2019

Quadratic Reciprocity: Proofs and Applications

Awatef Noweafa Almuteri
University of Mississippi

QUADRATIC RECIPROCITY: PROOFS AND APPLICATIONS

THESIS

A Thesis
presented in partial fulfillment of requirements
for the degree of Master of Science
in the Department of Mathematics
The University of Mississippi

by

AWATEF ALMUTERI

May 2019

ABSTRACT

The law of quadratic reciprocity is an important result in number theory. The purpose of this thesis is to present several proofs as well as applications of the law of quadratic reciprocity. I will present three proofs of the quadratic reciprocity. We begin with a proof that depends on Gauss's lemma and Eisenstein's lemma. We then describe another proof due to Eisentein using the nth roots of unity. Then we provide a modern proof published in 1991 by Rousseau. In the second part of the thesis, we present two applications of quadratic reciprocity. These include special cases of Dirichlet's theorem on primes in arithmetic progressions and Fermat's theorem on sums of two squares.

ACKNOWLEDGEMENTS

I would like to thank my wonderful professor, Dr. Thi Hong L for providing me the opportunity to learn new valuable concepts in number theory and improving my writing skills. Without his support, I would have not made it where I am today.

I would also like to thank my committee members for their time and comments on my thesis.

I would further like to thank my friend Moriah Gibson for helping me with Latex and giving me comments to my thesis.

I would also like to thank the Saudi Arabian Cultural Mission for providing the funds to complete my education.

Finally, I would like to thank my family for their love and the continuous support they have given me throughout my time in graduate school.

TABLE OF CONTENTS

1 INTRODUCTION

The law of quadratic reciprocity is a fundamental result of number theory. Among other things, it provides a way to determine if a congruence $x^2 \equiv a \pmod{p}$ is solvable even if it does not help us find a specific solution.

Having a total of 246 proofs, the quadratic reciprocity Law can qualify as one of the more complex and mind-boggling laws in the natural sciences. During the period 17th - 20th centuries, there were several mathematicians who came up with at least two proofs for this law. They include Eisenstein, Kronecker, Schmidt, Dirichlet, Jacobi, and Rousseau. In a chronological order, Euler, Legendre and Gauss are the three principal mathematicians of the formulations of this theory (see the list of proofs of quadratic reciprocity in [Lem]. The list starts with Legendre who presented an incomplete proof in 1788 then completed by Dirichlet. Carl Friedrich Gauss who was known as the father of the modren theory of numbers, conjectured in 1795 that the theorem was correct [Dud12]. Gauss provided 8 rigorous proofs of quadratic reciprocity. He presented a complete proof in 1801. In his book *Disquisitiones Arithmeticae*, he refered to the law of quadratic reciprocity as the fundamental theorem. Even as recently as 2013, there are new proofs of the law of quadratic reciprocity.

The organization of the thesis is as follows. The first chapter will provide basic concepts of quadratic reciprocity and useful tools such as Legendre's symbol and Euler's criterion. Our first proof of quadratic reciprocity is due to Eisenstein and relies on a lemma on couting lattice points. The second proof we give is also due to Eisenstein, using the nth roots of unity. After that, we will provide a recent proof given by Rousseau in 1991 [Rou91] which is quite simple and uses group theory.

We close this thesis with a discussion of famous results due to Dirichlet and Fermat. We will use quadratic recprocity to prove special cases of Dirichlet's theorem for primes of the forms $5k+4$, $8k+3$ and $12k+11$. As another application of quadratic reciprocity, we will prove Fermat's theorems on primes of the form a^2+b^2, a^2+2b^2 and a^2+3b^2.

1.1 Basic concepts of quadratic reciprocity

Definition 1.1. *If p is an odd prime, a and p are relatively prime, then a is a quadratic residue* $\pmod p$ *if $x^2 \equiv a \pmod p$ is solvable. If this is not solvable, then we call a a quadratic non-residue* $\pmod p$.

As an example, let us find the quadratic residues $\pmod{17}$. We calculate that $1^2 \equiv 16^2 \equiv 1 \pmod{17}$, $2^2 \equiv 15^2 \equiv 4 \pmod{17}$, $3^2 \equiv 14^2 \equiv 9 \pmod{17}$, $4^2 \equiv 13^2 \equiv 16 \pmod{17}$, $5^2 \equiv 12^2 \equiv 8 \pmod{17}$, $6^2 \equiv 11^2 \equiv 2 \pmod{17}$, $7^2 \equiv 10^2 \equiv 15 \pmod{17}$ and $8^2 \equiv 9^2 \equiv 13 \pmod{17}$. Thus the quadratic residues of $p = 17$ are $1, 2, 4, 8, 9, 13, 15$ and 16.

His first theorem according to the law of quadratic reciprocity was known as Euler's criterion. In 1744, Euler proved the following criterion for quadratic residues [Lem13].

Theorem 1.2 (Euler's Criterion)**.** *If p is an odd prime and $(a,p)=1$, then*

1. *$x^2 \equiv a \pmod p$ is solvable if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.*
2. *$x^2 \equiv a \pmod p$ is not solvable if and only if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.*

Proof. For any $(a,p)=1$, by Fermat's theorem, we have

$$0 \equiv a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod p. \tag{1.1}$$

By Euclid's lemma so either $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Therefore, 1 and 2 are equivalent. It suffices to prove 1. Suppose that a is a quadratic residue. Then there is a solution x_0 such that $x_0^2 \equiv a \pmod p$. Since $p \nmid a$ we have $p \nmid x_0$. Therefore, $a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod p$ by Fermat's theorem.

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

$$a^{\frac{p-1}{2}} \equiv \left(g^{\frac{p-1}{2}}\right)^k \equiv \left(g^{\frac{k}{2}}\right)^{p-1} \equiv 1 \pmod{p}. \tag{1.2}$$

Since $\mathrm{ord}_p(g) = p-1$, we have $p-1 \mid \frac{k(p-1)}{2}$. Therefore, $k = 2l$ for some $l \in \mathbf{Z}$.

$(g^x)^2 = g^k \equiv a \pmod{p}$. Therefore, g^l is a solution for $x^2 \equiv a \pmod{p}$ and a is a quadratic residue.

□

To express the quadratic reciprocity law, the French Mathematician A.M. Legendre introduced a useful symbol.

Definition 1.3. *If $p \neq 2$ is a prime and a is an integer, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by*

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

By using previous example, we see that $\left(\frac{4}{17}\right) = 1$ because 4 is a quadratic residue (mod 17), and $\left(\frac{7}{17}\right) = -1$ because $x^2 \equiv 7 \pmod{17}$ has no solutions.

We will prove some properties of the Legendre symbol.

Theorem 1.4. *Let $p \neq 2$ be a prime and $(a,p) = (b,p) = 1$. Then*

- ***a.*** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ *(Euler's Criterion)*
- ***b.*** *If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*
- ***c.*** $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- ***d.*** $\left(\frac{a^2}{p}\right) = 1$

Proof.

a. Follows from the definition of $\left(\frac{a}{p}\right)$ and Euler's criterion.

b. If $p \mid a-b$, then $a \equiv b \pmod{p}$. Suppose that there is a solution for $x^2 \equiv a \pmod{p}$ and since $a \equiv b \pmod{p}$ then $x^2 \equiv b \pmod{p}$ has a solution too. Hence $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

c. From part **a**, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ and $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$ by multiplying both sides we get, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv (\frac{ab}{p}) \pmod{p}$. Since Legendre symbol assumes only values 1 or -1 . If , $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \not\equiv (\frac{ab}{p})$. Then $1 \equiv -1 \pmod{p}$. Therefore, $2 \equiv 0 \pmod{p}$ which is a contradiction.

d. Obviously, a is a solution of $x^2 \equiv a^2 \pmod{p}$, therefore,$\left(\frac{a^2}{p}\right) = 1$.

□

Now we can state the law of quadratic reciprocity.

Theorem 1.5 (Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

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

Another way to state this is as follows: if either p or q is of the form $4k+1$, then both congruences $x^2 \equiv q \pmod{p}$ and $x^2 \equiv p \pmod{q}$ are solvable or both are not. If p and q are both of the form $4k+3$, then one of the congruences is solvable and the other is not. In the next section, we will provide 3 proofs of the quadratic reciprocity.

Now, we also have some complementary results about $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

Theorem 1.6. *If p is an odd prime, then*

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

Proof. By Euler's Criterion, substitute $a = -1$ and we get that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod{p}. \tag{1.3}$$

If $p = 4k + 1$ for some integer k, then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1. \tag{1.4}$$

If $p = 4k + 3$, we get that

$$(-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1.$$

□

Theorem 1.7. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)} \tag{1.5}$$

Theorems 1.5 and 1.7 will be proved in the next chapter.

Before proving the law of quadratic reciprocity, we mention an important application, namely to determine quickly $\left(\frac{a}{p}\right)$ for any a and prime p.

Example 1.8. $x^2 \equiv 150 \pmod{1009}$ *is solvable since* $\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{5}{1009}\right)$

$\left(\frac{2}{1009}\right) = (-1)^{\left(\frac{1009^2-1}{8}\right)} = 1$

$\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right)(-1)^{\left(\frac{1009-1}{2}\right)} = \left(\frac{1}{3}\right)(-1)^{504} = 1$

$\left(\frac{5^2}{1009}\right) = 1.$

Thus, $\left(\frac{150}{1009}\right) = 1.$

2 PROOFS OF THE LAW OF QUADRATIC RECIPROCITY

Besides Euler, the law of quadratic reciprocity was also formulated by other mathematicians such as Gauss in 1795 and Eisenstein in 1844. While it was true that Euler and Legendre initiated the study of quadratic reciprocity, it was Gauss who first came up with a rigourous proof. He would eventually come up with eight proofs in the first decades of the 18th century and called it the *golden theorem*. One important lemma we will need in the proofs of quadratic reciprocity is Gauss's lemma [see [NZM13].

Lemma 2.1 (Gauss's Lemma)**.** *Let p be an odd prime and $p \nmid a$. Consider the integers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ and their least positive residues module p. If n counts the number of these residues that are greater than $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^n$.*

Proof. Let $r_1, r_2, \cdots, r_n$ be the integers greater than $\frac{p}{2}$ in the set of the residues and $s_1, s_2, \cdots s_m$ be those less than $\frac{p}{2}$. We know $n + m = \frac{p-1}{2}$.

We claim that $(p - r_i)$ and (s_j) are all distinct. For a contradiction, suppose that for some i, j, $p - r_i \equiv s_j \pmod{p}$. Then $p - ha \equiv ga \pmod{p}$ for some $1 \leq h, g \leq \frac{p-1}{2}$, so that $-ha \equiv ga \pmod{p}$. Since $p \nmid a$, this implies that $-h \equiv g \pmod{p}$ which is impossible because $2 \leq g+h \leq p-1$. This means that the numbers $(p-r_i)$ and (s_j) form a permutation of numbers $1, 2, \ldots \frac{p-1}{2}$. Multiplying these numbers, we get that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \prod_{i=1}^{n}(p-r_i)\prod_{j=1}^{m}s_j \\ &\equiv (-r_1)(-r_2)\cdots(-r_n)s_1s_2\cdots s_m \\ &\equiv (-1)^n r_1r_2\cdots r_ns_1\cdot s_2\cdots s_m \\ &\equiv (-1)^n(a)(2a)\cdots\left(\frac{p-1}{2}\right)a \\ &\equiv (-1)^n\left(\frac{p-1}{2}\right)!\,a^{\frac{p-1}{2}} \pmod{p}. \end{aligned} \tag{2.1}$$

Since $(p, (\frac{p-1}{2})!) = 1$, we get that

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

and therefore

$$(-1)^n \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}, \text{by Theorem 1.2.}$$

□

Using Gauss' lemma, we can now prove Theorem 1.7.

Proof of Theorem 1.7. The statement of the theorem is equivalent to saying that 2 is a quadratic residue $\pmod{p}$ if p is of the form $8k \pm 1$ and a quadratic non-residue $\pmod{p}$ if p is of the form $8k \pm 3$. Let $F = \{2, 4, 6, 8, \cdots, p-1\}$. Since p is an odd prime, then it can be written as $p = 4k+1$ or $4k+3$ for some integers k.

If $p = 4k+1$, then $\{x \in F | x = sp + r, r > \frac{p}{2}\} = \{x \in F | x = \frac{p-1}{2} + 2m, \quad m = 1, \cdots, \frac{p-1}{4}\}$. Therefore, $\left(\frac{2}{p}\right) = (-1)^n$ where $n = \frac{p-1}{4}$.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} \begin{cases} 1 & \text{if } p = 8k+1 \\ -1 & \text{if } p = 8k-3. \end{cases}$$

If $p = 4k + 3$, then $\{x \in F | x = \frac{p-1}{2} + 2m - 1\}$. Then $n = \frac{p+1}{4}$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} \begin{cases} 1 & \text{if } p = 8k - 1 \\ -1 & \text{if } p = 8k + 3. \end{cases}$$

Therefore, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. If $p = 8k \pm 1$, then $\frac{p^2-1}{8} = \frac{(8k\pm1)^2-1}{8} = 8k^2 \pm 2k$. Then $\frac{p^2-1}{8}$ is even. Therefore, $(-1)^{\frac{p^2-1}{8}} = 1$, but if $p = 8k \pm 3$, then $\frac{p^2-1}{8} = \frac{(8k\pm3)^2-1}{8} = 8k^2 + 6k + 1$ is odd. Then $(-1)^{\frac{p^2-1}{8}} = -1$. □

2.1 First proof using Eisenstein's lemma

Our first proof of the quadratic reciprocity depends on Gauss's lemma and Eisenstein's lemma. For more information on this proof, please see [Dud12, Section 12].

Lemma 2.2 (Eisenstein's Lemma)**.** *If p and q are odd primes, then*

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

Proof. As in the proof of Gauss's lemma, we consider the numbers $q, 2q, \cdots \frac{p-1}{2}q \pmod p$. Let $r_1, r_2, \cdots r_n$ be the residues greater than $\frac{p-1}{2}$ and $s_1, s_2, \cdots s_m$ be the residues smaller than $\frac{p-1}{2}$. Thus $n + m = \frac{p-1}{2}$. Using the division algorithm we find that

$$kq = p\left[\frac{kq}{p}\right] + r.$$

where r is the least residue $\pmod p$ of kq. If we sum these equations by k, we get

$$\sum_{k=1}^{\frac{p-1}{2}} kq = \sum_{k=1}^{\frac{p-1}{2}} p[\frac{kq}{p}] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j.$$

We have

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}} k &= 1+2+\cdots \frac{p-1}{2} \\ &= \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)/2 \\ &= \left(\frac{p-1}{2}\right)\left(\frac{p-1+2}{2}\right)\frac{1}{2} \\ &= \left(\frac{(p-1)(p+1)}{8}\right) \\ &= \left(\frac{p^2-1}{8}\right).\end{aligned}$$

Therefore

$$q\frac{(p^2-1)}{8} = p\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{2.2}$$

$$q\frac{(p^2-1)}{8} = p\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] + \sum_{j=1}^{n}(p-r_j) + \sum_{j=1}^{m} s_j \tag{2.3}$$

Since the numbers $(p-r_j)$ and s_j form a permutation of numbers $1, 2, \ldots, \frac{p-1}{2}$, then

$$\frac{(p^2-1)}{8} = \sum_{j=1}^{n}(p-r_j) + \sum_{j=1}^{m} s_j = S + np - R \tag{2.4}$$

By subtracting 2.2 from 2.4, we get

$$(q-1)\left(\frac{p^2-1}{8}\right) = p\left(\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] - n\right) + 2R.$$

Notice that p and q are odd primes, so the left-hand side is even and $2R$ is even. So, it follows that $\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] - n$ is even too. Hence

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]-n} = 1. \tag{2.5}$$

On the other hand,

$$(-1)^n = \left(\frac{q}{p}\right) \tag{2.6}$$

by Gauss' lemma. Therefore,

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]} = (-1)^n = \left(\frac{q}{p}\right), \tag{2.7}$$

as desired. □

We will need the following lemma.

Lemma 2.3. *If p and q are odd primes, then*

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kp}{q}] + \sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] = \frac{(p-1)(q-1)}{4}. \tag{2.8}$$

Proof. The main idea of the proof is the sum has a geometrical interpretation. Consider the points $A = (0,0), B = (\frac{p-1}{2}, 0), C = (\frac{p-1}{2}, \frac{q-1}{2}), D = (0, \frac{q-1}{2})$. Then $\sum_{k=1}^{\frac{p-1}{2}}[\frac{kp}{q}]$ is the number of lattice points contained in the interior of triangle ABC. Also, $\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]$ is the number of lattice points to the left of the line $AC = \frac{qx}{p}$ and contained in ADC. Note that there are no integral points on the line AC because $(p,q) = 1$. Thus the total number of the points in the rectangle ABCD is $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$. □

Now we are in a position to prove the quadratic reciprocity. From the Lemma 2.2, we get

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]} = \left(\frac{q}{p}\right). \tag{2.9}$$

By repeating the argument with $\left(\frac{p}{q}\right)$, we get

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kp}{q}]} = \left(\frac{p}{q}\right). \tag{2.10}$$

By multiplying 2.9 and 2.10, we find that

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

by Lemma 1.1. Hence

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

2.2 Second proof using roots of unity

In this section, we shall prove our second proof of the law of quadratic reciprocity. This proof published by Eisenstein in 1844. For more information on this proof, please see the text [IR13, Chapter 5].

Lemma 2.4. *If n is an odd integer, then*

$$x^n - y^n = \prod_{k=0}^{n-1}\left(\zeta^k x - \zeta^{-k} y\right) \tag{2.11}$$

where $\zeta = e^{\frac{2\pi i}{n}}$.

Proof. Note that $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ are all the nth roots of $z^n - 1$. We have

$$z^n - 1 = \prod_{k=0}^{n-1}(z - \zeta^k).$$

Applying this for $z = \frac{x}{y}$, we have

$$\frac{x^n}{y^n} - 1 = \prod_{k=0}^{n-1}\left(\frac{x}{y} - \zeta^k\right). \tag{2.12}$$

By multiplying both sides by y^n, we have

$$x^n - y^n = \prod_{k=0}^{n-1} \left(x - \zeta^k y\right) \tag{2.13}$$

Since n is odd, when k ranges from 0 to $n-1$, $-2k$ forms a complete system of residues (mod n). Therefore,

$$\begin{aligned}
x^n - y^n &= \prod_{k=0}^{n-1} \left(x - \zeta^{-2k} y\right) && (2.14)\\
&= \prod_{k=0}^{n-1} \left(x - \zeta^{-k} \times \zeta^{-k} y\right) && (2.15)\\
&= \prod_{k=0}^{n-1} \left(x - \frac{\zeta^{-k}}{\zeta^k} y\right) && (2.16)\\
&= \prod_{k=0}^{n-1} \left(\frac{\zeta^k x - \zeta^{-k} y}{\zeta^k}\right) && (2.17)\\
&= \frac{\prod_{k=0}^{n-1} \left(\zeta^k x - \zeta^{-k} y\right)}{\prod_{k=0}^{n-1} \zeta^k} && (2.18)\\
&= \frac{\prod_{k=0}^{n-1} \left(\zeta^k x - \zeta^{-k} y\right)}{\zeta^1 \cdot \zeta^2 \ldots \zeta^{n-1}} && (2.19)\\
&= \zeta^{-1} \cdot \zeta^{-2} \ldots \zeta^{-n+1} \prod_{k=0}^{n-1} \left(\zeta^k x - \zeta^{-k} y\right). && (2.20)
\end{aligned}$$

Since$-(1 + 2 + 3 + \cdots + (n-1) = \dfrac{n(n-1)}{2}$ is divisible by n, we have

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y). \tag{2.21}$$

□

Define the function $f(z) = e^{2\pi iz} - e^{-2i\pi z} = 2i\,\sin(2\pi z)$ where $i = \sqrt{-1}$. Then $f(z+1) = f(z)$ and $f(z) = -f(z)$, and the only real zeros of $f(z)$ are the integers $\frac{n}{2}$ where n is an integer.

Proposition 2.5. *Let n be an odd integer. Then*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right). \tag{2.22}$$

Proof. Let $x = e^{2\pi iz}$ and $y = e^{-2\pi iz}$. By Lemma 2.4,

$$\begin{aligned} f(nz) &= e^{2\pi inz} - e^{-2\pi inz} && (2.23)\\ &= \prod_{k=0}^{n-1} \left(e^{2\pi iz} e^{\frac{2\pi ik}{n}} - e^{-2\pi iz} e^{\frac{-2\pi ik}{n}}\right) && (2.24)\\ &= \prod_{k=0}^{n-1} \left(e^{\frac{2\pi ik + 2\pi inz}{n}} - e^{\frac{-2\pi ik - 2\pi inz}{n}}\right) && (2.25)\\ &= \prod_{k=0}^{n-1} \left(e^{2\pi i(\frac{k}{n} + z)} - e^{-2\pi i(\frac{k}{n} + z)}\right) && (2.26)\\ &= \prod_{k=0}^{n-1} f\left(\frac{k}{n} + z\right). && (2.27) \end{aligned}$$

When k ranges from $\frac{n+1}{2}$ to $(n-1)$, then $n-k$ ranges from $\frac{n-1}{2}$ to 1

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n} + z\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(\frac{k}{n} + z\right). \tag{2.28}$$

Since f is periodic with period 1

$$f\left(\frac{k}{n} + z\right) = f\left(\frac{k}{n} - 1 + z\right) = f\left(z - \frac{n-k}{n}\right).$$

Therefore

$$\prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n}+z\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z-\frac{n-k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n}+z\right) f\left(z-1-\frac{k}{n}\right).$$

Since $f(z+1)=f(z)$, we have

$$\prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n}+z\right) f\left(z-1-\frac{k}{n}\right) = \prod_{k=1}^{\frac{n-1}{2}} f\left(\frac{k}{n}+z\right) f\left(z-\frac{k}{n}\right).$$

□

Proposition 2.6. *Let $p \neq 2$ be a prime, $a \in \mathbf{Z}$ and $(p,a)=1$. Then*

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right) \tag{2.29}$$

Proof. Let $r_1, r_2, \cdots, r_n, s_1, s_2, \ldots s_m$ be the least residues of $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, where as in the proof of Gauss's lemma the $r_i > \frac{p-1}{2}$ and $s_i \leq \frac{p-1}{2}$. For each $1 \leq l \leq \frac{p-1}{2}$, let $t_l \in \{p-r_1, p-r_2, \ldots, p-r_n, s_1, \ldots, s_m\}$ be the unique number in $\{1, \ldots, \frac{p-1}{2}\}$ such that $\pm t_l \equiv la \pmod{p}$. Since f is periodic with period 1 and $f(-z) = -f(z)$, we have

$$f\left(\frac{la}{p}\right) = f\left(\frac{\pm t_l}{p}\right) = \pm f\left(\frac{t_l}{p}\right). \tag{2.30}$$

where the sign is + of − depending on whether $t \in \{s_1, \ldots, s_m\}$ or $t_l \in \{p-r_1, p-r_2, \ldots, p-r_n\}$. Multiplying (2.30) over all $l \in \{1, \ldots, \frac{p-1}{2}\}$, we have

$$\prod_{l=1}^{\frac{p-1}{2}} \pm f\left(\frac{t_l}{p}\right) \equiv \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right). \tag{2.31}$$

As l ranges from 1 to $\frac{p-1}{2}$, t_l also ranges from $\frac{p-1}{2}$. By Gauss's lemma the number of negative signes in (2.31) is $(-1)^n = \left(\frac{a}{p}\right)$. Hence

$$\left(\frac{a}{p}\right)\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) \tag{2.32}$$

as desired. □

Now we can prove the law of quadratic reciprocity. By Proposition 2.6

$$\left(\frac{q}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} \frac{f\left(\frac{lq}{p}\right)}{f\left(\frac{l}{p}\right)} \tag{2.33}$$

By Proposition 2.5

$$\frac{f\left(\frac{lq}{p}\right)}{f\left(\frac{l}{p}\right)} = \prod_{k=1}^{\frac{q-1}{2}} f\left(\frac{l}{p}+\frac{k}{q}\right) f\left(\frac{l}{p}-\frac{k}{q}\right) \tag{2.34}$$

Therefore

$$\left(\frac{q}{p}\right) = \prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}+\frac{k}{q}\right) f\left(\frac{l}{p}-\frac{k}{q}\right) \tag{2.35}$$

By repeating the argument with $\left(\frac{p}{q}\right)$, we will get

$$\left(\frac{p}{q}\right) = \prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{k}{q}+\frac{l}{p}\right) f\left(\frac{k}{q}-\frac{l}{p}\right). \tag{2.36}$$

Because $f(\frac{k}{q}-\frac{l}{p}) = -f(\frac{l}{p}-\frac{k}{q})$, we find that

$$\left(\frac{p}{q}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}\left(\frac{q}{p}\right) \tag{2.37}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}. \tag{2.38}$$

2.3 Third proof using group theory

Our third proof is due to George Rousseau [Rou91] in 1991. It does not depend on Gauss's lemma or Eisenstein's lemma on lattice points. This proof is seen to rely on nothing more than Wilson's theorem, Euler's criterion and the Chinese remainder theorem.

Recall that $(\mathbf{Z}/n\mathbf{Z})^\times$ is the multiplicative group of integers modulo n. Let G/H be the quotient group where $G = (\mathbf{Z}/pq\mathbf{Z})^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ and $H = \{\pm 1\} \cong \{(1,1),(-1,-1)\}$ is a normal subgroup of G. We determine the product of elements of G/H by multiplying the coset representatives of H.

We will give two results which are needed in Rousseau's proof.

Theorem 2.7 (Wilson's theorem)**.** *If p is a prime, then*

$$(p-1)! \equiv -1 \pmod{p}. \tag{2.39}$$

Proof. The congruence is obvious when $p = 2$ or $p = 3$. Suppose that $p \geq 5$. Consider the numbers $\{1, 2, \ldots, p-1\}$. Then each integer a has a unique inverse $\bar{a} \pmod{p}$. The integer a is equal to its own inverse if and only if

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow a \equiv 1 \quad \text{or} \quad a \equiv p-1 \pmod{p}. \tag{2.40}$$

Therefore, if $2 \leq a \leq p-2$, then $a \neq \bar{a}$. By dividing the remaining into pairs we find that

$$\prod_{a=2}^{p-2} a \equiv 1 \pmod{p}, \tag{2.41}$$

so that

$$(p-1)! \equiv 1 \times \prod_{a=2}^{p-2} a \times (p-1) \tag{2.42}$$

$$\equiv 1 \times 1 \times (-1) \equiv -1 \pmod{p}. \tag{2.43}$$

□

Lemma 2.8. *If p is a prime, then*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \pmod{p}. \tag{2.44}$$

Proof. For any $1 \leq i \leq \frac{p-1}{2}$, we have $p - i \equiv -i \pmod{p}$. Therefore,

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

□

Now we will provide Rousseau's proof of the quadratic reciprocity.

Proof. By Chinese reminder theorem, we have an isomorphic map

$$G = (\mathbf{Z}/pq\mathbf{Z})^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times. \tag{2.45}$$

Any element of the group G can be represented in the (a, b) where $a \in \{1, 2, \ldots, p-1\}$ and $b \in \{1, 2, \ldots, q-1\}\}$.

Consider the quotient of G by the subgroup $H = \{(1, 1), (-1, -1)\}$. We consider the representatives of G/H and take their product π. There are two ways to do that. First, let us take the whole of $(\mathbf{Z}/p\mathbf{Z})^\times$ and the first half of $(\mathbf{Z}/q\mathbf{Z})^\times$, then a list of representatives of G/H is

$$\{(a, b) : 1 \leq a \leq p-1, \quad 1 \leq b \leq \frac{q-1}{2}\} \tag{2.46}$$

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

$$(p-1)!^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} \pmod{p} \tag{2.47}$$

by Wilson's theorem.

Each b-component $1, 2, \ldots, \frac{q-1}{2}$ is repeated $p-1$ times. The b-component of π is

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

Therefore, the product of the representatives is

$$\pi \equiv \left((-1)^{\frac{q-1}{2}} \pmod{p}, (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{q}\right). \tag{2.48}$$

Finally, we will choose the representatives by taking the first half of $(\mathbf{Z}/pq\mathbf{Z})^\times$. We shall multiply all the integers between 1 and $\frac{pq-1}{2}$ which are not divisible by p or q. Let A be the set of integers in $[1, \frac{pq-1}{2}]$ that are not divisible by p. The elements of A are as follows.

$$\begin{array}{l} 1 \quad 2 \quad 3 \ldots\ldots p-1 \\ p+1 \quad p+2 \quad p+3 \ldots\ldots 2p-1 \\ 2p+1 \quad 2p+2 \quad 2p+3 \ldots\ldots 3p-1 \\ \vdots \\ \frac{q-1}{2}p+1 \quad \frac{q-1}{2}p+2 \quad \frac{q-1}{2}p+3 \ldots\ldots \frac{pq-1}{2} \end{array}$$

Then $B = \{q, 2q, \ldots, \frac{p-1}{2}q\}$ is the set of all integers in A that are divisible by q. Thus the a-component of π is

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

By Euler's criterion

$$q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) \pmod p. \tag{2.49}$$

Thus the a-component of π is

$$\equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \pmod p = (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p. \tag{2.50}$$

Working similarly $\pmod q$, the b-component of π is

$$\equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q. \tag{2.51}$$

Hence

$$\pi = \left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p, (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q\right). \tag{2.52}$$

Recall that π is determined up to a factor of ± 1. Comparing the two expressions (2.48) and (2.52), we get

$$\begin{aligned}&\left((-1)^{\frac{q-1}{2}} \pmod p, (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q\right) \\ = \;& \pm\left((-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p, (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod q\right).\end{aligned}$$

If the sign is $+$, then $\left(\frac{q}{p}\right) = 1$, $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. If the sign is $-$, then $\left(\frac{p}{q}\right) = -1$, $\left(\frac{q}{p}\right) = -(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. In any case $\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

3 APPLICATIONS OF QUADRATIC RECIPROCITY

In this chapter, we will discuss applications of quadratic reciprocity. The first application is to prove the existence of primes in certain arithmetic progressions, i.e. special cases of Dirichlet's theorem. In the second application, we will prove that certain primes can be expressed in terms of some quadratic forms (e.g. Fermat's theorem on sums of two squares).

3.1 Quadratic reciprocity and infinitude of primes

Recall Dirichlet's theorem, which states that if $(a, q) = 1$, then there are infinitely many primes $\equiv a \pmod{q}$. We will prove some special cases of Dirichlet's theorem using quadratic reciprocity. Since our proofs are similar to Euclid's proof of the infinitude of primes, we will first recall Euclid's proof.

Theorem 3.1 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose that there are finitely many primes. Call them $p_1, p_2, \ldots, p_k$. Let N be the number

$$N = p_1 p_2 \ldots p_k + 1.$$

Since N is greater than 1, it has a prime divisor p. Since the $p_1 p_2 \ldots p_k$ are all the primes, therefore $p = p_i$ for some i. Therefore, $p \mid p_1 p_2 \ldots p_k$. Thus $p \mid 1$, which is a contradiction since no primes divide 1. □

Our goal is to use a similar strategy. Using quadratic reciprocity, we will prove that there exist infinitely many primes of the forms $5k + 4$, $8k + 3$ and $12k + 11$. We need the following lemma to prove that.

Lemma 3.2. *If p is a prime and $(p,5)=1$, then $\left(\frac{5}{p}\right)=1$ if and only if $p\equiv 1$ or $4 \pmod 5$.*

Proof. By quadratic reciprocity, we have

$$\begin{aligned}\left(\frac{5}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{5}\right)\\ &= (-1)^{p-1}\left(\frac{p}{5}\right)\end{aligned}$$

On the other hand,

$$\left(\frac{p}{5}\right)=\begin{cases}1 & \text{if } p\equiv 1 \quad or \quad 4 \pmod 5\\ -1 & \text{if } p\equiv 2 \quad or \quad 3 \pmod 5.\end{cases}$$

Thus $\left(\frac{5}{p}\right)=1$ if and only if $p\equiv 1$ or $4 \pmod 5$. □

Theorem 3.3. *There are infinitely many primes congruent to* $4 \pmod 5$.

Proof. Suppose there are finitely many primes congruent to $4 \pmod 5$. Call these numbers $p_1, p_2, \ldots, p_k$. Consider the number

$$N=(2p_1p_2\ldots p_k)^2-5.$$

First we claim that all prime divisors of N are congruent to 1 or $4 \pmod 5$. Indeed, let p be any prime divisor of N. Then $p \mid (2p_1p_2\ldots p_k)^2-5$ and $(2p_1p_2\ldots p_k)^2\equiv 5 \pmod p$. Therefore, 5 is a quadratic residue mod p. By Lemma 3.2, $p\equiv 1$ or $4 \pmod 5$.

Next we claim that N has a prime divisor that is congruent to $p\equiv 4 \pmod 5$. If all the prime divisors of N are congruent to $1 \pmod 5$, then

$$N\equiv 1 \pmod 5. \tag{3.1}$$

On the other hand, we know $p_i\equiv 4 \pmod 5$ for all i, so $p_i^2\equiv 16\equiv 1 \pmod 5$. Thus, $N\equiv 4 \pmod 5$, which is a contradiction. Therefore, there must be at least one odd prime p dividing N which is $\equiv 4 \pmod 5$.

By assumption, $p_1, \ldots, p_k$ are all the primes congruent to 4 (mod 5). Then $p = p_i$ for some i. We have $p \mid N$ and $p \mid (2p_1p_2 \ldots p_k)^2$, so $p \mid 5$. This is a contradiction. Hence, there are infinitely many primes $p \equiv 4 \pmod 5$. □

Lemma 3.4. *If p is an odd prime and, then -2 is a quadratic residue mod p if and only if $p \equiv 1$ or $3 \pmod 8$.*

Proof. By quadratic reciprocity , we have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}. \tag{3.2}$$

But

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

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

Therefore, $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1$ or $3 \pmod 8$. □

Theorem 3.5. *There are infinitely many primes $p \equiv 3 \pmod 8$.*

Proof. Suppose there are finitely many primes congruent to 3 (mod 8). Let $p_1, p_2, \ldots, p_k$ be primes $p \equiv 3 \pmod 8$. Consider the number

$$N = (p_1p_2 \ldots p_k)^2 + 2 \tag{3.3}$$

First we claim that all prime divisors of N are congruent to 1 or 3 (mod 8). Indeed, let p be any prime divisor of N. Then $p \mid (p_1p_2 \ldots p_k)^2 + 2$ and $(p_1p_2 \ldots p_k)^2 \equiv -2 \pmod p$. Therefore, -2 is a quadratic residue mod p. By Lemma 3.4, $p \equiv 1$ or $3 \pmod 8$.

Next we claim that N has a prime divisor that is congruent to $p \equiv 3 \pmod 8$. If all the prime divisors of N are congruent to $1 \pmod 8$, then

$$N \equiv 1 \pmod 8. \tag{3.4}$$

On the other hand, since $p_i \equiv 3 \pmod 8$, we have $p_i^2 \equiv 9 \equiv 1 \pmod 8$ for all i. Therefore, $N \equiv 3 \pmod 8$ which is a contradiction. Therefore, there must be at least one odd prime p dividing N which is $\equiv 3 \pmod 8$.

By our assumption, there are only finitely many primes congruent to 3 (mod 8). Then $p = p_i$ for some i. Therefore, $p \mid (p_1 p_2 \dots p_k)^2$. We have $p \mid N$. Thus, $p \mid 2$, which is a contradiction since $p \equiv 3 \pmod 8$. Hence, there are infinitely many primes $p \equiv 3 \pmod 8$. □

Lemma 3.6. *If p is an odd prime and $(p, 3) = 1$, then $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1$ or $11 \pmod{12}$.*

Proof. By quadratic reciprocity, we know that

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}. \tag{3.5}$$

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

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hence, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1$ or $11 \pmod{12}$. □

Theorem 3.7. *There are infinitely many primes $p \equiv 11 \pmod{12}$.*

Proof. Suppose there are finitely many primes congruent to 11 (mod 12). Call these numbers $p_1, p_2, \ldots, p_k$. Consider

$$N = 3(p_1 p_2 \ldots p_k)^2 - 4. \tag{3.6}$$

First we claim that all prime divisors of N are congruent to 1 or 11 (mod 12). Indeed, let p be any prime divisor of N. Then $p \mid 3(p_1 p_2 \ldots p_k) - 4$ and $3(p_1 p_2 \ldots p_k) \equiv 4 \pmod{p}$. Therefore, 3 is a quadratic residue mod p. By Lemma 3.6, $p \equiv 1$ or 11 (mod 12).

Next we claim that N has a prime divisor that is congruent to $p \equiv 11 \pmod{12}$. If all the prime divisors of N are congruent to 1 (mod 12), then

$$N \equiv 1 \pmod{12}. \tag{3.7}$$

But we have $p_i \equiv 11 \pmod{12}$, so $p_i^2 \equiv 1 \pmod{12}$ for each i. Then, $N \equiv -1 \pmod{12}$. This is a contradiction since $N \equiv 1 \pmod{12}$. Therefore, there must be at least one odd prime p dividing N which is $\equiv 11 \pmod{12}$.

By our assumption, there are only finitely many primes congruent to $p \equiv 11 \pmod{12}$, so $p = p_i$ for some i. Then $p \mid 3(p_1, p_2, \ldots, p_k)^2$. We have $p \mid N$. Thus, $p \mid 4$ this is a contradiction since $p \equiv 11 \pmod{12}$. Hence, there are infinitely many primes $p \equiv 11 \pmod{12}$. □

3.2 Fermat's theorem on sums of two squares

In this section, we prove Fermat's theorem, which says that any prime number congruent to 1 (mod 4) can be expressed as the sum of two squares. We will use the same strategy to prove results about primes of the form $a^2 + 2b^2$ and $a^2 + 3b^2$.

In a letter to Mersenne in 1640, Fermat claimed that every prime congruent to 1 (mod 4) can be expressed as the sum of two perfect squares. Fermat did not provide a proof of his claim, but Euler was the first mathematician to prove the claim and published the detailed proof between 1752 and 1755. Our purpose is to prove Fermat's theorem and similar results using quadratic reciprocity.

In order to prove Fermat's theorem, we need the following fact.

Lemma 3.8. *For any integers a,b,c and d*

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2. \tag{3.8}$$

Proof. By multiplying out each expression, we have

$$\begin{aligned}
(ac+bd)^2 + (ad-bc)^2 &= \left((ac)^2 + 2\,(ac)\,(bd) + (bd)^2\right) + \left((ad)^2 - 2\,(ab)\,(cd) + (bc)^2\right) \\
&= \left(a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2\right) \\
&= \left(a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2\right) \\
&= \left(a^2+b^2\right)\left(c^2+d^2\right).
\end{aligned}$$

□

For the proofs of other quadratic forms, we will need the following more general identity.

Lemma 3.9. *If a, b, c, d and $n \in \mathbf{Z}$*

$$\left(a^2+nb^2\right)\left(c^2+nd^2\right) = (ac+nbd)^2 + n\,(ad-bc)^2.$$

Theorem 3.10 (Fermat)**.** *If p is an odd prime and $p \equiv 1 \pmod 4$, then there are integers a, b such that $p = a^2+b^2$.*

Proof. Our proof uses the descent method. First we find integers a, b and a positive integer $k < p$ such that

$$a^2 + b^2 = kp. \tag{3.9}$$

If $k = 1$, then we are done. If $k > 1$, then we will find integers a_1 and b_1 such that

$$a_1^2 + b_1^2 = k_1 p \tag{3.10}$$

for some integer $1 \leq k_1 < k$. This process must stop and $p = a_n^2 + b_n^2$ for some integers a_n, b_n.

To see the existence of a, b, k satisfying (3.9), by Theorem 1.6 we know that -1 is a quadratic residue $\pmod{p}$. Therefore, for some $0 \leq u \leq p-1$, we have

$$p \mid u^2 + 1 \Rightarrow u^2 + 1 = kp,$$

for some integer k and (3.9) is satisfied with $a = u, b = 1$. Since $0 \leq u \leq p-1$, we have $1 \leq k \leq p-1$. If $k = 1$, then we are done. If $k > 1$, we will show how to construct a_1, b_1 and k_1 satisfying (3.10). Set r and s by

$$a \equiv r \pmod{k}, \qquad b \equiv s \pmod{k} \text{ and } \qquad |r|, |s| \leq \frac{k}{2}. \tag{3.11}$$

Then

$$r^2 + s^2 \equiv a^2 + b^2 \equiv 0 \pmod{k}. \tag{3.12}$$

Therefore, $r^2 + s^2 = k_1 k$ for some $k_1 > 0$. We claim that then $k_1 > 0$. If not, then $r = s = 0$ and $a \equiv b \equiv 0 \pmod{k}$. Since $a^2 + b^2 = kp$, this implies that $k^2 \mid kp$ and $k \mid p$. This is impossible since $1 \leq k < p$. Therefore, $k_1 > 0$.

From Lemma 3.8 we get that

$$(r^2 + s^2)(a^2 + b^2) = (ra + sb)^2 + (rb - sa)^2. \tag{3.13}$$

Therefore

$$(ra + sb)^2 + (rb - sa)^2 = k_1 k^2 p. \tag{3.14}$$

Since $ra + sb \equiv r^2 + s^2 \equiv 0 \pmod{k}$, $rb - sa \equiv rs - sr \equiv 0 \pmod{k}$, we have $k^2 \mid (ra + sb)^2$ and $k^2 \mid (rb - sa)^2$. Dividing 3.14 by k^2, we have

$$\left(\frac{ra + sb}{k}\right)^2 + \left(\frac{rb - sa}{k}\right)^2 = k_1 p. \tag{3.15}$$

Also,

$$k_1 k = r^2 + s^2 \leq \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 = \frac{k^2}{2}. \tag{3.16}$$

Therefore, $0 < k_1 \leq \frac{k}{2} < k$ and we are done. □

Theorem 3.11. *If p is an odd prime and $p \equiv 1$ or $3 \pmod 8$, then there are integers a, b such that $p = a^2 + 2b^2$.*

Proof. Similarly to the proof of the previous theorem, we use the descent method. First we find integers a, b and a positive integer $k < p$ such that

$$a^2 + 2b^2 = kp. \tag{3.17}$$

If $k = 1$, then we are done. If $k > 1$, then we will find integers a_1 and b_1 such that

$$a_1^2 + 2b_1^2 = k_1 p \tag{3.18}$$

for some integer $1 \leq k_1 < k$.

To see the existence of a, b, k satisfying (3.17), by Lemma 3.4 we know that -2 is a quadratic residue $\pmod p$. Therefore, for some $0 \leq u \leq p-1$, we have

$$p \mid u^2 + 2 \Rightarrow u^2 + 2 = kp,$$

for some integer k and (3.17) is satisfied with $a = u, b = 1$. Since $0 \leq u \leq p-1$, we have $kp \leq (p-1)^2 + 2 = p^2 - 2p + 3 < p^2$. Therefore, $1 \leq k < p$. If $k = 1$, then we are done. If $k > 1$, we will show how to construct a_1, b_1 and k_1 satisfying (3.18). Set r and s by

$$a \equiv r \pmod k, \qquad b \equiv s \pmod k \text{ and } \qquad |r|, |s| \leq \frac{k}{2}. \tag{3.19}$$

Then

$$r^2 + 2s^2 \equiv a^2 + 2b^2 \equiv 0 \pmod k. \tag{3.20}$$

Therefore, $r^2 + 2s^2 = k_1 k$ for some $k_1 > 0$. We claim that $k_1 > 0$. If not, then $r = s = 0$ and $a \equiv b \equiv 0 \pmod{k}$. Since $a^2 + 2b^2 = kp$, this implies that $k^2 \mid kp$ and $k \mid p$. This is impossible since $1 \leq k < p$. Therefore, $k_1 > 0$.

From Lemma 3.8 we get that

$$(r^2 + 2s^2)(a^2 + 2b^2) = (ra + 2sb)^2 + 2(rb - sa)^2. \tag{3.21}$$

Therefore

$$(ra + 2sb)^2 + 2(rb - sa)^2 = k_1 k^2 p. \tag{3.22}$$

Since $ra+2sb \equiv r^2+2s^2 \equiv 0 \pmod{k}$, $rb-sa \equiv rs-sr \equiv 0 \pmod{k}$, we have $k^2 \mid (ra+2sb)^2$ and $k^2 \mid (rb - sa)^2$. Dividing 3.22 by k^2, we have

$$\left(\frac{ra + 2sb}{k}\right)^2 + 2\left(\frac{rb - sa}{k}\right)^2 = k_1 p. \tag{3.23}$$

Also,

$$k_1 k = r^2 + 2s^2 \leq \left(\frac{k}{2}\right)^2 + 2\left(\frac{k}{2}\right)^2 = \frac{3k^2}{4}. \tag{3.24}$$

Therefore, $0 < k_1 < k$ and we are done. □

Theorem 3.12. *If p is an odd prime and $p \equiv 1 \pmod{3}$, then $p = a^2 + 3b^2$.*

Proof. As breviuos proofs, First we find integers a, b and a positive integer $k < p$ such that

$$a^2 + 3b^2 = kp. \tag{3.25}$$

If $k = 1$, then we are done. If $k > 1$, then we will find integers a_1 and b_1 such that

$$a_1^2 + 3b_1^2 = k_1 p \tag{3.26}$$

for some integer $1 \leq k_1 < k$. This process must stop and $p = a_n^2 + 3b_n^2$ for some integers a_n, b_n.

To see the existence of a, b, k satisfying (3.25), by Theorem 1.6 we know that -3 is a quadratic residue $\pmod{p}$. Therefore, for some $0 \leq u \leq p-1$, we have

$$p \mid u^2 + 3 \Rightarrow u^2 + 3 = kp,$$

for some integer k and (3.25) is satisfied with $a = u, b = 1$. Since $0 \leq u \leq p-1$, we have $1 \leq kp \leq (p-1)^2 + 3 = p^2 - 2p + 4 < p^2$ and therefore $1 \leq k < p$. If $k = 1$, then we are done. If $k > 1$, we will show how to construct a_1, b_1 and k_1 satisfying (3.26). Set r and s by

$$a \equiv r \pmod{k}, \qquad b \equiv s \pmod{k} \text{ and } \qquad |r|, |s| \leq \frac{k}{2}. \tag{3.27}$$

Then

$$r^2 + 3s^2 \equiv a^2 + 3b^2 \equiv 0 \pmod{k}. \tag{3.28}$$

Therefore, $r^2 + 3s^2 = k_1 k$ for some $k_1 > 0$. We claim that then $k_1 > 0$. If not, then $r = s = 0$ and $a \equiv b \equiv 0 \pmod{k}$. Since $a^2 + 3b^2 = kp$, this implies that $k^2 \mid kp$ and $k \mid p$. This is impossible since $1 \leq k < p$. Therefore, $k_1 > 0$.

From Lemma 3.8 we get that

$$(r^2 + 3s^2)(a^2 + 3b^2) = (ra + 3sb)^2 + 3(rb - sa)^2. \tag{3.29}$$

Therefore

$$(ra + 3sb)^2 + 3(rb - sa)^2 = k_1 k^2 p. \tag{3.30}$$

Since $ra+3sb \equiv r^2+3s^2 \equiv 0 \pmod{k}$, $rb-sa \equiv rs-sr \equiv 0 \pmod{k}$, we have $k^2 \mid (ra+3sb)^2$ and $k^2 \mid (rb-sa)^2$. Dividing 3.30 by k^2, we have

$$\left(\frac{ra+3sb}{k}\right)^2 + 3\left(\frac{rb-sa}{k}\right)^2 = k_1 p. \tag{3.31}$$

Also,

$$k_1 k = r^2 + 3s^2 \leq \left(\frac{k}{2}\right)^2 + 3\left(\frac{k}{2}\right)^2 = \frac{4k^2}{4}. \tag{3.32}$$

Therefore, $0 < k_1 \leq k$.

At this step the proof is slightly more involved than the proofs for a^2+b^2 and a^2+2b^2. We have to rule out the posibility that $k_1 = k$. Suppose that $k_1 = k$. This implies that $r = s = \frac{k}{2}$ (and in particular k is even). Hence $a \equiv b \equiv \frac{k}{2} \pmod{k}$ and $\frac{k}{2}$ divides a and b. Since $a^2 + 3b^2 = kp$, we have $(\frac{k}{2})^2 \mid kp$ and therefore $k \mid 4p$. Since p is prime, $k < p$ and k is even, the only possibilities are $k = 2$ or 4.

If $k = 2$, then $a^2 + 3b^2 = 2p$. Furthermore, a and b are odd. Therefore, $a^2 + 3b^2 \equiv 0 \pmod{4}$, which is impossible since p is odd.

If $k = 4$, then $a^2 + 3b^2 = 4p$. Furthermore, a and b are congruent to 2 (mod 4). In this case, $(a/2)^2 + 3(b/2)^2 = p$, which is exactly what we need.

□

BIBLIOGRAPHY

[Dud12] Underwood Dudley. *Elementary number theory*. Courier Corporation, 2012.

[IR13] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.

[Lem] Franz Lemmermeyer. Proofs of the quadratic reciprocity law. `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`.

[Lem13] Franz Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein*. Springer Science & Business Media, 2013.

[NZM13] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 2013.

[Rou91] G Rousseau. On the quadratic reciprocity law. *Journal of the Australian Mathematical Society*, 51(3):423–425, 1991.

.

VITA

I was born and raised in Saudi Arabia. I pursued my Bachelor's in Mathematics from Taibah University, Saudi Arabia in 2012. After completing my undergradute degree, I spent around two years as bank marketing in Samba bank in Saudi Arabia. I decided to learn English and complete my master's degree in the United State. Before I came to Oxford, Mississippi, I attended the University of California, San Diego, in English language program in 2015.