6-2016

Mathematical Reasoning and the Inductive Process: An Examination of The Law of Quadratic Reciprocity

Nitish Mittal
California State University - San Bernardino

Mathematical Reasoning and the Inductive Process: An Examination of the law of Quadratic Reciprocity

---

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Nitish Mittal

June 2016

Mathematical Reasoning and the Inductive Process: An Examination of the law of Quadratic Reciprocity

---

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Nitish Mittal

June 2016

Approved by:

Dr. James Paul Vicknair, Committee Chair	Date
Dr. Zahid Hassan, Committee Member	
Dr. Rolland Trapp, Committee Member	
Dr. Charles Stanton, Chair, Department of Mathematics	Dr. Corey Dunn Graduate Coordinator, Department of Mathematics

Abstract

This project investigates the development of four different proofs of the law of quadratic reciprocity, in order to study the critical reasoning process that drives discovery in mathematics. We begin with an examination of the first proof of this law given by Gauss. We then describe Gauss' fourth proof of this law based on Gauss sums, followed by a look at Eisenstein's geometric simplification of Gauss' third proof. Finally, we finish with an examination of one of the modern proofs of this theorem published in 1991 by Rousseau. Through this investigation we aim to analyze the different strategies used in the development of each of these proofs, and in the process gain a better understanding of this theorem.

Acknowledgements

I wish to thank Dr. James Paul Vicknair for all his help and support during the preparation of this paper. I would also like to thank Dr. Hassan and Dr. Trapp for their comments and contribution to this thesis. I would especially like to thank Dr. Stanton for helping me fully assimilate into the graduate program, and Dr. Dunn in helping me re-enter the program after an extended leave of absence. I would further like to acknowledge my classmates and friends Leonard Lamp, Kevin Baccari, and Avi Misra whose help and support played a pivotal role in my learning and development throughout my tenure in the masters program.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Observation and Induction in Mathematics

> There are even many properties of numbers with which we are well acquainted, but which we are not yet able to prove; only observations have led us to their knowledge. Hence we see that in the theory of numbers, which is still very imperfect, we can place our highest hopes in observations; they will lead us continually to new properties which we shall endeavor to prove afterwards. The kind of knowledge which is supported only by observations and is not yet proved must be carefully distinguished from the truth; it is gained by induction as we usually say. Yet we have seen cases in which mere induction led to error. Therefore we should take care not to accept as true such properties of the numbers which we have discovered by observation and which are supported by induction alone. Indeed, we should use such a discovery as an opportunity to investigate more than exactly the properties discovered and to prove or disprove them; in both cases we may learn something useful.
>
> Leonhard Euler (in [Pól54])

Euler's quote about the use of observation in mathematics is a great commentary on mathematical reasoning and the inductive process itself. As Euler mentions above even in fields as abstract as pure mathematics and the theory of numbers, observation and induction are important tools in helping identify the various intriguing behaviors and patterns of numbers. However, observation alone is not sufficient and the true strength of mathematical discovery lies in the use of mathematical tools to prove without exception what is being observed. As students of mathematics we are no strangers to this process. Identifying a pattern in a given example and applying inductive reasoning to generalize

said pattern is the basis of modern mathematics; however, as Euler notes, we should be vary of proofs by induction alone. The strongest conjectures are those which can not only be supported by inductive reasoning, but proved and reproved using other methods as well. The Law of Quadratic Reciprocity is one such example in the theory of numbers. [Pól54]

1.2 The Law of Quadratic Reciprocity

Dubbed the golden theorem of number theory by the prince of mathematics, Carl Friedrich Gauss, the law of quadratic reciprocity is one of the most pursued theorems of 18th and 19th century mathematics. The theorem was first formulated by Euler in 1783 and later tackled by Legendre in 1785, and again in *Essai sur la Theorie des Nombres* in 1798. Though both his proofs were later shown to be invalid, the elegant notation employed by Legendre eventually became the modern Law of Quadratic Reciprocity. The first complete proof of the theorem was written by Gauss when he was 18, and published in his book *Disquisitiones Arithmaticae* in 1801. In his first attempt Gauss looked at individual cases and used elementary techniques to prove the law and subsequently generalized it using mathematical induction. Gauss later published 6 more proofs of the same theorem, each time employing a different method, refining the proof and making it more elegant. [Büh81]

We will begin with examining thoroughly Gauss's first attempt, which, though rather long, uses only basic techniques. We will then examine two of his latter proofs to see the developments he made over time to further refine his proof. We will look at iterations or simplifications of his third and fourth proofs of the law of quadratic reciprocity. In his fourth proof Gauss used Gaussian sums to prove the law. We will describe his proof in complete detail and examine the differences between this proof and his first attempt, the most apparent of which is the sheer difference in length between the two. We will then analyze his third proof of this theorem. In this proof Gauss employed the use of Gauss's lemma to prove the fundamental theorem in a very concise and elegant fashion. Eisenstein's simplification of this proof is perhaps one of the most commonly used in elementary number theory courses. Finally, we will conclude with a modern elementary proof of the law of quadratic reciprocity.

1.3 What is Covered in this Project

This project will take us through the first known proof of one of the fundamental laws of the theory of numbers and one of the most scrutinized theorems in all of mathematics, and illustrate the ways in which it was reformulated and refined over time. The project is an interesting examination of the essence of the process of "inductive reasoning" described by Polya and provides us a firsthand experience whilst also examining one of Gauss' celebrated contributions to the field of mathematics. While the significance of the latter cannot be denied we stand to gain much more from the former. The "inductive attitude" has been a major driving force for continuous investigation and invention in mathematics and other natural sciences. The process is a telling tale of how the human mind works and how new knowledge is discovered. A journey that is not very different from that of a diamond, starting off as a pebble in a mine and constantly cleaned and refined along the way until it is finally cut and polished to reveal the elegant jewel that it is.

This project outlines a paradigm that has been employed in the discovery of countless other theorems in the past and will continue to help discover countless more in the future. It highlights the process from the recognition of patterns observed by the investigation of special cases, to forming a conjecture and eventually using known techniques to simplify, generalize and prove our conjecture. It further illustrates the importance of continued investigation in helping uncover new implications and interpretations of a theorem. This project ultimately highlights the point that while the saying "necessity is the mother of all invention" may hold true in other natural sciences, the "inductive" attitude and reasoning are certainly the root of all discovery in the abstract field of pure mathematics.

Chapter 2

Background Definitions and Theorems

We will begin by giving some elementary definitions and theorems in number theory, which can be found in the following sources: [Bur07] [Nag51]

2.1 Theory of Congruences

Definition 2.1. *Let n be a fixed positive integer. Two integers a and b are said to be* ***congruent modulo n****, symbolized by*

$$a \equiv b(mod\ n)$$

if n divides the difference $a - b$; that is, given that $a - b = kn$ for some integer k.

Lemma 2.2. *Let a, b and $n > 0$ be integers, then $a \equiv b(mod\ n) \Leftrightarrow n|(a - b)$.*

Proof. If $a \equiv b(\text{mod } n)$, then a and b have the same remainder when divided by n. Thus, by the division algorithm $a = np+r$ and $b = nq+r$, for integers p, q and r with $0 \leq r \leq n$. Now we have,

$$a - np = b - nq$$

$$\Rightarrow a - b = np - nq$$

$$\Rightarrow a - b = n(p - q)$$

Thus, $n|(a-b)$. Conversely, If $n|(a-b)$, then there exist integers x and y such that, $a = nx + r_1$ and $b = ny = r_2$, where $0 \leq r_1 \leq n$ and $0 \leq r_2 \leq n$. Then,

$$a - b = (nx + r_1) - (ny + r_2)$$

$$\Rightarrow a - b = n(x + y) - (r_1 - r_2)$$

Thus, since $n|(a-b)$, n must also divide $(r_1 - r_2)$. However $|r_1 - r_2| < n$, thus $-n < r_1 - r_2 < n$, therefore $r_1 - r_2 = 0$ and $r_1 = r_2$, and so $a \equiv b(\text{mod } n)$. □

Example 2.3. *Let $n = 7$, then $10 \equiv 24(mod\ 7)$ since, $24 - 10 = (2)(7)$. On the other hand, $25 \not\equiv 12(mod\ 7)$, since $25 - 12 \neq (k)(7)$ for any integer k.*

Theorem 2.4. *Let $n > 1$ and a, b, c, d be integers, then the following properties hold:*

(a) $a \equiv a(mod\ n)$.

(b) If $a \equiv b(mod\ \ n)$, then $b \equiv a(mod\ n)$.

(c) If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$.

(d) If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$, then $a + c \equiv b + d(mod\ n)$ and $ac \equiv bd(mod\ n)$.

(e) If $a \equiv b(mod\ n)$, then $a + c \equiv b + c(mod\ n)$ and $ac \equiv bc(mod\ n)$.

(f) If $a \equiv b(mod\ n)$, then $a^k \equiv b^k(mod\ n)$ for any positive integer k.

Proof. For any integer a, $a - a = 0 * n$, so that $a \equiv a(\text{mod } n)$. Furthermore, if $a \equiv b(\text{mod } n)$, then $a - b = kn$ for some integer k. And, $b - a = -kn = (-k)n$ and since $-k$ is an integer property (b) holds.

Now suppose $a \equiv b(\text{mod } n)$ and also $b \equiv c(\text{mod } n)$, then there exist integers p, q such that $a - b = pn$ and $b - c = qn$. Then,

$$a - c = (a - b) + (b - c) = pn + qn = (p + q)n$$

$$\Rightarrow a \equiv c(\text{mod } n)$$

Similarly, if $a \equiv b(\text{mod } n)$ and $c \equiv d(\text{mod } n)$, then $a - b = pn$ and $c - d = qn$ for some p, q and

$$(a + c) - (b + d) = (a - b) + (c - d) = pn + qn = (p + q)n \Rightarrow a + c \equiv b + d(\text{mod } n)$$

Also,

$$ac = (b + pn)(d + qn) = bd + (bq + dp + pqn)n$$

$$\Rightarrow n|(ac - bd) \text{ and } ac \equiv bd(\text{mod } n)$$

The result of property (e) follows from property (d) and property (a). For property (f) we can use mathematical induction. Since the argument holds for $k = 1$, we can assume $a^k \equiv b^k(\text{mod } n)$. Given that $a \equiv b(\text{mod } n)$, (d) implies:

$$aa^k \equiv bb^k(\text{mod } n) \Leftrightarrow a^{k+1} \equiv b^{k+1}(\text{mod } n)$$

□

Lemma 2.5. *If $gcd(a, n) = 1$ and $n > 0$, then there exists a unique integer x modulo n, such that $ax \equiv 1(mod\ n)$.*

Proof. Given $\gcd(a, n) = 1$, we can write $ax + ny = 1$ for some integers x and y. This can be rewritted as $ax - 1 = n(-y)$, thus $n|(ax - 1)$ and $ax \equiv 1(\text{mod } n)$.

Suppose $ax \equiv 1(\text{mod } n)$ and $ax' \equiv 1(\text{mod } n)$, then

$$ax \equiv ax'(\text{mod } n) \Leftrightarrow n|(ax - ax') \Leftrightarrow n|a(x - x')$$

Since $\gcd(a, n) = 1$, n must divide $(x - x')$ and $x \equiv x'(\text{mod } n)$. Therefore the solution x is unique modulo n. □

Example 2.6. *Let $a = 3$ and $n = 5$ then, we know that $gcd(a, n) = 1$ and $(2)(3) = 6 \equiv 1(mod\ 5)$.*

Theorem 2.7. *If $ca \equiv cb(mod\ n)$, then $a \equiv b(mod\ \frac{n}{d})$, where $d = gcd(c, n)$.*

Proof. Let, $c(a - b) = ca - cb = kn$ for som integer k. Given that $\gcd(c, n) = d$, there exist relatively prime integers p and q such that $c = dp$ and $n = dq$. Then,

$$dp(a - b) = kdq \Rightarrow p(a - b) = kq$$

Thus $q|p(a - b)$, and since $\gcd(p, q) = 1$, then by Lemma 2.2

$$q|(a - b) \Rightarrow a \equiv b(\text{mod } q) \text{ or } a \equiv b(\text{mod } \frac{n}{d})$$

□

Example 2.8. *Let $a = 7, b = 2$ and $n = 20$, then for $c = 4$, $28 \equiv 8(mod\ 20)$ and $gcd(c, n) = d = 4$. Therefore, $7 \equiv 2(mod\ \frac{20}{4}) \Rightarrow 7 \equiv 2(mod\ 5)$.*

2.2 Wilson's and Fermat's Theorems

Theorem 2.9. ***Wilson's Theorem.*** *If p is a prime, then $(p-1)! \equiv -1(mod\ p)$.*

Proof. It is apparent that this theorem holds for $p = 2$ or 3, therefore let $p > 3$. Suppose a is an integer from

$$1, 2, 3, ..., p-1$$

Since p is a prime number, $\gcd(a, p) = 1$ and by Lemma 2.5 there is a unique integer a' such that, $1 \leq a' \leq p-1$, that satisfies $aa' \equiv 1(\text{mod } p)$.

Since p is prime, $a = a'$ if and only if $a = 1$ or $p-1$. As we can see $a^2 \equiv 1(\text{mod } p)$ is equivalent to $(a-1)(a+1) \equiv 0(\text{mod } p)$. Thus, either $a - 1 \equiv 0(\text{mod } p)$ and $a = 1$ or $a + 1 \equiv 0(\text{mod } p)$ and $a = p - 1$.

If we remove 1 and $p-1$ the remaining integers $2, 3, ..., p-2$ can be grouped in to pairs a, a' such that $a \neq a'$ and $aa' \equiv 1(\text{mod } p)$. Thus,

$$(p-2)! \equiv 1(\text{mod } p)$$

multiplying both sides by $p-1$, we get

$$(p-1)! \equiv -1(\text{mod } p)$$

□

Example 2.10. *Let $p = 7$, then $(p-1)! = 6! = 720$ and $720 + 1 = (103)(7) \Rightarrow 720 \equiv 1(mod\ 7)$.*

Similarly, for $p = 19$, then $(p-1)! = 18! = 6402373705728000$

$$\textit{and, } 6402373705728000 + 1 = (336967037143579)(19)$$

$$\Rightarrow 6402373705728000 \equiv -1(mod\ 19).$$

Theorem 2.11. ***Fermat's little Theorem.*** *Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1(mod\ p)$.*

Proof. Let us consider the first $p-1$ postitive multiple of a:

$$a, 2a, 3a, ..., (p-1)a$$

These numbers are not congruent modulo p to each other or to zero. Otherwise,

$$ma \equiv na(\text{mod } p) \quad \text{where,} \quad 1 \leq m < n \leq p-1$$

$$\Rightarrow m \equiv n(\text{mod } p)$$

which is impossible. Thus it is apparent that these integer multiples of a are distinct and must be congruent modulo p to $1, 2, 3, ..., p-1$. Multiplying these together we get,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)(\text{mod } p)$$

$$\Rightarrow a^{p-1}(p-1)! \equiv (p-1)!(\text{mod } p)$$

By cancelling $(p-1)!$ from both sides we get the desired result. □

Example 2.12. *Let $p = 7$ and $a = 5$, then $7 \nmid 5$ and,*

$$5^{7-1} = 5^6 = 15625 \text{ and } 15625 - 1 = (2232)(7)$$

$$\Rightarrow 15625 \equiv 1(mod\ 7)$$

Similarly, for $p = 13$ and $a = 28$, then $13 \nmid 28$ and,

$$28^{13-1} = 28^{12} = 232218265089212416$$

$$\Rightarrow 232218265089212416 - 1 = (17862943468400955)(13)$$

$$\Rightarrow 232218265089212416 \equiv 1(mod\ 13)$$

2.3 Euler's Criterion and Legendre Symbol

Definition 2.13. *Let p be an odd prime and $gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a(mod\ p)$ has a solution, then a is said to be a **quadratic residue** of p. Otherwise, a is called a **quadratic nonresidue** of p.*

Example 2.14. *Let $p = 11$ then,*

$$1^2 \equiv 10^2 \equiv 1, \quad 2^2 \equiv 9^2 \equiv 4, \quad 3^2 \equiv 8^2 \equiv 9$$

$$4^2 \equiv 7^2 \equiv 5, \quad 5^2 \equiv 6^2 \equiv 3(mod\ 11)$$

Thus $1, 3, 4, 5$, and 9 are quadratic residues of 11 and $2, 6, 7, 8$, and 10 and nonresidues of 11.

Definition 2.15. *If $gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a* ***primitive root*** *of the integer n.*

Example 2.16. *The definition can be restated as, $a^{\phi(n)} \equiv 1(mod\ n)$ and $a^k \not\equiv 1(mod\ n)$ for all $k < \phi(n)$ if a is a primitive root of n. Furthermore, if n is a prime number, $\phi(n) = n - 1$, for all n. Then for $a = 2$ and $n = 13$ we have,*

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 3, \quad 2^5 \equiv 6, \quad 2^6 \equiv 12, \quad 2^7 \equiv 11$$

$$2^8 \equiv 9, \quad 2^9 \equiv 5, \quad 2^{10} \equiv 10, \quad 2^{11} \equiv 7, \quad 2^{12} \equiv 1(mod\ 13)$$

Theorem 2.17. ***Euler's Criterion.*** *Let p be an odd prime and $gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.*

Proof. Suppose a is a quadratic residue of p, such that $x^2 \equiv a(\text{mod } p)$ has a solution. Lets call it x_1. Then, $\gcd(x_1, p) = 1$ since $\gcd(a, p) = 1$. Thus by Fermat's little theorem

$$a^{\frac{(p-1)}{2}} \equiv (x_1^2)^{\frac{(p-1)}{2}} \equiv 1(\text{mod } p)$$

If we assume that the congruence $a^{\frac{(p-1)}{2}} \equiv 1(\text{mod } p)$ holds, and let r be a primitive root of p. Then $a \equiv r^k(\text{mod } p)$ for some integer k, with $1 \leq k \leq p - 1$. It follows that

$$r^{\frac{k(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} \equiv 1(\text{mod } p)$$

The order of $r = (p - 1)$ must divide the exponent $\frac{k(p-1)}{2}$ implying k is even. Lets say $k = 2j$, then

$$(r^j)^2 = r^{2j} = r^k \equiv a(\text{mod } p)$$

making r^j a solution of the congruence $x^2 \equiv a(\text{mod } p)$. □

Corollary 2.18. *Let p be an odd prime and $gcd(a, p) = 1$. Then a is a quadratic residue or non residue of p according to whether*

$$a^{\frac{p-1}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{p-1}{2}} \equiv -1(mod\ p)$$

Proof. Since p is always an odd prime and $\gcd(a, p) = 1$, then

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} \equiv 1(\text{mod } p)$$

Hence, either $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$ or $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, but not both, otherwise $1 \equiv -1(\text{mod } p)$ and $p|2$. A quadratic nonresidue of p does not satisfy $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, therefore it must satisfy $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$. □

Definition 2.19. *Let p be an odd prime and let $gcd(a, p) = 1$. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by*

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

*Legendre's symbol is only defined for primes p. Jacobi later introduced a more general symbol known as the **Jacobi Symbol** $\left(\frac{a}{P}\right)$, for all natural odd numbers P, when:*

$$P = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

is a product of primes $p_1^{e_1}, p_2^{e_2}, \ldots, p_m^{e_m}$, and when a is relatively prime to P. Then:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_m}\right)^{e_m}$$

where the factors on the right hand side are Legendre symbols. Thus when P is a quadratic residue of a, $\left(\frac{a}{P}\right) = 1$ since all the factors on the right hand side equal 1. However, when P is not a quadratic residue it is not necessarily true that $\left(\frac{a}{P}\right) = -1$. This is because when an even number of factors on the right hand side have the value -1, the resulting product will be $+1$. We will use Jacobi symbol in Gauss' first proof of quadratic reciprocity and we note that the Jacobi symbol in not defined for the integers $P < 0$ or for even P.

Example 2.20. *Using legendre symbol, we can rewrite Example 2.14 as:*

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

and

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Theorem 2.21. *Let p be and odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties:*

(a) If $a \equiv b(\text{mod } p)$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) $\left(\frac{a^2}{p}\right) = 1$

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

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

(e) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = -1^{\frac{(p-1)}{2}}$, *and* $\left(\frac{0}{p}\right) = 0$.

(f) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$.

Proof. If $a \equiv b(\text{mod } p)$, then the two congruences $x^2 \equiv a(\text{mod } p)$ and $x^2 \equiv b(\text{mod } p)$ have the same exact solutions, and thus either both are solvable or both unsolvable, hence $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. For property (b) integer a trivially satisfies the congruence $x^2 \equiv a(\text{mod } p)$, hence $\left(\frac{a^2}{p}\right) = 1$. Property (c) is a direct result of Euler's criterion. Using (c) we get

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} b^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\text{mod } p)$$

Since Legendre symbol assumes only values 1 or -1, if $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ we would get $1 \equiv -1(\text{mod } p)$ or $2 \equiv 0(\text{mod } p)$, but $p > 2$. Thus,

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

The first part of property (e) is a special case of property (b), when $a = 1$, and the second part is derived from property (c) when $a = -1$. The result for property (f) follows directly from properties (b) and (d). □

Theorem 2.22. *If p is an odd prime, then*

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

Hence, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues of p.

Proof. Let r be a primitive root of p. Then modulo p, the powers $r, r^2, ..., r^{p-1}$ are just a permutation of the integers $1, 2, ..., p-1$. Thus for any a between 1 and $p-1$, there exists a unique positive integer $k(1 \leq k \leq p-1)$, such that $a \equiv r^k(\text{mod } p)$. By Euler's criterion we have

$$\left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right) \equiv (r^k)^{\frac{(p-1)}{2}} = (r^{\frac{(p-1)}{2}})^k \equiv (-1)^k(\text{mod } p)$$

where, $r^{\frac{(p-1)}{2}} \equiv -1 (\text{mod } p)$ because r is a primitive root of p. We can then add up the Legendre symbols to obtain

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

□

Corollary 2.23. *The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.*

2.4 Gauss' Lemma

Theorem 2.24. ***Gauss' Lemma.*** *Let p be an odd prime and let $gcd(a, p) = 1$. If n denotes the number of integers in the set*

$$S = \left\{a, 2a, 3a, ..., \left(\frac{p-1}{2}\right) a\right\}$$

whose remainders upon division by p exceed $p/2$, then

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

Proof. Because $\gcd(a, p) = 1$, none of the $\frac{(p-1)}{2}$ integers in S are congruent to zero or to one another modulo p. Let $r_1, ..., r_m$ be those remainders upon division by p such that $0 < r_i < \frac{p}{2}$, and let $s_1, ..., s_n$ be those remainders such that $p > s_i > \frac{p}{2}$. Then $m + n = \frac{(p-1)}{2}$, and the integers

$$r_1, ..., r_m \qquad p - s_1, ..., p - s_n$$

are all positive and less than $\frac{p}{2}$.

To prove that these integers are all distinct, it suffices to show that no $p - s_i$ is equal to any r_j. Let us assume that $p - s_i = r_j$, for some i and j, then there exist u and v $(1 \leq u, v \leq \frac{(p-1)}{2})$ such that $s_i \equiv ua (\text{mod } p)$ and $r_j \equiv va (\text{mod } p)$. Thus,

$$(u + v)a \equiv s_i + r_j = p \equiv 0 (\text{mod } p)$$

However, $u + v \not\equiv 0 (\text{mod } p)$ since $1 < u + v \leq p - 1$. The central point is that the $\frac{(p-1)}{2}$ numbers

$$r_1, ..., r_m \qquad p - s_1, ...p - s_n$$

are the integers $1, 2, ..., \frac{(p-1)}{2}$ (in some order). Thus, their product is $\frac{(p-1)}{2}!$:

$$\left(\frac{p-1}{2}\right)! = r_1 \cdots r_m (p - s_1) \cdots (p - s_n)$$

$$\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) (\text{mod } p)$$

$$\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n (\text{mod } p)$$

We know that $r_1, ..., r_m, s_1, ..., s_n$ are congruent modulo p to $a, 2a, ..., \frac{(p-1)}{2}a$ (in some order), thus

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a (\text{mod } p)$$

$$\equiv (-1)^n a^{\frac{(p-1)}{2}} \left(\frac{p-1}{2}\right)! (\text{mod } p)$$

Since $\left(\frac{p-1}{2}\right)!$ is relatively prime to p, we can cancel it from both sides:

$$1 \equiv (-1)^n a^{\frac{(p-1)}{2}} (\text{mod } p)$$

multiplying both sides by $(-1)^n$, we get

$$a^{\frac{(p-1)}{2}} \equiv (-1)^n (\text{mod } p)$$

Using Euler's criterion we get:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \equiv (-1)^n (\text{mod } p)$$

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

□

Example 2.25. *Now we can look at Gauss's lemma with an example, where* $a = 7$ *and* $p = 17$. *Then* $(p - 1)/2 = 8$ *and:*

$$S = \{7, 14, 21, 28, 35, 42, 49, 56\}$$

Modulo 17, we can rewrite S as the following:

$$S = \{7, 14, 4, 11, 1, 8, 15, 5\}$$

Three of these are greater that $17/2$; therefore, $n = 3$, and according to Theorem 2.24:

$$\left(\frac{7}{17}\right) = (-1)^3 = -1$$

We can also confirm this using the Corollary 2.18 to Euler's criterion:

$$7^{\left(\frac{17-1}{2}\right)} \equiv 16 \equiv -1 (mod\ 17)$$

Theorem 2.26. *Using Gauss's lemma, we can show that if p is an odd prime, then*

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

Proof. According to Gauss's lemma, $\left(\frac{2}{p}\right) = (-1)^n$ where n is the number of integers in the set

$$S = \left\{2, 4, 6, ..., 2\left(\frac{p-1}{2}\right)\right\}$$

whose remainders upon division by p are greater than $p/2$. Since all members of S are less than p modulo p it suffices to count the number of even integers $1 < 2k < (p-1)/2$ that exceed $p/2$. We see that $2k < p/2$ when $k < p/4$; therefore, if we let $[p/4]$ be the largest even integer less than $p/2$, then

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

Now we can look at the individual cases for the four different forms of p:

$$\text{If } p = 8M + 1, \text{ then } n = 4M - \left[2M + \frac{1}{4}\right] = 4M - 2M = 2M$$

$$\text{If } p = 8M + 3, \text{ then } n = 4M + 1 - \left[2M + \frac{3}{4}\right] = 4M + 1 - 2M = 2M + 1$$

$$\text{If } p = 8M + 5, \text{ then } n = 4M + 2 - \left[2M + 1 + \frac{1}{4}\right] = 4M + 2 - 2M - 1 = 2M + 1$$

$$\text{If } p = 8M + 7, \text{ then } n = 4M + 3 - \left[2M + 1 + \frac{3}{4}\right] = 4M + 3 - 2M - 1 = 2M + 2$$

Thus, when $p \equiv \pm 1 \pmod 8 \Leftrightarrow p = 8M + 1$ or $8M + 7$, n is even and $(-1)^n$ is 1.

Conversely, if $p \equiv \pm 3 \pmod 8 \Leftrightarrow p = 8M + 3$ or $8M + 5$, n is odd and $(-1)^n$ is -1. □

2.5 Gauss Sums

More information on the Gauss Sum can be found in the following text: [Lem00]

Definition 2.27. *An* ***n^{th} root of unity*** *is a complex number ζ_n such that, $\zeta_n^n = 1$. Thus,*

$$\zeta_n = cos\ \frac{2\pi}{n} + i\ sin\ \frac{2\pi}{n} = e^{i\frac{2\pi}{n}}$$

Example 2.28. *Let $\zeta_3 = e^{i\frac{2\pi}{3}}$. Now,*

$$(\zeta_3)^3 = (e^{i\frac{2\pi}{3}})^3 = e^{i2\pi} = cos\ 2\pi + i\ sin\ 2\pi = 1 + i \cdot 0 = 1$$

Definition 2.29. *If we fix an odd prime p, then the* ***Gauss Sum*** *associated with an integer a is:*

$$G_a = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an}$$

Example 2.30. *Let $p = 5$ and $a = 3$, now the Gauss sum G_3 is:*

$$\sum_{n=0}^{4} \left(\frac{n}{p}\right) \zeta_5^{3n} = \left(\frac{1}{5}\right) \zeta_5^3 + \left(\frac{2}{5}\right) \zeta_5 + \left(\frac{3}{5}\right) \zeta_5^4 + \left(\frac{4}{5}\right) \zeta_5^2$$

$$= \zeta_5^3 - \zeta_5 - \zeta_5^4 + \zeta_5^2$$

Theorem 2.31. *For any integer a*

$$\sum_{n=0}^{p-1} \zeta_p^{an} = \begin{cases} p & \text{if } p \mid a \\ 0 & \text{if } p \nmid a \end{cases}$$

Proof. 1. When $p \mid a$ we can write $a = xp$, and we get:

$$\sum_{n=0}^{p-1} \zeta_p^{an} = \sum_{n=0}^{p-1} \zeta_p^{xpn}$$

Now, since $(\zeta_p)^p = 1$, we have:

$$\sum_{n=0}^{p-1} \zeta_p^{xpn} = \sum_{n=0}^{p-1} 1^{xn} = p$$

2. When $p \nmid a$. First we look at the following identity:

$$x^p - 1 = (x-1) \cdot (x^{p-1} + \cdots + 1)$$

$$\Rightarrow (x^{p-1} + \cdots + 1) = \frac{(x^p - 1)}{(x - 1)}$$

Now, if we substitute ζ_p^a for x, we get:

$$\sum_{n=0}^{p-1} (\zeta_p^a)^n = ((\zeta_p^a)^{p-1} + \cdots + 1) = \frac{(\zeta_p^{ap} - 1)}{(\zeta_p^a - 1)}$$

Now, since $(\zeta_p)^p = 1$, we get:

$$\frac{(\zeta_p^{ap} - 1)}{(\zeta_p^a - 1)} = \frac{(1^a - 1)}{(\zeta_p^a - 1)} = 0$$

□

Corollary 2.32. *For any integer x, y*

$$\sum_{n=0}^{p-1} \zeta_p^{(x-y)n} = \begin{cases} p & \text{if } x \equiv y (mod\ p) \\ 0 & \text{if } x \not\equiv y (mod\ p) \end{cases}$$

The proof for Corollary 2.31 is exactly the same as that of Theorem 2.30, and can be acheived by replacing $(x - y)$ with a.

Example 2.33. *Let $p = 3$ and $a = 6$, then $p \mid a$ and:*

$$\sum_{n=0}^{2} \zeta_3^{6n} = \sum_{n=0}^{2} \left(\zeta_3^3\right)^{2n} = \sum_{n=0}^{2} 1^{2n} = 1 + 1 + 1 = 3 = p$$

Example 2.34. *Let $p = 3$ and $a = 2$, then $p \nmid a$ and:*

$$\sum_{n=0}^{2} \zeta_3^{2n} = 1 + \zeta_3^2 + \zeta_3 \tag{2.1}$$

We know that ζ_3 is a solution for the equation $x^3 - 1 = 0$, which can be expanded to $(x-1)(x^2+x+1)$. Here we take the right hand side of the product to be 0 (since $\zeta_3 \neq 1$), then $x^2 + x + 1 = 0$ and $x^2 = -x - 1$. Substituting ζ_3 back in for x, we get $\zeta_3^2 = -\zeta_3 - 1$. Applying this to Equation 2.1 above, we get:

$$\sum_{n=0}^{2} \zeta_3^{2n} = 1 - \zeta_3 - 1 + \zeta_3 = 0$$

Theorem 2.35. *The **Gauss Sum** $G_0 = 0$.*

Proof.

$$G_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{0n} = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)$$

Now by applying Theorem 2.22 to the right hand side, we get:

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0$$

since there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues of p. □

Example 2.36. *Let $p = 3$ and $a = 0$, then:*

$$G_0 = \sum_{n=0}^{2} \left(\frac{n}{3}\right) \zeta_3^{0n} = \left(\frac{0}{3}\right) \cdot 1 + \left(\frac{1}{3}\right) \cdot 1 + \left(\frac{2}{3}\right) \cdot 1$$

$$\Rightarrow 0 + 1 - 1 = 0$$

2.6 Normal Subgroups and Quotient Groups

More information on the theorems and definitions of group theory delineated below can be found in the following text: [Rom05]

Definition 2.37. *An **abelian group** G^* is a set G with a binary operation $*$ such that the following properties hold:*

1. (**Closure**) *If $x, y \in G$, then $x * y \in G$.*
2. (**Associativity**) *$x * (y * z) = (x * y) * z$, for all $x, y, z \in G$.*
3. (**Identity**) *There exists an element $e \in G$, such that $e * x = x$ for all $x \in G$.*
4. (**Inverse**) *For all $x \in G$, there exists $y \in G$, such that $x * y = e$.*
5. (**Commutativity**) *$x * y = y * x$ for all $x, y \in G$.*

Example 2.38. *The group of all integers $\mathbb{Z}$ is an abelian group under addition.*

1. *The sum of any two integers is an integer.*
2. *The associativity law applies to all integers. Eg:* $2 + (3 + 4) = (2 + 3) + 4$.
3. *The additive identity for all integers is* 0.

4. *The additive inverse for any integer x is $-x$, which is also an integer.*
5. *Integer addition is commutative. Eg:* $2 + 3 = 3 + 2$

Example 2.39. *The group of rational numbers $\mathbb{Q}$, without 0, is an abelian group under multiplication. We need to remove 0, because 0 does not have a multiplicative inverse.*

1. *The products of two rational numbers is a rational number.*
2. *Integers are a subgroup of rationals, thus associativity applies as seen in the example above.*
3. *The multiplicative identitiy for rationals is* 1.
4. *The multiplicative inverse for any rational $\frac{x}{y}$, where $x, y \in \mathbb{Z}$ is $\frac{y}{x}$.*
5. *Rational multiplication is commutative. Eg.* $2 * 3 = 3 * 2$.

Definition 2.40. *A subset S of a group G, is said to be a* **subgroup** *of G, if it is a group itself.*

Example 2.41. *Consider the set of real numbers $\mathbb{R}$, which is a group under addition. Then the integers $\mathbb{Z}$, which are a subset of real numbers, and also form a group under addition (see Example 2.38), are said to a be a subgroup of $\mathbb{R}$.*

Definition 2.42. *Let H be a subgroup of G, and let $x \in G$ be an element of G, then we define $x * H$, as the subset $\{x * h \mid h \in H\}$, to be a* ***left coset*** *of H, and $H * x$, as the subset $\{h * x \mid h \in H\}$ to be the* ***right coset*** *of H. Where $*$ is a binary operation, such as addition or multiplication, depending on the definition of the group G.*

Example 2.43. *Consider the set of all even integers $2\mathbb{Z}$, it is clear that this is a group under addition. We also know that the set of all integers $\mathbb{Z}$ is a group, thus $2\mathbb{Z}$ is clearly a subgroup of $\mathbb{Z}$. Then we can say that, $1 + 2\mathbb{Z}$ is a left coset of $2\mathbb{Z}$, and $2\mathbb{Z} + 1$ is a right coset of $2\mathbb{Z}$.*

Definition 2.44. *A subgroup H is said to be a* ***normal subgroup*** *of G, if the left cosets of H are equal to the right cosets of H. That is $x * H = H * x$ for all $x \in G$.*

Example 2.45. *Let's look at the subgroup $2\mathbb{Z}$ from Example 2.43 above. We can see that the left coset of $2\mathbb{Z}$, $1 + 2\mathbb{Z}$, is equal to the set of odd integers $\{\ldots, -3, -1, 1, 3, \ldots\}$. Furthermore, the right coset of $2\mathbb{Z}$, $2\mathbb{Z} + 1$, is also equal to the set of odd integers $\{\ldots, -3, -1, 1, 3, \ldots\}$. Thus, $2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.*

Definition 2.46. *If H is a normal subgroup of G, then we can construct a group G/H by multiplying the left cosets of H, such that for all $\alpha, \beta \in G$, $\alpha H \beta H = \alpha\beta H$. The group G/H is called the* ***quotient group*** *of G by H. (Note: Here we say left cosets for the sake of illustration. However, since H is a normal subgroup of G, the left and the right cosets of H are equal.)*

Example 2.47. *Let $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and let H be the normal subgroup $\{0, 3\}$. The cosets of H are:*

$$\{0, 3\}\,, \qquad 1 + \{0, 3\} = \{1, 4\}\,, \qquad 2 + \{0, 3\} = \{2, 5\}$$

Then the quotient group G/H is a group of order 3 containing the following elements: $\{0, 3\}, \{1, 4\}, \{2, 5\}$.

2.7 The Chinese Remainder Theorem

Fore more information on the Chinese Remainder Theorem, please refer to the following text: [Sti94]

Definition 2.48. *A non-empty set R, along with the binary operations of multiplication and addition, is called a* ***ring****, if it satisfies the following properties:*

1. *R is an abelian group under the order addition.*
2. *Multiplication in R is associative. That is $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ for all $\alpha, \beta, \gamma \in R$.*
3. *Multiplication in R is distributive. That is $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ for all $\alpha, \beta, \gamma \in R$.*

Example 2.49. *Consider the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Let $n = 7$ and we can see that $\mathbb{Z}/7\mathbb{Z}$ is a ring.*

1. *We can check that $\mathbb{Z}/7\mathbb{Z}$ is abelian under addition using Definition 2.37.*
   - *i.* $3 + 5 = 8 \equiv 1 (mod\ 7) \in \mathbb{Z}/7\mathbb{Z}$.
   - *ii.* $1 + (2 + 3) = (1 + 2) + 3 \equiv 6 (mod\ 7) \in \mathbb{Z}/7\mathbb{Z}$.
   - *iii. The additive identity for all elements in $\mathbb{Z}/7\mathbb{Z}$ is 0.*
   - *iv. The additive inverse for any element $x \in \mathbb{Z}/7\mathbb{Z}$ is $-x \in \mathbb{Z}/7\mathbb{Z}$.*
   - *v.* $2 + 3 = 3 + 2 = 5 (mod\ 7) \in \mathbb{Z}/7\mathbb{Z}$.
2. $1 * (2 * 3) = (1 * 2) * 3 \equiv 6 (mod\ 7) \in \mathbb{Z}/7\mathbb{Z}$.
3. $2 * (3 + 5) = (2 * 3) + (2 * 5) \equiv 2 (mod\ 7) \in \mathbb{Z}/7\mathbb{Z}$.

Definition 2.50. *Let G and H be two groups. A function $f : G \to H$ is called an isomorphism between G and H, if*

1. *f is a homomorphism, that is for any $a, b \in G$, $f(ab) = f(a)f(b)$.*
2. *f is a one-to-one and onto mapping from G to H.*

Example 2.51. *Let G be the positive real numbers under addition, and H be the real numbers under multiplication. Then $f = log: G \to H$ is an isomorphism.*

1. *log (xy) = log x + log y.*
2. *Let log x = log y, then $e^{log\ x} = e^{log\ y} \Rightarrow x = y$. Thus f is one-to-one.*
3. *Since, the log function spans all real numbers it is clear that f is onto.*

Theorem 2.52. ***The Chinese Remainder Theorem.***
If gcd$(m, n) = 1$, then the map $f(x) = (x \bmod m, x \bmod n)$ is an isomorphism of $\mathbb{Z}/mn\mathbb{Z}$ onto $(\mathbb{Z}/m\mathbb{Z}) * (\mathbb{Z}/n\mathbb{Z})$.

Proof. Let m be a non-zero integer, then there is a ring homomorphism $g : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ such that $g(x) = x \pmod m$. We have already seen in an example above that $\mathbb{Z}/m\mathbb{Z}$ is indeed a ring. We can also see that it is a homomorphism:

$$g(x + y) = (x + y)(\text{mod } m)$$
$$= x(\text{mod } m) + y(\text{mod } m)$$
$$= g(x) + g(y)$$

and

$$g(xy) = (xy)(\text{mod } m)$$
$$= x(\text{mod } m)y(\text{mod } m)$$
$$= g(x)g(y)$$

Similarly, if n is another non-zero integer, then $h(x) = x \pmod n$ is another ring homomorphism that takes $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
Let f be a mapping that combines these two homomorphisms, such that $f : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) * (\mathbb{Z}/n\mathbb{Z})$, by defining:

$$f(x) = (g(x), h(x))$$
$$= (x(\text{mod } m), x(\text{mod } n))$$

Now, the ring operations on $(\mathbb{Z}/m\mathbb{Z}) * (\mathbb{Z}/n\mathbb{Z})$ are component-wise addition and multiplication.

$$(x, u) + (y, v) = (x + y, u + v)$$
$$(x, u)(y, v) = (xy, uv)$$

where $x, y \in \mathbb{Z}/m\mathbb{Z}$ and $u, v \in \mathbb{Z}/n\mathbb{Z}$.
Now, we can see that f is a homomorphism, since:

$$f(x+y) = (g(x+y), h(x+y))$$
$$= (g(x) + g(y), h(x) + h(y))$$
$$= (g(x), h(x)) + (g(y), h(y))$$
$$= f(x) + f(y)$$

and

$$f(xy) = (g(xy), h(xy))$$
$$= (g(x)g(y), h(x)h(y))$$
$$= (g(x), h(x))(g(y), h(y))$$
$$= f(x)f(y)$$

Moreover, we also note that:

$$f(x+mn) = ((x+mn(\text{mod } m)), (x+mn(\text{mod } n)))$$
$$= ((x(\text{mod } m)), (x(\text{mod } n)))$$
$$= f(x)$$

Thus it is clear that $f(x)$ only depends on $x \pmod{mn}$, and we can say that f is a homomorphism from $\mathbb{Z}/mn\mathbb{Z}$ to $(\mathbb{Z}/m\mathbb{Z}) * (\mathbb{Z}/n\mathbb{Z})$.
Now we only need to show that f is one-to-one and onto from $\mathbb{Z}/mn\mathbb{Z}$ to $(\mathbb{Z}/m\mathbb{Z})*(\mathbb{Z}/n\mathbb{Z})$. We can show that f is one-to-one if $f(x) = 0 \leftrightarrow x = 0$. Let us assume that $f(x) = 0$, then:

$$f(x) = 0 = (0 \text{ mod } m, 0 \text{ mod } n)$$
$$= (x \text{ mod } m, x \text{ mod } n)$$
$$\Rightarrow x = 0 \text{ mod } m, \qquad \text{and} \qquad 0 \text{ mod } n$$

Since, $\gcd(m, n) = 1$, x must be congruent to 0 mod mn. Thus, $x = 0$ in $\mathbb{Z}/mn\mathbb{Z}$ and f is one-to-one.
In order to show that f is onto, for any two integers a, b, there exists an integer x, such that:

$$f(x) = (a \bmod m, b \bmod n)$$

Thus, we have:

$$x = a \bmod m \qquad \text{and} \qquad x = b \bmod n \tag{2.2}$$

Now, since m and n are relatively prime, we know that there exist unique integers u and v, such that:

$$um + nv = 1 \tag{2.3}$$

We claim that

$$x = bum + anv \tag{2.4}$$

is a solution to Equation 2.2. We can test this by first multiplying a to both sides of Equation 2.3:

$$aum + anv = a \tag{2.5}$$

Now, combining Equation 2.4 and 2.5, it is clear that:

$$x \bmod m \equiv anv \bmod m \equiv a \bmod m$$

A similar calculation can be done by multiplying Equation 2.3 with b:

$$bum + bnv = b \tag{2.6}$$

Now, combining Equation 2.5 and 2.6, we get:

$$x \bmod n \equiv bum \bmod n \equiv b \bmod n$$

This shows that $x = a \bmod m$ and $x = b \bmod n$, therefore f is also an onto mapping. This proves that f is indeed an isomorphism and completes our proof.

□

Chapter 3

Proofs of The Law of Quadratic Reciprocity

3.1 The Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity is one of the fundamental theorems of number theory. Legendre attempted two incomplete proofs of the law in 1785 and 1798 respectively, and it was eventually proved by Gauss in 1801. Despite Legendre's incomplete attempts to prove the law, his elegant notation, most importantly the Legendre symbol, eventually became the modern Law of Quadratic Reciprocity. The iteration of Gauss's first proof of quadratic reciprocity described here was composed with information from the following sources: [Bau15] [Dir91] [GC86] [Lem00]

Theorem 3.1. ***Quadratic Reciprocity Law.***

If p and q are distinct odd primes, then

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

3.2 Gauss's First Proof of Quadratic Reciprocity

In his first proof Gauss utilized the method of induction to prove the Generalized Quadratic Reciprocity Law. The startegy he used was to show that if we assume the Quadratic Reciprocity Law to be true for every distinct pair of odd primes less than a prime q then it must also hold true for every combination of those primes with q. Since,

the theorem holds true for the two smallest odd primes 3 and 5, that is: $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1$, then it must also hold for every combination of 3 and 5 with the next largest prime 7. Consequently, if it holds true for every combination of the primes 3, 5 and 7, then it must also hold true for every combination of 3, 5 and 7 with the prime 11 and so on. Thus by mathematical induction it will hold true for every pair of distinct odd primes.

In the first proof, Gauss looked at each of the following eight cases for the primes p and q, where p is an odd prime less than q and we assume that Theorem 3.1 holds for each pair of distinct odd primes less than q. The eight cases are as follows:

1. If $q = 4n+1, p = 4n+1$ and $\left(\frac{p}{q}\right) = 1$, then we have to prove that $\left(\frac{q}{p}\right) = 1$;
2. If $q = 4n+1, p = 4n+3$ and $\left(\frac{p}{q}\right) = 1$, then we have to prove that $\left(\frac{q}{p}\right) = 1$;
3. If $q = 4n+1, p = 4n+1$ and $\left(\frac{p}{q}\right) = -1$, then we have to prove that $\left(\frac{q}{p}\right) = -1$;
4. If $q = 4n+1, p = 4n+3$ and $\left(\frac{p}{q}\right) = -1$, then we have to prove that $\left(\frac{q}{p}\right) = -1$;
5. If $q = 4n+3, p = 4n+3$ and $\left(\frac{p}{q}\right) = 1$, then we have to prove that $\left(\frac{q}{p}\right) = -1$;
6. If $q = 4n+3, p = 4n+1$ and $\left(\frac{p}{q}\right) = 1$, then we have to prove that $\left(\frac{q}{p}\right) = 1$;
7. If $q = 4n+3, p = 4n+3$ and $\left(\frac{p}{q}\right) = -1$, then we have to prove that $\left(\frac{q}{p}\right) = -1$;
8. If $q = 4n+3, p = 4n+1$ and $\left(\frac{p}{q}\right) = -1$, then we have to prove that $\left(\frac{q}{p}\right) = -1$;

Later demonstrations by Dedekind and Bachmann showed that these 8 possibilites can be collapsed into the following two mutually exclusive cases, which encompass all of the possibilities listed above:

i. at least one of $\left(\frac{p}{q}\right)$ or $\left(\frac{-p}{q}\right)$ is 1, then $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$;
ii. q is of the form $4M+1$ and $\left(\frac{p}{q}\right) = -1$, then $\left(\frac{q}{p}\right) = -1$

We know from the Corollary 2.18 to Euler's criterion that $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$, therefore case (i) covers the following possibilities:

$$q \text{ is of the form } 4M+3 \text{ and } \left(\frac{q}{p}\right) = 1;$$

$$q \text{ is of the form } 4M+3 \text{ and } \left(\frac{q}{p}\right) = -1;$$

$$q \text{ is of the form } 4M+1 \text{ and } \left(\frac{q}{p}\right) = 1;$$

When $q = 4M + 3$,

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

Thus, either $\left(\frac{p}{q}\right) = 1$ or $\left(\frac{-p}{q}\right) = 1$. Conversely, when $q = 4M + 1$,

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

Therefore, either both $\left(\frac{-p}{q}\right) = \left(\frac{p}{q}\right) = 1$ or $\left(\frac{-p}{q}\right) = \left(\frac{p}{q}\right) = -1$ (which constitutes case (ii)).

Proof. We desire to show that if p and q are distinct odd primes and the Quadratic Reciprocity Law holds for all primes less than q, then when $p < q$:

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

Proving cases (i) and (ii) listed above will thus prove the Generalized Quadratic Reciprocity law, which simply states that the theorme is also true for two relatively prime odd integers P and Q, given that all prime factors of P and Q are less than q; that is,

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \tag{3.1}$$

In order to prove case (i), we assume that at least one (or both) of $\left(\frac{p}{q}\right)$ and $\left(\frac{-p}{q}\right)$ is 1, and we need to show that

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \tag{3.2}$$

Let $w = \pm p$, for which $\left(\frac{w}{p}\right) = 1$. Now, there are two distinct solutions x for the equation $x^2 \equiv w (\text{mod } q)$. Let these solutions be positive and $< q$. If x_0 is one such integer, then the other is $q - x_0$. (Since, $x_0^2 = x^2$ and $(q - x_0)^2 = (-x_0)^2 = x^2$.) Let e be the solution which is even. (Since, q is odd, one of x_0 or $q - x_0$ must be even.) Then, for $0 < e < q$,

$$e^2 - w = fq \tag{3.3}$$

Now we can see that f cannot be negative. In order for f to be negative, p would have to be positive and greater than e^2. Consequently, $p - e^2 = fq$, where $p - e^2$ is divisible by q; however, since $p - e^2 < p$ and $p < q$ this is impossible because q is a prime and cannot divide any number smaller than itself. Furthermore, $f < q$ because both e and w are less than q and therefore: $fq = e^2 - w \leq (q-1)^2 - w = q^2 - 2q - (w-1) < q^2 - 3q = q(q-3)$. Therefore, $f < q$. Moreover, f is odd, since $fq = e^2 - w$ is odd. Now there are two possibilities for Equation 3.3.

1. e and f are coprime to w.

Since, $e^2 \equiv fq \pmod{w}$, $\left(\frac{fq}{|w|}\right) = 1$, and $\left(\frac{f}{|w|}\right) = \left(\frac{q}{|w|}\right)$. Also, $e^2 \equiv w \pmod{f}$, therefore, $\left(\frac{w}{f}\right) = 1$. Now, both f and w are relatively prime odd integers less than q, therefore we can apply Equation 3.1 and we get:

$$\left(\frac{q}{|w|}\right) = \left(\frac{f}{|w|}\right) = \left(\frac{|w|}{f}\right)(-1)^{\frac{w-1}{2}\frac{f-1}{2}} = (-1)^{\frac{w-1}{2}\frac{f-1}{2}} \tag{3.4}$$

Since e is even, e^2 is divisible by 4. Therefore, $-w \equiv fq \pmod{4}$. Also:

$$-w - 1 = fq - 1 (\text{mod } 4) \qquad \text{and} \qquad \frac{-w-1}{2} = \frac{fq-1}{2} (\text{mod } 2)$$

Setting $f' = (f-1)/2$ and $q' = (q-1)/2$, we get

$$fq - 1 = (2f' + 1)(2q' + 1) - 1 = 4f'q' + 2f' + 2q'$$

Now,

$$\frac{fq+1}{2} = 2f'q' + f' + q'$$
$$\Rightarrow -\frac{(w+1)}{2} = \frac{fq+1}{2} = f' + q' (\text{mod } 2)$$
$$\Rightarrow -\frac{(w+1)}{2} = \frac{f-1}{2} + \frac{q-1}{2} (\text{mod } 2)$$

Multiplying both sides by $(w-1)/2$, we get

$$-\frac{w+1}{2}\frac{w-1}{2} = \frac{f-1}{2}\frac{w-1}{2} + \frac{q-1}{2}\frac{w-1}{2} (\text{mod } 2)$$

Since, $(w+1)/2$ and $(w-1)/2$ are consecutive integers, their product is even and we have:

$$-\frac{f-1}{2}\frac{w-1}{2} = \frac{q-1}{2}\frac{w-1}{2} (\text{mod } 2)$$

Since, 1 (mod 2) $= -1$ (mod 2), we can remove the negative sign from the left side of the equation above. Thus,

$$\frac{f-1}{2}\frac{w-1}{2} = \frac{q-1}{2}\frac{w-1}{2} (\text{mod } 2)$$

Applying this to Equation 3.4, we get:

$$\left(\frac{q}{|w|}\right) = (-1)^{\frac{w-1}{2}\frac{q-1}{2}} \tag{3.5}$$

Now, when $w = p$ and $\left(\frac{w}{q}\right) = \left(\frac{p}{q}\right) = 1$, we have:

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

When $w = -p$ and $\left(\frac{w}{q}\right) = \left(\frac{-p}{q}\right) = 1$, we have:

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

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

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

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

Since, the only two solutions for this equation are 1 and -1 and raising either of them to the -1 power does not change the result, we can remove the negative sign from the exponent without affecting the solution. Therefore, when $w = -p$ we also have:

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

This proves Case (i), when e and f are coprime to w. Next we look at the second possiblity:

2. f and e are divisible by w

Let $f = wf_1$, for some odd number $f_1 < f$ and let $e = we_1$ for some even number $e_1 < e$. Now we can rewrite Equation 3.3 as:

$$e_1^2 w^2 - w = wf_1 q \;\Rightarrow\; \frac{w(e_1^2 w - 1)}{w} = f_1 q$$
$$\Rightarrow e_1^2 w - 1 = f_1 q \quad \text{or} \quad e_1^2 w = 1 + f_1 q \tag{3.6}$$

Then, $e_1^2 w \equiv 1 \pmod{f_1}$ and $\left(\frac{e_1^2}{|f_1|}\right) = \left(\frac{w}{|f_1|}\right) = 1$. Moreover, $1^2 \equiv -f_1 q \pmod{w}$; therefore, $\left(\frac{-f_1}{|w|}\right) = \left(\frac{q}{|w|}\right)$. Since f_1 and w are both less than q, we can apply Equation 3.1 and get:

$$\left(\frac{|f_1|}{|w|}\right) = (-1)^{\frac{|w-1|}{2}\frac{|f_1|-1}{2}} \left(\frac{|w|}{|f_1|}\right)$$
$$\Rightarrow \left(\frac{|f_1|}{|w|}\right) = (-1)^{\frac{|w|-1}{2}\frac{|f_1|-1}{2}}$$

Now, we can see that:

$$\left(\frac{q}{|w|}\right) = \left(\frac{-f_1}{|w|}\right) = \left(\frac{-1}{|w|}\right)\left(\frac{f_1}{|w|}\right)$$
$$\Rightarrow \left(\frac{q}{|w|}\right) = \left(\frac{-1}{|w|}\right)(-1)^{\frac{w-1}{2}\frac{f_1-1}{2}}$$
$$\Rightarrow \left(\frac{q}{|w|}\right) = (-1)^{\frac{w-1}{2}}(-1)^{\frac{w-1}{2}\frac{f_1-1}{2}} = (-1)^{(\frac{w-1}{2})+(\frac{w-1}{2}\frac{f_1-1}{2})}$$

Therefore, now we have:

$$\left(\frac{q}{|w|}\right) = (-1)^{\frac{f_1+1}{2}\frac{w-1}{2}} \tag{3.7}$$

We know that e_1 is even, therefore $e_1^2 \equiv 0 \pmod 4$. Now from Equation 3.6 we have $e_1^2 w \equiv 0 \pmod 4 \equiv f_1 q + 1 \pmod 4$. Since, both f_1 and q are odd $f_1 q + 1 \equiv 0 \pmod 4$, if and only if one of f_1 or q is of the form $4M + 1$ and the other is of the form $4M + 3$. In either case we have:

$$\frac{f_1 + 1}{2} \equiv \frac{q - 1}{2} \pmod 2$$

Applying this to Equation 3.7, we get:

$$\left(\frac{q}{|w|}\right) = (-1)^{\frac{q-1}{2}\frac{w-1}{2}} \tag{3.8}$$

Now we can see that Equation 3.8 is analogous to Equation 3.5 above and holds true for both $w = p$ and $w = -p$. This concludes the proof for Case (i). Now we look at Case (ii).

In Case (ii) we need to show that when q is of the form $4M + 1$ and $\left(\frac{p}{q}\right) = -1$ and p is not a quadratic residue mod q, then q is also a non residue mod p and $\left(\frac{q}{p}\right) = -1$. In order to prove this, we will first prove the following lemma give by Gauss.

Lemma 3.2. *If q is a prime of the form $4N + 1$, there exists an odd prime $p' < q$ for which $\left(\frac{q}{p'}\right) = -1$.*

Proof.

1. This is apparent when q is of the form $8N + 5$. In this case, $\frac{q+1}{2}$ is of the form $4N + 3$. Now since, not all of its prime factors can be of the form $4N + 1$. There must be a prime factor p' of the form $4N + 3$, which divides $q + 1$ such that $q + 1 \equiv 0 \pmod{p'}$ and $q \equiv -1 \pmod{p'}$. Thus:

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

2. When q is of the form $8N + 1$, if we assume that q is a quadratic residue of every odd prime less than $2m + 1 < q$. Then since we know from Theorem 2.26 that $\left(\frac{2}{q}\right) = 1$, we can see that q is also a quadratic residue of every positive integer which is a product of numbers $\leq 2m + 1$. Now if $M = 1 \cdot 2 \cdot 3 \cdots 2m(2m + 1)$, then, the congruence $x^2 \equiv q \pmod{M}$ is solvable. Let $k = x$ be one of its solutions, then k and q are relatively prime to M, and:

$$(k^2 - 1^2) \cdots (k^2 - m^2) \equiv (q - 1^2) \cdots (q - m^2) (\text{mod } M)$$

Moreover,

$$k \cdot (k^2 - 1^2) \cdots (k^2 - m^2) \equiv (k+m)(k+m-1) \cdots (k+1)k(k-1) \cdots (k-(m-1))(k-m) (\text{mod } M)$$

The right side of the equation is a product of $(2M+1)$ consecutive integers, it must be divisible by M, thus the product:

$$\frac{(q-1^2)(q-2^2)\cdots(q-m^2)}{1\cdot 2\cdots(2m+1)}$$

is an integer. Furthermore, since $(2m+1)!$ can be rewritten as:

$$[(m+1)-m]\cdot[(m+1)-(m-1)]\cdots[(m+1)-1]\cdot[(m+1)-0]$$

$$\cdot[(m+1)+m]\cdot[(m+1)+(m-1)]\cdots[(m+1)+1]$$

$$\Rightarrow (m+1)[(m+1)^2-m^2]\cdots[(m+1)^2-1^2]$$

Therefore, the following is an integer:

$$\frac{1}{m+1}\frac{q-1^2}{(m+1)^2-1^2}\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2} \tag{3.9}$$

Now, if we choose $m=[\sqrt{q}]$ to be the largest integer less than $\sqrt{q}$, such that $m<\sqrt{q}<m+1$, then $m^2<q<(m+1)^2$, and every factor of the product in Equation 3.9 is a proper fraction, which is a contradiction. Furthermore, since q is of the form $8N+1$, and the smallest possible prime of that form is 17, $q\geq 17$, and it is apparent that $8<(q-3)^2$. Then, $4q<q^2-2q+1=(q-1)^2$, and $2\sqrt{q}<q-1$ or $2\sqrt{q}+1<q$. Since we chose $m=[\sqrt{q}]$ to be the largest integer less than $\sqrt{q}$, it follows that $2m+1<q$. Thus, there must exist some prime $p'<2m+1<q$, which is a quadratic non residue of q if q is of the form $8M+1$. This completes the proof for Lemma 3.2. □

Now, if $q=4N+1$, there is an odd prime $p'<q$ with $\left(\frac{q}{p'}\right)=-1$, then $\left(\frac{p'}{q}\right)$ must also be -1. If $\left(\frac{p'}{q}\right)=1$, then we can apply Case (i), and we get:

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

This contradicts the assumption that $\left(\frac{q}{p'}\right)=-1$. In order to complete the proof of Case (ii), we only need to show that if there exists another prime $p<q$ separate from the existing prime p', such that $\left(\frac{p}{q}\right)=-1$, then also $\left(\frac{q}{p}\right)=-1$ or in other words:

$$\left(\frac{q}{pp'}\right)=1 \tag{3.10}$$

Now we know that $\left(\frac{p'}{q}\right) = -1$, and by assumption we have $\left(\frac{p}{q}\right) = -1$, thus $\left(\frac{pp'}{q}\right) = +1$, and the congruence $x^2 \equiv pp' \pmod{q}$ is solvable. Then the solutions for x are x_0 and $q - x_o$, let e be the solution which is even, then:

$$e^2 = pp' + fq \tag{3.11}$$

where f is an odd integer less than q. Now we can look at the following cases:

1. e and f are not divisible by p or p'.
Then we can see that $e^2 \equiv pp' \pmod{f}$, and $\left(\frac{pp'}{|f|}\right) = 1$. Moreover, $e^2 \equiv qf \pmod{pp'}$, therefore, $\left(\frac{qf}{pp'}\right) = 1$, and $\left(\frac{f}{pp'}\right) = \left(\frac{q}{pp'}\right)$. Now when $f > 0$ we get:

$$\left(\frac{q}{pp'}\right) = \left(\frac{f}{pp'}\right) = (-1)^{\frac{(pp'-1)}{2}\frac{(f-1)}{2}} \tag{3.12}$$

Furthermore, when f is negative, we get:

$$\left(\frac{q}{pp'}\right) = \left(\frac{f}{pp'}\right)\left(\frac{-1}{pp'}\right) = (-1)^{\frac{(pp'-1)}{2}\frac{(-f-1)}{2}}(-1)^{\frac{(pp'-1)}{2}}$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{(pp'-1)}{2}\frac{(-f+1)}{2}} = (-1)^{\frac{(pp'-1)}{2}\frac{(f-1)}{2}}$$

Since e is even, we have $-pp' \equiv fq \pmod{4}$. Moreover, since $q \equiv 1 \pmod{4}$, $-pp' \equiv f \pmod{4}$:

$$\frac{f-1}{2} \equiv -\frac{pp'+1}{2} \equiv \frac{pp'+1}{2} \pmod{2}$$

Since $\frac{pp'+1}{2}$ and $\frac{pp'-1}{2}$ are consecutive integers, their product is even. Thus replacing $\frac{f-1}{2}$ with $\frac{pp'+1}{2}$ in Equation 3.12 gives us an even exponent and yields:

$$\left(\frac{q}{pp'}\right) = 1$$

which is what we wanted to show.

2. e and f are divisible by p', but not p.
Then we can set $f = p'f_1$, and $e = p'e_1$. Then Equation 3.11 takes the form:

$$p'e_1^2 - p = f_1 q \tag{3.13}$$

From Equation 3.13 we see that $p'e_1^2 \equiv p \pmod{f_1}$. Therefore,

$$\left(\frac{p'e_1^2}{|f_1|}\right) = \left(\frac{p'}{|f_1|}\right)\left(\frac{e_1^2}{|f_1|}\right) = \left(\frac{p'}{|f_1|}\right) = \left(\frac{p}{|f_1|}\right)$$

Now, $\left(\frac{p'p}{|f_1|}\right) = 1$. Moreover,

$$\left(\frac{f_1 q}{p}\right) = \left(\frac{p'}{p}\right) = \left(\frac{-p}{p'}\right)$$

Also,

$$\left(\frac{q}{pp'}\right) = \left(\frac{|f_1|}{pp'}\right)^2 \left(\frac{q}{pp'}\right) = \left(\frac{|f_1|}{pp'}\right)\left(\frac{|f_1|q}{pp'}\right)$$

Since $|f_1|$ and pp' are less than q, by our assumption the generalized quadratic reciprocity law holds for $|f_1|$ and pp', and we get:

$$\left(\frac{|f_1|}{pp'}\right) = (-1)^{\frac{|f_1|-1}{2}\frac{pp'-1}{2}} \left(\frac{pp'}{|f_1|}\right) = (-1)^{\frac{|f_1|-1}{2}\frac{pp'-1}{2}}$$

Now if $f_1 > 0$, we have:

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{f_1-1}{2}\frac{pp'-1}{2}} \left(\frac{f_1 q}{p}\right)\left(\frac{f_1 q}{p'}\right)$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{f_1-1}{2}\frac{pp'-1}{2}} \left(\frac{p'}{p}\right)\left(\frac{-p}{p'}\right)$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{f_1-1}{2}\frac{pp'-1}{2}+\frac{p'-1}{2}} \left(\frac{p'}{p}\right)\left(\frac{p}{p'}\right)$$

Since the quadratic reciprocity law also holds for p and p', we get:

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{f_1-1}{2}\frac{pp'-1}{2}+\frac{p+1}{2}\frac{p'-1}{2}} \tag{3.14}$$

If $f_1 < 0$, we have:

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{-f_1-1}{2}\frac{pp'-1}{2}} \left(\frac{-1}{p}\right)\left(\frac{-1}{p'}\right)\left(\frac{f_1 q}{p}\right)\left(\frac{f_1 q}{p'}\right)$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{-f_1-1}{2}\frac{pp'-1}{2}+\frac{p-1}{2}+\frac{p'-1}{2}} \left(\frac{p'}{p}\right)\left(\frac{-p}{p'}\right)$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{-f_1-1}{2}\frac{pp'-1}{2}+\frac{p-1}{2}+\frac{p-1}{2}\frac{p'-1}{2}}$$

$$\Rightarrow \left(\frac{q}{pp'}\right) = (-1)^{\frac{f_1+1}{2}\frac{pp'-1}{2}+\frac{p-1}{2}\frac{p'+1}{2}}$$

Since e_1 in Equation 3.13 is even and $q \equiv 1$ (mod4), we get $f_1 \pmod 4 \equiv -p \pmod 4$. Thus:

$$\frac{f_1 - 1}{2} \equiv \frac{-p-1}{2} (\text{mod } 2)$$

Now,

$$\frac{f_1-1}{2}\frac{pp'-1}{2}+\frac{p'-1}{2}\frac{p-1}{2}\equiv-\frac{p+1}{2}\frac{pp'-1}{2}+\frac{p'-1}{2}\frac{p+1}{2}$$
$$\frac{p+1}{2}\frac{1-pp'}{2}+\frac{p'-1}{2}\equiv\frac{p+1}{2}\frac{-pp'+p'}{2}\equiv-p'\frac{p+1}{2}\frac{p-1}{2}$$

Moreover,

$$\frac{f_1+1}{2}\equiv\frac{p-1}{2}(\text{mod } 2)$$

Therefore,

$$\frac{f_1+1}{2}\frac{pp'-1}{2}+\frac{p-1}{2}\frac{p'+1}{2}\equiv\frac{p-1}{2}\frac{pp'-1}{2}+\frac{p-1}{2}\frac{p'+1}{2}$$
$$\frac{p-1}{2}\frac{pp'+p'}{2}\equiv\frac{p-1}{2}p'\frac{p+1}{2}\equiv p'\frac{p-1}{2}\frac{p+1}{2}$$

Since $\frac{p+1}{2}$ and $\frac{p-1}{2}$ are consecutive integers, their product is even. Thus in both cases where either $f1>0$ or $f_1<0$, we have:

$$\left(\frac{q}{pp'}\right)=1$$

which is what we wanted to show.

3. Since in the proof of 2. above, we did not utilize the fact that $\left(\frac{q}{p'}\right)=-1$, we can see that simply interchanging p' with p in the proof above will similarly prove the case where e and f are divisible by p, but not p'.

4. The final case is where e and f are divisible by both p and p'.
Let $f=pp'f_1$, and $e=pp'e_1$. Then Equation 3.11 takes the form:

$$pp'e_1^2-1=f_1q \tag{3.15}$$

From Equation 3.15, we can see that:

$$1=\left(\frac{pp'e_1^2}{|f_1|}\right)=\left(\frac{pp'}{|f_1|}\right)\text{ and }\left(\frac{-f_1q}{pp'}\right)=1$$

Thus, we can see that:

$$\left(\frac{q}{pp'}\right)=\left(\frac{-f_1}{pp'}\right)=\left(\frac{-1}{pp'}\right)\left(\frac{f_1}{pp'}\right)$$

Since, f_1 and pp' are less than q, we can apply the generalized quadratic reciprocity law and we get:

$$\left(\frac{|f_1|}{pp'}\right) = \left(\frac{pp'}{|f_1|}\right)(-1)^{\frac{|f_1|-1}{2}\frac{pp'-1}{2}}$$

Thus when $f_1 > 0$,

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{pp'-1}{2}+\frac{f_1-1}{2}\frac{pp'-1}{2}} = (-1)^{\frac{f_1+1}{2}\frac{pp'-1}{2}} \tag{3.16}$$

And when $f_1 < 0$,

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{pp'-1}{2}+\frac{pp'-1}{2}+\frac{-f_1-1}{2}\frac{pp'-1}{2}} = (-1)^{\frac{f_1+1}{2}\frac{pp'-1}{2}}$$

Now, since e_1 is even and $q \equiv 1 \pmod 4$, we can see from Equation 3.15 that $f_1 \equiv -1 \pmod 4$, thus $\frac{f_1+1}{2}$ is even and consequently the exponent is even in both cases for f_1. Therefore,

$$\left(\frac{q}{pp'}\right) = 1$$

which is what we wanted to show.

This concludes the proof for Case (ii), and hence completes Gauss's first proof of the Law of Quadratic Reciprocity by induction. □

Although Gauss looked at each of the eight cases outlined at the beginning of this proof in his seminal demonstration, here we chose a slightly smaller version of the proof, which allowed us to collapse several of these cases. This by no means takes aways from the purpose of this demonstration, which was to show that such a fundamental theorem of number theory could be proven via observation and the very basic technique of induction. We also add that while Gauss listed each of the eight cases separately in his own proof in *Disquisitiones Arithmeticae*, he also chose to forgo repetition of the proof in cases where the strategy was the same as one of the earlier cases. This brings up an important insight that can be gleaned from this proof. Despite the fact that we were able to collapse our version of the proof into two mutually exclusive cases, these two cases still presented us with several distinctions and subdivisions. Yet many of these subdivisions utilized very similar strategies, specifically, they entailed equating the quadratic character of q to another odd prime less than q and then determining whether the resulting combination

of exponents would be even or odd. This should suggest that it would be possible to further collapse this proof and identify approaches which are even shorter.

Indeed, in his second proof Gauss used the genus theory of quadratic binary forms, which consisted of establishing a bound on the number of existing genera of the quadratic forms of a given determinant and subsequently investigating the only two cases for the primes p and q. The resulting proof is far shorter than his first proof. We will not look at his second proof here, but the original proof can be found in *Disquisitiones Arithmeticae*, and another version of it can be seen in *The Quadratic Reciprocity Law: A Collection of Classical Proofs*. Instead we will investigate Gauss's fourth proof, which made use of quadratic Gauss sums and eventually helped advance the field of algebraic number theory. The first step of our journey showed us how observation and induction helped establish one of the fundamental theorems of number theory. Next, we will look at how further attempts to refine and strengthen this theorem resulted in the discovery of new territories and gave rise to new features of the mathematical landscape.

3.3 Gauss's Fouth Proof of Quadratic Reciprocity

In his fourth proof Gauss used quadratic Gauss sums to investigate the Law of Quadratic Reciprocity. This proof extended the law of quadratic reciprocity to cyclotomic fields and in so doing contributed greatly to the development of this field. We have already defined Gauss Sums and given some of their fundamental characteristics in the previous chapter. In order to give the proof of quadratic reciprocity, we first need to prove two additional propositions, which will then allow us to proceed with the complete proof using Gauss Sums. For more information on this proof please refer to the following texts: [Bau15] [Lan94] [Lem00]

Proposition 3.3. *For any integer a,*

$$G_a = \left(\frac{a}{p}\right) G_1$$

Proof.

1. When $p \mid a$, $a \equiv 0 \pmod{p}$ and:

$$G_0 = G_1 \left(\frac{0}{p}\right) = 0$$

2. In the more difficult case, where $p \nmid a$, we need to show that

$$\left(\frac{a}{p}\right) G_a = G_1 \Rightarrow G_a = \left(\frac{a}{p}\right) G_1$$

Now,

$$\left(\frac{a}{p}\right) G_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta_p^{an}$$

Since $p \nmid a$, we can see that the product an will permute all the numbers $0 < n < p$ modulo p. Therefore, the sum:

$$\sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta_p^{an} = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{n} = G_1$$

□

Example 3.4. *Let $a = 3$ and $p = 5$, then:*

$$G_3 = \sum_{n=0}^{4} \left(\frac{n}{5}\right) \zeta_5^3 = \left(\frac{1}{5}\right) \zeta_5^3 + \left(\frac{2}{5}\right) \zeta_5 + \left(\frac{3}{5}\right) \zeta_5^4 + \left(\frac{4}{5}\right) \zeta_5^2$$

$$G_3 = \zeta_5^3 - \zeta_5 - \zeta_5^4 + \zeta_5^2 \tag{3.17}$$

$$G_1 = \sum_{n=0}^{4} \left(\frac{n}{5}\right) \zeta_5^n = \left(\frac{1}{5}\right) \zeta_5 + \left(\frac{2}{5}\right) \zeta_5^2 + \left(\frac{3}{5}\right) \zeta_5^3 + \left(\frac{4}{5}\right) \zeta_5^4$$

$$G_1 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \tag{3.18}$$

We know that $\left(\frac{3}{5}\right) = -1$. Therefore, from Equations 3.17 and 3.18, we can see that:

$$G_3 = (-1) G_1$$

Proposition 3.5. *For any integer a, such that $p \nmid a$:*

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

Proof.

Since $p \nmid a$, from the definition of Gauss Sum, we have:

$$G_a^2 = \sum_{a,b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta_p^{a+b}$$

Moreover, because $p \nmid a, b$ and both a and b range over $1, \ldots, p-1$. We can rewrite $b \equiv ac \pmod{p}$ (where c also ranges over $1, \ldots, p-1$). Then:

$$G_a^2 = \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a^2 c}{p}\right) \zeta_p^{a+ac}$$

Since $\left(\frac{a^2}{p}\right) = 1$, we can further simplify to:

$$G_a^2 = \sum_{c=1}^{p-1} \left(\sum_{a=1}^{p-1} \zeta_p^{a(1+c)}\right) \left(\frac{c}{p}\right)$$

Now if $1 + c \not\equiv 0 \bmod p$, then the sum of the series $1, \zeta_p^{(1+c)}, \zeta_p^{2(1+c)}, \ldots, \zeta_p^{(p-1)(1+c)} = \frac{\zeta_p^p - 1}{\zeta_p - 1} = 0$. Thus,

$$\sum_{a=1}^{p-1} \zeta_p^{a(1+c)} = -1$$

Now if $1 + c \equiv 0 \bmod p$, then we are summing $p - 1$ ones, and:

$$\sum_{a=1}^{p-1} \zeta_p^{a(1+c)} = p - 1$$

Here we note that $c = p - 1 \leftrightarrow 1 + c \equiv 0 \bmod p$. Therefore,

$$G_a^2 = \sum_{c=1}^{p-1} \left(\sum_{a=1}^{p-1} \zeta_p^{a(1+c)}\right) \left(\frac{c}{p}\right) = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + (p-1)\left(\frac{-1}{p}\right)$$

We can sum from 1 to $p - 1$, if we add $\left(\frac{-1}{p}\right)$. Therefore, we get:

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

Here we can see that the summation on the left is equal to 0, by Theorem 2.22. Moreover, $\left(\frac{-1}{p}\right) = -1^{\frac{(p-1)}{2}}$, by Theorem 2.21. Thus we have:

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

□

Example 3.6. *Let $p = 3$ and $a = 1$, then:*

$$G_1^2 = -1^{\frac{(3-1)}{2}} 3 = -3$$

Using the definition of Gauss Sum, we get:

$$G_1 = \left(\frac{1}{3}\right)\zeta_3 + \left(\frac{2}{3}\right)\zeta_3^2 = \zeta_3 - \zeta_3^2$$

We know that by definition of the n^{th} root of unity $\zeta_3^3 = 1$ or $\zeta_3^3 - 1 = 0$. Moreover, $x^3 - 1 = (x-1)(x^2 + x + 1) = 0$, therefore $x^2 = -x - 1$. Substituting x for ζ_3 we get $\zeta_3^2 = -\zeta_3 - 1$. Now,

$$G_1 = \zeta_3 - \zeta_3^2 = \zeta_3 + \zeta_3 + 1 = 2\zeta_3 + 1$$

and:

$$G_1^2 = (2\zeta_3 + 1)^2 = 4\zeta_3^2 + 4\zeta_3 + 1$$

Substituting for $\zeta_3^2 = -\zeta_3 - 1$ again, we get:

$$G_1^2 = -4\zeta_3 - 4 + 4\zeta_3 + 1 = -3$$

Using Propositions 3.3 and 3.5, we can now prove the law of Quadratic Reciprocity via Gauss Sums. In order to prove the law we will calculate G_1^q in two different ways and show them to be equal. Let us restate the theorem here before we begin the proof:

Theorem 3.7. *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.

i) Let $p^* = (-1)^{\frac{p-1}{2}} p$. Let $G = G_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\zeta_p^n \in \mathbb{C}$. Then from Proposition 3.5 we know that:

$$G^2 = p^*$$

Moreover, from Corollary 2.18 we know that:

$$\left(\frac{p^*}{q}\right) \equiv (p^*)^{\frac{q-1}{2}} (\text{mod } q)$$

Now, we can see that:

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

Thus,

$$G^q \equiv (p^*)^{\frac{q-1}{2}} \cdot G(\text{mod } q) \equiv \left(\frac{p^*}{q}\right) \cdot G(\text{mod } q) \tag{3.19}$$

ii) $G = G_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n \in \mathbb{C}$. Therefore,

$$G^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n\right)^q = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta_p^{qn}$$

Since, q is an odd prime, we know that $\left(\frac{n}{p}\right)^q \equiv \left(\frac{n}{p}\right)$. Therefore:

$$G^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{qn} \equiv G_q$$

Now we can apply Proposition 3.3 to the equation above and we get:

$$G^q \equiv G_q \equiv \left(\frac{q}{p}\right) \cdot G(\text{mod } q) \tag{3.20}$$

By combining Equations 3.19 and 3.20, we can see that:

$$G^q \equiv \left(\frac{p^*}{q}\right) \cdot G(\text{mod } q) \equiv \left(\frac{q}{p}\right) \cdot G(\text{mod } q)$$

By cancelling G from both sides, we have:

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right)$$

Since both residue symbols are ± 1 and q is odd, we can say that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ and:

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

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

Multiplying both sides by $\left(\frac{p}{q}\right)$ we get:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{3.21}$$

which is what we wanted to show.

□

The proof using Gauss sums can also be restated using elementary techniques from basic algebraic number theory. In particular, one can use Galois theory and algebraic number theory to first define the following concepts: quadratic subfields of cyclotomic fields, the spilitting of prime ideals and the Frobenius element. Then, using these properties one can then produce a relatively simple proof of quadratic reciprocity, similar in principle to the one above. Interestingly, these theories did not fully develop until the late 19th century (after Gauss' time). Yet Gauss was able to utilize Gauss sums to construct a unique quadratic subfield and indetify the splitting of the prime q, without using any of the definitions or language from either of these theories. Gauss had done some early work with cyclotomic fields in connection to the construction of a 17-gon. His later work, which generalized the law of quadratic reciprocity to cyclotomic fields, helped demonstrate properties which eventually became an important part of the theory of cyclotomy. This may shed some light on Gauss' motivation to explore his "fundamental theorem" using different techniques. He was not simply looking for more arguments in support of his theorem, instead his ultimate goal was to explore new branches of mathematics as he worked through his various proofs, in order to identify techniques and strategies which would eventually form the basis of modern number theory.

Next, we will look at a variation of Gauss' third proof of the law of quadratic reciprocity. Gauss considered his third proof to be the most direct and natural of the eight proofs of this theorem provided by him. This third proof greatly simplifies and reduces the number of steps required to acheive the desired conclusion in his first proof. However, rather than look at the proof provided by Gauss himself, here we will instead focus on a further version on Gauss' third proof provided by Gotthold Eisenstein. Although Gauss' third proof was simpler and more direct than his first proof, it utilized Gauss' lemma and required several technical manipulations before his lemma could be successfully applied. In the version presented here, Eisenstein follows a very similar outline to the one used by Gauss; however, is able to use a geometric transformation to greatly simplify some of the steps, which otherwise required Gauss to consider several different cases to arrive at the desired conclusion. For more information on this proof, please refer to the following sources: [Bau15] [Bur07] [LP94]

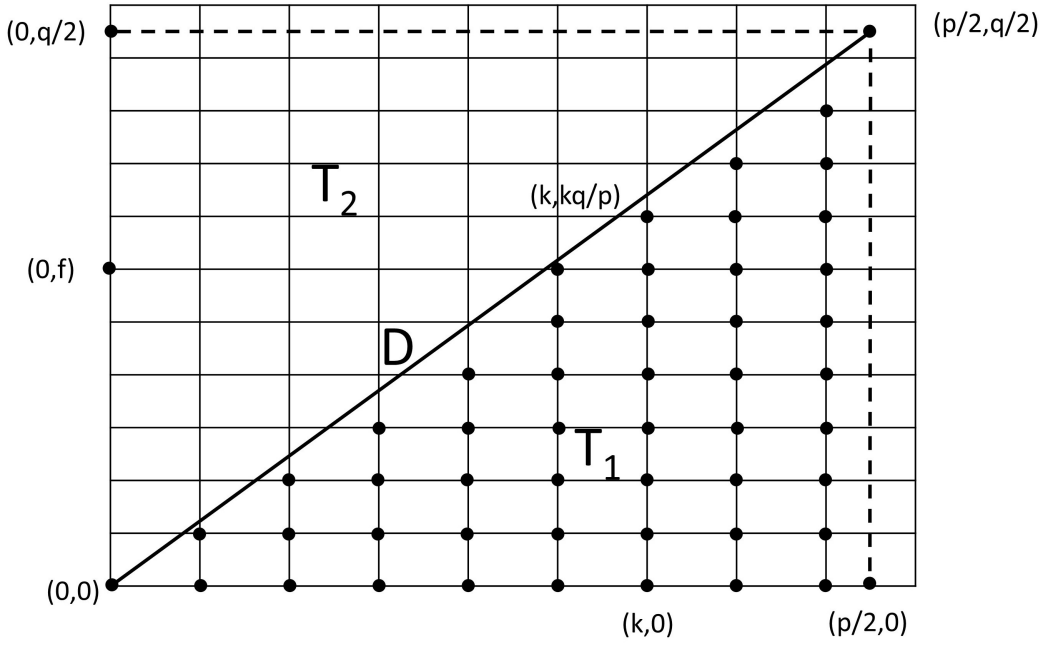

Figure 3.1: Eisenstein's Lattice Points

3.4 Eisenstein's Geometric Proof of Quadratic Reciprocity

The strategy for Eisenstein's proof of the law of quadratic reciprocity will be as follows. First, we will introduce a geometric coordinate system on the cartesian xy plane using familiar notation. We will then show how equations that are very visually apparent from this geometric system relate to Gauss's lemma and in the process we will arrive at the desired conclusion. Let us restate the theorem here before we begin our proof.

Theorem 3.8. *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. Consider the rectangle R in figure 3.1 whose vertices are $(0,0)$, $(p/2,0)$, $(0,q/2)$ and $(p/2,q/2)$.

Here the diagonal D, which goes from $(0,0)$ to $(p/2,q/2)$ has the equation $y = (q/p)x$ or $py = qx$. Let us define *lattice points* as point whose coordinates have integer values. Then we can see that none of the lattice points inside the rectangle R lie on

the diagonal D. For if that were the case, then p would divide qx. However, this is not possible because we know that $\gcd(p,q) = 1$, and $1 \leq x \leq \frac{p-1}{2}$. Let us now divide the rectangle R into two symmetrical triangles T_1 and T_2.

Now, we can use the floor function $[x]$, where $[x]$ represents the largest integer less than the number x, to count the total number of lattice points that are below the diagonal D and contained within the triangle T_1. We can see that for each value of k, the corresponding point on the diagonal can be calculated using the equation $y = kq/p$. Since we have already determined that the diagonal D does not contain any lattice points, then the lattice points in T_1, corresponding to each value of k, are less than $y = kq/p$ or equal to $\left[\frac{kq}{p}\right]$. Thus the total number of lattice points in T_1 are:

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] \tag{3.22}$$

Since triangles T_1 and T_2 are symmetrical, it is apparent that the total number of lattice points in T_2 can be calculated similarly, by switching p with q and k with f. Thus the total number of lattice points in T_2 are:

$$\sum_{f=1}^{(q-1)/2} \left[\frac{fp}{q}\right] \tag{3.23}$$

Now we will give a lemma, which shows that the summations in Equations 3.22 and 3.23 are equivalent modulo 2, to the exponent n seen in Gauss' Lemma (Theorem 2.24). That is:

Lemma 3.9. *Let p and q be odd primes and let $gcd(q,p) = 1$. Then,*

$$\left(\frac{q}{p}\right) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$$

or in other words:

$$n = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]$$

Proof. Let us consider the set:

$$S = \left\{q, 2q, \ldots, \frac{p-1}{2}q\right\}$$

If we divide each multiple of q by p, we get:

$$kq = y_k p + t_k \quad 0 < t_k < p - 1$$

Now, $kq/p = y_k + t_k/p$, here we know that y_k is an integer whose value is equal to $\left[\frac{kq}{p}\right]$. Thus, for $1 \leq k \leq \frac{p-1}{2}$, we may then write kq in the form:

$$kq = \left[\frac{kq}{p}\right] p + t_k \tag{3.24}$$

Here if the remainder $t_k < p/2$ then we say that it is one of the integers $r_1, \ldots, r_m$; on the other hand if $t_k > p/2$, then it belongs to the set $s_1, \ldots, s_n$. Now we can see that the sum for $1 \leq k \leq (p-1)/2$ in Equation 3.24 is:

$$\sum_{k=1}^{(p-1)/2} kq = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k \tag{3.25}$$

We already saw in the proof of Gauss' Lemma (Theorem 2.24), that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m \qquad p - s_1, \ldots, p - s_n$$

are simply a rearrangement of the numbers $1, 2, \ldots, (p-1)/2$. Thus we can write:

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = np + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \tag{3.26}$$

We can now subtract Equation 3.26 from Equation 3.25 and we are left with:

$$(q-1) \sum_{k=1}^{(p-1)/2} k = p \left(\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] - n \right) + 2 \cdot \sum_{k=1}^{m} r_k \tag{3.27}$$

Since, p and q are odd primes, we know that $p \equiv q \equiv 1 \pmod 2$. Therefore,

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] - n \right) \pmod 2 + 0 \cdot \sum_{k=1}^{m} r_k$$

which then gives us:

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] \pmod 2 \tag{3.28}$$

or

$$\left(\frac{q}{p}\right) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]} \tag{3.29}$$

□

Thus from Lemma 3.9, and Equations 3.22 and 3.23 we have:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{f=1}^{(q-1)/2}\left[\frac{fp}{q}\right]} \tag{3.30}$$

We are now nearly done with our proof. Recall the rectangle R from figure 3.1.

We know that the summations in Equations 3.22 and 3.23 represent the total number of lattice points in the triangles T_1 and T_2 respectively. We also know that none of the lattice points in R lie on the diagonal D, which divides R into the the triangles T_1 and T_2. Thus the total number of lattice points in R is equal to the sum of the lattice points in T_1 and T_2 (which is exactly the exponent in Equation 3.30). Looking at figure 3.11, it should be apparent that the total number of lattice points in R is:

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

Thus:

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{f=1}^{(q-1)/2}\left[\frac{fp}{q}\right] = \frac{(p-1)}{2}\frac{(q-1)}{2} \tag{3.31}$$

Combining Equations 3.30 and 3.31, we get the desired result:

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

□

This completes Eisenstein's simplification of Gauss' third proof of quadratic reciprocity based on Gauss' lemma. Gauss' version of this proof is longer and a bit more technical; however Eisenstein was able to greatly simplify it when he realized that the exponent in Gauss' lemma can be restated as the sum of lattice points on a geometric coordinate system. We saw this result in Lemma 3.9, which can be referred to as Eisenstein's Lemma. Once we accept the truth of this lemma, the result of quadratic reciprocity becomes very apparent simply by looking at the rectangle R with coordinates bounded by $p/2$ and $q/2$. The product is a streamlined and simple proof of Gauss' fundamental theorem, which is one of the most common proofs of this law, and often used as the introductory proof for this theorem in many elementary number theory texts.

3.5 Rousseau's Proof of Quadratic Reciprocity

We have now looked at three iterations of Gauss' original proofs of the law of quadratic reciprocity. All of these proofs were developed during early to mid 1800s and greatly shaped the field of number theory. This process of proving also helped set the basis for new disciplines in mathematics, such as the field of cyclotomy. Next, we will switch gears and look at one of the most recent proofs of the law of quadratic reciprocity. This proof was described by Rousseau in 1991 [Rou91], it does not rely on Gauss' lemma or even Eisenstein's lattice counting, but instead utilizes only Wilson's theorem, Euler's formula and the Chinese Remainder Theorem to directly prove quadratic reciprocity.

The strategy for this proof is rather simple and utilizes the construction of ring isomorphisms formed by the cyclic group of integers modulo prime numbers. First we describe a normal subgroup for integers modulo the prime numbers p and q, and then we calculate the product of all the coset representatives for this subgroup using two different strategies. The end result is a very short and direct proof of the law of quadratic reciprocity. Let us restate the theorem once again, before we proceed with the proof:

Theorem 3.10. *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 us define $(\mathbb{Z}/p\mathbb{Z})^*$ as the multiplicative group of non-zero integers modulo a prime p. Now cosider the group $G = (\mathbb{Z}/p\mathbb{Z})^* * (\mathbb{Z}/q\mathbb{Z})^*$ for odd primes p and q. We know that $H = \{(1,1),(-1,-1)\}$ is a normal subgroup of G. (It is clear that H is a group in and of itself, and as such a subgroup of G. Moreover, it is normal since component-wise multiplication of any element of $(a,b) \in G$ with H from either the right or the left side will yield the same results.) Let $A = G/H$ the quotient group, then we can find the product of all elements of A, by listing out and multiplying all the coset representatives for H.

We know that any element $(a,b) \in G$ can be written as $(a, \pm b)$, where $1 \leq a \leq p-1$ and $1 \leq b \leq \frac{q-1}{2}$. Moreover, since $(\mathbb{Z}/p\mathbb{Z})^*$ is a group and both a and $-a$ are in $(\mathbb{Z}/p\mathbb{Z})^*$ for every value of a, multiplying a with 1 or -1 in H will not affect the first coordinate of these elements of G. Thus, we can list the set of coset representatives for H as: $S = \{(x,y) \mid 1 \leq x \leq p-1, 1 \leq y \leq \frac{q-1}{2}\}$. Taking a product of all the element of S gives us:

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

Since, we know that in $(\mathbb{Z}/q\mathbb{Z})^*$,

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

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

Thus the product of all elements of S can be rewritten as:

$$\left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{q-1}{2}\frac{p-1}{2}}(q-1)!^{\frac{p-1}{2}}\right) \tag{3.32}$$

We know from the Chinese Remainder Theorem (2.52), that the group $G = (\mathbb{Z}/p\mathbb{Z})^* * (\mathbb{Z}/q\mathbb{Z})^*$ is isomorphic to the group $(\mathbb{Z}/pq\mathbb{Z})^*$, which is the set of elements from 1 to pq, which are relatively prime to pq. Let us define the set: $T = \{(k \bmod p, k \bmod q) \mid$

$k = 1, 2, \ldots, \frac{pq-1}{2}$; $\gcd(k, pq) = 1\}$, which maps $k \to (k \bmod p,\ k \bmod q)$. Since, multiplication of T with H will generate all the elements of G, it is clearly another set of coset representatives.

Now, let us look at the product of all elements $(x, y) \in T$. Where x is the product of all k modulo p and y is the product of all k taken modulo q. Since $\gcd(p, q) = 1$, the product of k modulo p is:

$$x \equiv \frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1}\left(\frac{q-1}{2}-1\right)p+i\right)\left(\prod_{i=1}^{p-1}\left(\frac{q-1}{2}\right)p+i\right)}{(1\cdot q)(2\cdot q)\cdots(\frac{pq-1}{2}\cdot q)}$$

$$\Rightarrow x \equiv \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}$$

Using a similar product for $y \equiv k$ modulo q, we get:

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

Thus the product of all elements $(x, y) \in T$ is equal to:

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

Applying Euler's Criterion (Theorem 2.17), we get:

$$\left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) \tag{3.33}$$

We have already stated that the sets S and T, represent the same set of coset representatives for H in G, and as such, their products are equal. Therefore, we can put together Equations 3.32 and 3.33 to yield:

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

where $\alpha = \pm 1$. By equating the first coordinates we get $\alpha = \left(\frac{q}{p}\right)$, and by equating the second coordinates we get:

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

Multiplying both sides by $\left(\frac{p}{q}\right)$, we get the quadratic reciprocity law:

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

□

This completes Rousseau's proof of the law of quadratic reciprocity. An elegant proof in its own right, which does not depend on Gauss' Lemma or even Eisenstein's lattice counting. Instead it relies solely on some very basic priniciples of group theory. We see that by looking at the product of the coset representatives of the cyclic group of integers, modulo the odd primes p and q in two different ways we arrive directly at the conclusion of the quadratic reciprocity law. This strategy is reminiscent of the one we saw in Gauss' fourth proof of this law, where we calculated the Gauss sum using two different methods, and ended up with the law of quadratic reciprocity. Although the field of Group Theory as we know it today did not exist in Gauss' time, therefore this notation and these elementary definitions were not yet available to Gauss for his own proofs.

Chapter 4

Conclusion

.

The Law of Quadratic Reciprocity has played an important role in the development of number theory. While Gauss was the first to give a complete proof of this theorem, his predecessors Euler and Legendre had attempted to prove the law as well. Gauss eventually gave 8 different proofs of quadratic reciprocity, and with each attempt he explored new territories, along the way contributing greatly to the expansion and development of new areas in number theory. Following Gauss, other great mathematicians, including Eisenstein, Cauchy and Kronecker each gave their own proofs of this law, and in the process introduced new ways to approach this seemingly simple congruence relationship between two odd primes.

To date, there are over 300 different published proofs of the Law of Quadratic Reciprocity, with the latest one published as recently as 2014. Yet many more proofs may still exist. The search for higher reciprocity laws resulted in the development of algebraic number theory, and serves as the perfect example for how the inductive attitude and the pursuit of discovery has advanced the field of mathematics. Here we explored four different proofs of quadratic reciprocity and analyzed the strategies utilized in each attempt. We identified the differences and similarities in the different proofs and along the way deepened our understanding of the Law of Quadratic Reciprocity.

Bibliography

[Bau15] Oswald Baumgart. *The Quadratic Reciprocity Law: A Collection of Classical Proofs*. Springer International Publishing, Heidelberg, New York, 2015.

[Büh81] Walter Kaufmann Bühler. *Gauss: A Biographical Study*. Springer-Verlag, Berlin, New York, 1981.

[Bur07] David M Burton. *Elementary Number Theory*. McGraw-Hill Higher education. McGraw-Hill Higher Education, Boston, 6th edition, 2007.

[Dir91] P G L Dirichlet. *Lectures on Number Theory*. History of mathematics / History of mathematics. American Mathematical Society, 1991.

[GC86] Carl Friedrich Gauss and Arthur A. Clark. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986.

[Lan94] Serge Lang. *Algebraic Number Theory*. Applied Mathematical Sciences. Springer-Verlag, New York, 1994.

[Lem00] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*. Monographs in Mathematics. Springer-Verlag, Berlin, New York, 2000.

[LP94] Reinhard C. Laubenbacher and David J. Pengelley. Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem. *The College Mathematics Journal*, 25(1):29, jan 1994.

[Nag51] Trygve Nagell. *Introduction to Number Theory*. John Wiley & Sons, Inc., Uppsala, 1st edition, 1951.

[Pól54] George Pólya. *Induction and Analogy in Mathematics*. Mathematics and plausible reasoning. Princeton University Press, Princeton, 1954.

[Rom05] Steve Roman. *Field Theory*. Graduate Texts in Mathematics. Springer, New York, 2nd edition, 2005.

[Rou91] G Rousseau. On the quadratic reciprocity law. *Journal of the Australian Mathematical Society*, 51(03):423, dec 1991.

[Sti94] John Stillwell. *Elements of Algebra: Geometry, Numbers, Equations*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1994.