divides $x \mp y$, i.e. $x \equiv \pm y \bmod p$, which is impossible because x and y are distinct elements of $P = \{1, 2, ..., (p-1)/2\}$.
Now, it is impossible for both k and $-k$ (k is any integer between 1 and $(p-1)/2$ inclusive) to be in aP at the same time; otherwise, there would exist distinct x, $y \in P$ such that $ax = k$ and $ay = -k$ in U_p, so $ax = -ay$ in U_p (contradiction).
Thus, the elements of aP lie in distinct sets $\{\pm 1\}$, $\{\pm 2\}$, ..., $\{\pm(p-1)/2\}$ (each set contains at most one element of aP). There are $(p-1)/2$ such sets, and there are $(p-1)/2$ elements of aP, so each set contains exactly one element of aP. Hence, we have

$$aP = \{\varepsilon_i i : i = 1, 2, ..., (p-1)/2\}$$

where each $\varepsilon_i = \pm 1$. It is clear that $\varepsilon_i = 1$ if and only if $\varepsilon_i i \in P$, and $\varepsilon_i = -1$ if and only if $\varepsilon_i i \in N$.
Since aP is contained in the abelian group U_p, we can multiply all its elements together in any order, and obtain the same result, so

$$a^{(p-1)/2}((p-1)/2)! = \left(\prod_{i=1}^{(p-1)/2} \varepsilon_i\right)((p-1)/2)! = (-1)^\mu((p-1)/2)!$$

in U_p, where μ is the number of i such that $\varepsilon_i = -1$, which is the number of $\varepsilon_i i$ such that $\varepsilon_i i \in N$. This means $\mu = |aP \cap N|$.
Hence, we have $a^{(p-1)/2} = (-1)^\mu$ in U_p, so $a^{(p-1)/2} \equiv (-1)^\mu \bmod p$.
Now, Euler's Criterion (Theorem 4.1) gives $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.
Thus, we have $\left(\frac{a}{p}\right) \equiv (-1)^\mu \bmod p$.
Both sides of this congruence are equal to ± 1, so they must be equal to each other since $p > 2$. □

The following corollary of Gauss's Lemma allows us to decide whether 2 is a quadratic residue modulo any odd prime number:

Corollary 4.3. *If p is an odd prime then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Thus, 2 is a quadratic residue mod p if and only if $p \equiv \pm 1$ mod 8.

Proof. Let $P = \{1, 2, ..., (p-1)/2\} \subset U_p$ and $N = (-1)P$ as before.
Then we have $2P = \{2, 4, ..., p-1\}$.
Suppose first that $p \equiv 1 \bmod 4$. Then we have $2P = \{2, 4, ..., (p-1)/2, (p+3)/2, ..., p-1\}$. It is clear that the first $(p-1)/4$ elements $2, 4, ..., (p-1)/2$ are in P, while the remaining $(p-1)/4$ elements $(p+3)/2, ..., p-1$ are in N. Thus, Gauss's Lemma gives

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = ((-1)^{(p+1)/2})^{(p-1)/4} = (-1)^{(p^2-1)/8},$$

where we have used the fact that $(p+1)/2$ is odd.
Now suppose that $p \equiv -1 \bmod 4$. Then we have $2P = \{2, 4, ..., (p-3)/2, (p+1)/2, ..., p-1\}$. It is clear that the first $(p-3)/4$ elements $2, 4, ..., (p-3)/2$ are in P, while the remaining $(p+1)/4$ elements $(p+1)/2, ..., p-1$ are in N. Thus, Gauss's Lemma gives

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = ((-1)^{(p-1)/2})^{(p+1)/4} = (-1)^{(p^2-1)/8},$$

where we have used the fact that $(p-1)/2$ is odd.
This proves $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Now, 2 is a quadratic residue mod p if and only if $\left(\frac{2}{p}\right) = 1$, i.e. $(p^2-1)/8$ is even; $(p^2-1)/8$ is even if and only if 16 divides $p^2 - 1 = (p+1)(p-1)$; 16 divides $p^2 - 1 = (p+1)(p-1)$ if and only if 8 divides $p+1$ or $p-1$, i.e. $p \equiv \pm 1 \bmod 8$. □

5. The Law of Quadratic Reciprocity

We are now ready to prove an important theorem in number theory, the Law of Quadratic Reciprocity, which states that for distinct odd primes p and q, q is a quadratic residue mod p if and only if p is a quadratic residue mod q, unless p and q are both congruent to 3 mod 4. This theorem can be elegantly expressed using the Legendre symbol:

Theorem 5.1. *(The Law of Quadratic Reciprocity) If p and q are distinct odd primes, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, except when $p \equiv q \equiv 3$ mod 4, in which case $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.*

Proof. First, we will show that $p \equiv q \equiv 3 \bmod 4$ if and only if $(p-1)(q-1)/4$ is odd.
When $p \equiv q \equiv 3 \bmod 4$, we have $p = 4k+3$ and $q = 4t+3$ for some integers k and t. Then $(p-1)(q-1)/4 = (4k+2)(4t+2)/4 = 4kt + 2k + 2t + 1$ is odd.
When $(p-1)(q-1)/4$ is odd, $(p-1)/2$ and $(q-1)/2$ must both be odd, so $(p-1)/2 = 2k+1$ and $(q-1)/2 = 2t+1$ for some integers k and t. Solving the two equations for p and q, we have $p = 4k+3$ and $q = 4t+3$, i.e. $p \equiv q \equiv 3 \bmod 4$.
It is clear that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ is equivalent to $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = 1$, and $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ is equivalent to $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = -1$.
Hence, we can rewrite the above theorem in the following way:
If p and q are distinct odd primes, then $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.
Now, let $P = \{1, 2, ..., (p-1)/2\} \subset U_p$ and $N = (-1)P$ as before, and similarly define $Q = \{1, 2, ..., (q-1)/2\} \subset U_q$. By Gauss's Lemma (Theorem 4.2), we have

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

where $\mu = |qP \cap N|$ is the number of elements $x \in P$ such that $qx \equiv n \bmod p$ for some $n \in N$; this congruence is equivalent to $qx - py \in N$ for some integer y, i.e.

$$-\frac{p}{2} < qx - py < 0$$

for some integer y. Given any $x \in P$, the values of $qx - py$ for $y \in \mathbb{Z}$ differ by multiples of p, so $-p/2 < qx - py < 0$ for at most one integer y. If such a y exists, then

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Since $x \leq (p-1)/2$, we have

$$y < \frac{qx}{p} + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}.$$

Thus, y is an integer strictly between 0 and $(q+1)/2$, i.e. $y \in \{1, 2, ..., (q-1)/2\} = Q$. Hence, we have shown that μ is the number of pairs $(x, y) \in P \times Q$ such that

$$-\frac{p}{2} < qx - py < 0.$$

Similarly, we also have

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

where ν is the number of pairs $(y, x) \in Q \times P$ such that

$$-\frac{q}{2} < py - qx < 0,$$

i.e. ν is the number of pairs $(x, y) \in P \times Q$ such that

$$0 < qx - py < \frac{q}{2}.$$

It follows that

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\mu+\nu},$$

where $\mu + \nu$ is the number of pairs $(x, y) \in P \times Q$ such that

$$-\frac{p}{2} < qx - py < 0 \ \ or \ \ 0 < qx - py < \frac{q}{2}.$$

There are no pair $(x, y) \in P \times Q$ satisfying $qx - py = 0$, since p and q are coprime, so the above condition can be simplified as

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Now, let

$$R = P \times Q = \{(x, y) : x \in P, y \in Q\} = \left\{(x, y) : x, y \in \mathbb{Z}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\right\},$$

$$S = \left\{(x, y) : x, y \in \mathbb{Z}, -\frac{p}{2} < qx - py < \frac{q}{2}\right\}$$

$$A = \left\{(x, y) : x, y \in \mathbb{Z}, qx - py < -\frac{p}{2}\right\},$$

and

$$B = \left\{(x, y) : x, y \in \mathbb{Z}, qx - py > \frac{q}{2}\right\}.$$

Thus, we have $\mu + \nu = |R \cap S|$. Now, it is clear that $|R| = |P \times Q| = |P|\,|Q| = (p-1)(q-1)/4$, so

$$\mu + \nu = \frac{(p-1)(q-1)}{4} - (\alpha + \beta)$$

where $\alpha = |R \cap A|$ and $\beta = |R \cap B|$. If we can show that $\alpha = \beta$, then $\mu + \nu \equiv (p-1)(q-1)/4 \bmod 2$, and hence

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

as required.
We will prove that $\alpha = \beta$ by introducing the function ρ given by

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

It is clear that ρ is injective: If $\rho(x_1, y_1) = \rho(x_2, y_2)$, then $\frac{p+1}{2} - x_1 = \frac{p+1}{2} - x_2$ and $\frac{q+1}{2} - y_1 = \frac{q+1}{2} - y_2$, so $x_1 = x_2$ and $y_1 = y_2$, i.e.$(x_1, y_1) = (x_2, y_2)$.
It is also straightforward to check that if x, y are integers satisfying $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$, and $qx - py < -p/2$, then x', y' are integers satisfying $1 \leq x' \leq (p-1)/2$, $1 \leq y' \leq (q-1)/2$, and $qx' - py' > q/2$, and if x, y are integers satisfying $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$, and $qx - py > q/2$, then x', y' are integers satisfying $1 \leq x' \leq (p-1)/2$, $1 \leq y' \leq (q-1)/2$, and $qx' - py' < -p/2$.
This means that ρ injects elements of $R \cap A$ to some elements of $R \cap B$, and injects elements of $R \cap B$ to some elements of $R \cap A$. Hence, ρ forms a bijection between $R \cap A$ and $R \cap B$, so $\alpha = \beta$ and the proof is complete. □

The Law of Quadratic Reciprocity provides us with a simple method to determine whether a number is a quadratic residue modulo an odd prime number:

Example 5.2. Is 219 a quadratic residue mod 383?
Since $219 = 3 \times 73$ and 383 is an odd prime, we have

$$\begin{aligned}
\left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right) \text{ (by Theorem 3.6)} \\
&= -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) \text{ (by Theorem 5.1, since } 383 \equiv 3 \bmod 4) \\
&= -\left(\frac{2}{3}\right)\left(\frac{18}{73}\right) \text{ (since } 383 \equiv 2 \bmod 3 \text{ and } 383 \equiv 18 \bmod 73) \\
&= -\left(\frac{2}{3}\right)\left(\frac{2}{73}\right)\left(\frac{3}{73}\right)^2 \text{ (by Theorem 3.6, since } 18 = 2 \times 3^2) \\
&= -\left(\frac{2}{3}\right)\left(\frac{2}{73}\right) \text{ (since } \left(\frac{3}{73}\right) = \pm 1) \\
&= -(-1) \cdot 1 \text{ (since } 2 \notin Q_3 \text{ and } 2 \in Q_{73}, \text{ by Corollary 4.3)} \\
&= 1,
\end{aligned}$$

so 219 is a quadratic residue mod 383.

As we can see, group theory is useful in proving certain fundamental results in number theory, such as Euler's Criterion and Gauss's Lemma, which can then be used to prove more complex theorems, such as the Law of Quadratic Reciprocity.

Acknowledgments. It is a pleasure to thank my mentor, Daniele Rosso, for his guidance and support.

References

[1] Michael Downes. Short Math Guide for LaTeX. http://ftp.ams.org/pub/tex/doc/amsmath/short-math-guide.pdf

[2] Gareth A. Jones and J. Mary Jones. Elementary Number Theory. Springer-Verlag London Limited. 1998.

[3] Tobias Oekiter, Hubert Partl, Irene Hyna and Elisabeth Schlegl. The Not So Short Introduction to LaTeX 2_ε. http://tobi.oetiker.ch/lshort/lshort.pdf.

[4] Paul J. Sally, Jr. Tools of the Trade: Introduction to Advanced Mathematics. American Mathematical Society. 2008.