# Congruent Number and Related Topics

by

**Shamik Das**


DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY
GUWAHATI
GUWAHATI-781039, INDIA
**June 23, 2021**

# Congruent Number and Related Topics

**Doctor of Philosophy**

by

**Shamik Das**

(Roll No. - 166123003)

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI-781039, INDIA

June 23, 2021

**Dedicated To My Parents**

*Shri. Chhedan Kumar Das*

*&*

*Smt. Rita Das*

# Declaration

I do hereby declare that this thesis entitled **Congruent Number and Related Topics** is a presentation of my original research work done under the supervision of **Prof. Anupam Saikia**, Professor, Department of Mathematics, Indian Institute of Technology Guwahati for the award of the degree of Doctor of Philosophy and this work has not been submitted elsewhere for a degree.

June 23, 2021

Shamik Das
Roll No. 166123003
Department of Mathematics
Indian Institute of Technology Guwahati

# Certificate

It is to certify that the work contained in this thesis entitled **Congruent Number and Related Topics** has been carried out by **Shamik Das**, a student in the Department of Mathematics, Indian Institute of Technology Guwahati, under my supervision for the award of the degree of Doctor of Philosophy and this work has not been submitted elsewhere for a degree.

June 23, 2021

Prof. Anupam Saikia
Professor
Department of Mathematics
Indian Institute of Technology Guwahati

# Acknowledgements

First and foremost, I am extremely grateful to my supervisor Prof. Anupam Saikia for his generous guidance, invaluable advice, continuous support, and patience during my the years of PhD. Also I would like to express my deep appreciation for his patience, understanding and support. He helped me to overcome many obstacles that emerged while working on several problems. In a good way, he always used to push for better results. He was deeply involved and helped me in every possible way. Without his tremendous understanding and encouragement in the past few years, it would be impossible for me to complete my study. I could not have imagined having a better advisor and mentor for my Ph.D study.

I want to convey my sincere thanks to my doctoral committee members, Dr. Rupam Barman, Dr. K.V. Krishna and Dr. Vinay wagh for their encouragement, precious comments to improve my research work. I want to convey my gratitude to Dr. Debopam Chakraborty, Birla Institute of Technology and Science, Pilani for several valuable suggestions, insightful comments and continuous encouragement during my research tenure.

I sincerely acknowledge Indian Institute of Technology Guwahati for providing me various facilities necessary to carry out my research. I am most grateful to Ministry of Human and Resource Development, Government of India, for providing me financial assistance for the completion of my thesis work. I am also grateful to all the staff members of the Department of Mathematics for their assistance in various ways during my research period.

I would like to thank my friends and colleagues Shyam, Ayan, Rony, Rakesh, Nilanjan, Somnath, Sunil, Rupak, Shanti, Sumit, Ajit, Gouranga, Arun, Anirban, Abhishek, Kaushik, Shubhadeep, Ankita and many others for all their encouragement and support during this period. My special appreciation goes to my close friends Rijubrata, Somenath, Nilay, Samprit, Pritam, Sayani, Prerona, Pranali and Soumi with whom I have shared some of the best moments of my life.

I am extremely grateful to my parents, my elder brother (Ranit Das), sister-in-law (Joyajyoti) and all other family members for their love, concern, care, encouragement and moral support throughout my life. I would like to express my deepest gratitude to them for staying besides me all the time. Finally, I would like to acknowledge everybody who is important to the successful completion of the thesis as well as express my apology that I could not mention each of them individually.

June 23, 2021 **Shamik Das**

# ABSTRACT

A positive integer $n$ is called a congruent number if it is equal to the area of a right triangle with rational sides. Determining whether a given positive number is congruent or not is known as the congruent number problem. It is well-known that $n$ is a congruent number if and only if the rank of the Mordell-Weil group consisting of all rational points on the *congruent number elliptic curve* $E_n : y^2 = x^3 - n^2x$ is positive. Although congruent numbers have been studied for centuries, the problem of providing a complete classification still remains elusive. Various mathematicians constructed infinite families of congruent and non-congruent numbers with prime factors that satisfy certain congruence conditions.

We begin the thesis by introducing congruent number and its generalization in chapter 1. In chapter 2, we briefly mention certain preliminaries from basic algebra, number theory and elliptic curves that we need later. Then we outline the method of complete 2-descent which plays a central role in our work. We conclude the second chapter with a description of Monsky's matrices that we use subsequently.

In chapter 3, we construct infinite families non-congruent numbers with arbitrarily many pairs of prime factors generalizing results of Lagrange [36] and Serf [46]. We use the method of complete 2-descent adopted earlier by Iskra [28] for constructing non-congruent numbers with prime factors congruent to 3 modulo 8. In chapter 4, we construct families of highly composite non-congruent numbers by considering Monsky's matrices introduced in the appendix of [26].

The notion of $\theta$-congruent number is a generalization of congruent number, where one considers the area of a triangle with all possible angles $\theta$ such that $\cos\theta$ is rational rather than just $\theta = \frac{\pi}{2}$ (see [19], [31]). In chapter 5 we prove a criterion for a natural number to be a $\theta$-congruent number over certain classes of real number fields.

Tunnell [54] and Kazalicki [32] investigated the 2-part of class number of an quadratic imaginary field $\mathbb{Q}(\sqrt{-p})$ where $p$ is congruent prime number equivalent to 1 modulo 8 by studying congruence between certain half-integral weight modular forms. In chapter 6, we prove a divisibility result for the class number of $\mathbb{Q}(\sqrt{-pq})$, where $p$ and $q$ are distinct primes satisfying $(p, q) \equiv (5, 7) \pmod 8$ and $pq$ is a congruent number. Rather than modular forms of half-integral weight, we exploit the method of complete 2-descent.

Steuding [50] and Komatsu [35] considered the continued fraction expansion of some special types of irrational numbers (such as $\sqrt{n^2+1}$ or $\sqrt{n^2+2}$), whose limit is related to rational right triangles of area close to certain natural number. Keeping that perspective in mind, we have studied the period of the regular continued fraction of certain quadratic irrationals $\sqrt{n}$ though we have not yet been able to link our findings to the question of $n$ being congruent or not. In chapter 7, we include our results concerning the period of the regular continued fraction of $\sqrt{pq}$ where $p < q$ are two primes congruent to 3 modulo 4. We prove that the length of the period is divisible by 4 when $q$ is a quadratic non-residue modulo $p$ and is of the form $4k + 2$ when $q$ is a quadratic residue modulo $p$. We further examine the parity of the the central term in the palindromic part of the period of $\sqrt{pq}$.

We conclude the thesis by outlining scope of future research in chapter 8.

# CONTENTS

# CHAPTER 1

# INTRODUCTION

## 1.1 Congruent Number

A *rational right triangle* is a right triangle all of whose sides are rational numbers. A natural number $n$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers $a$, $b$ and $c$ such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1.1}$$

Otherwise, we call $n$ a non-congruent number. For example, 6 is a congruent number given by the Pythagorean triple $(3, 4, 5)$. The first reference to congruent numbers appeared in an Arab manuscript written in the tenth century. Since then, many famous mathematicians including Fibonacci, Fermat, and Euler made noteworthy contributions towards the study of congruent numbers (see [34], [1]). Fermat showed that $n = 1$ is not congruent, which is equivalent to Fermat's Last Theorem for the exponent 4. Euler was the first to show that $n = 7$ is a congruent number (see [34]). The classical problem of determining whether a given natural number is congruent or not is known as the *congruent number problem*. Clearly, $n$ is a congruent number if and only if $n\alpha^2$ is congruent for any $\alpha \in \mathbb{Z}$. therefore, it is enough to consider the problem for square-free natural numbers.

In the twentieth century, an association between congruent numbers and elliptic curves was established (see [34]). A natural number $n$ is congruent if and only if the elliptic curve

$$E_n : y^2 = x(x^2 - n^2). \tag{1.2}$$

has a rational point $(x, y)$ with $y \neq 0$. Here, $E_n$ is called the *congruent number elliptic curve* (see section 2.3.2). This association led Tunnell [54] to prove a simple criterion for determining whether or not a given positive integer is a congruent number under the

assumption of the Birch and Swinnerton-Dyer (BSD) conjecture. Monsky [40] and Tian [53] have made further significant contributions toward identifying congruent numbers.

However, a straight forward criterion to tell whether a given natural number is congruent or not still remains elusive. Due to the difficult nature of finding a complete solution to the congruent number problem, many mathematicians have focused on describing and generating particular families of congruent and non-congruent numbers. For known results on the construction of non-congruent numbers with arbitrarily many prime factors of the form $8k+3$, one can refer to the work of Iskra [28]. Lagrange [36], Serf [46] described families of non-congruent numbers containing a maximum of four distinct prime factors satisfying certain Legendre symbol conditions. Reinholz, Spearman & Yang [45], [43] and Cheng & Guo [8], [9] constructed new families of non-congruent numbers which are product of distinct primes in certain congruence classes modulo 8. In chapters 3 and 4, we construct several new families of non-congruent numbers containing an arbitrarily large number of prime factors. In chapter 3, we adopt the method of complete 2-descent (see section 2.4 for a brief account) to construct the families in Theorems 3.1.1-3.1.2. In chapter 4, we use Monsky matrices (see section 2.5) to construct the families in Theorems 4.1.1- 4.1.2.

## 1.2 Generalization of Congruent Number

If $n$ is not a congruent number, a natural question arises whether $n$ appears as the area of a right triangle whose sides belong to some real number fields, leading to the following generalization. A positive integer $n$ is called a congruent number over a number field $K$ (or in short, a *$K$-congruent number*) if there exist $a,\ b,\ c \in K$ such that (1.1) holds. The study of congruent numbers over algebraic extensions dates back at least to Tada [52] who considered real quadratic fields. Some results were given by Jędrzejak in [30] concerning congruent numbers over certain other real number fields. Fujiwara [19] and Kan [31] considered a variant of the congruent number called *$\theta$-congruent number* as follows.

**Definition 1.2.1.** *Let $0 < \theta < \pi$ be an angle with rational cosine, i.e., $cos(\theta) = \frac{s}{r}$ with $0 < |s| < r$ and $\gcd(r,s) = 1$. Let $(u,v,w)_\theta$ denote a triangle with an angle $\theta$ between the sides $u$ and $v$.*

*A positive integer $n$ is called a $\theta$-congruent number if there exists a triangle $(u,v,w)_\theta$ with sides in $\mathbb{Q}$ having area $n\alpha_\theta$, where $\alpha_\theta = \sqrt{r^2 - s^2}$. In other words, $n$ is a $\theta$-congruent number if it satisfies*

$$2rn = uv, \quad w^2 = u^2 + v^2 - 2uv \cdot \frac{s}{r}. \tag{1.3}$$

Note that for $\theta = \frac{\pi}{2}$, $\theta$-congruent numbers are nothing but the classical congruent numbers. For $\theta$-congruent number we have a similar criterion to (2.3.7) in terms of the associated *$\theta$-congruent number elliptic curve* given by

$$E_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n), \tag{1.4}$$

where $r$ and $s$ are defined as above.

The following criterion is due to Fujiwara (see [19]).

**Criterion 1.2.2.** *Let $\theta \in (0, \pi)$ be an angle such that $\cos\theta$ is rational.*

1. *A positive integer $n$ is $\theta$-congruent if and only if $E_{n,\theta}$ has a rational point of order greater than 2.*
2. *If $n \neq 1, 2, 3, 6$, then $n$ is $\theta$-congruent if and only if $E_{n,\theta}$ has infinitely many rational points.*

The notion of $\theta$-congruent numbers over a real number field $K$ resembles that of congruent numbers over a number field $K$.

**Definition 1.2.3.** *We call a natural number $n$ to be a $(K, \theta)$-congruent number if there is a triangle $(u, v, w)_\theta$ with sides in a number field $K$ satisfying (1.3). We refer to the triangle $(u, v, w)_\theta$ as a $(K, \theta, n)$-triangle.*

Janfada and Salami [29] studied $\theta$-congruent number over real quadratic fields. Girard, Lalín and Nair [20] showed the existence of two infinite families of composite non-$\frac{\pi}{3}$-congruent numbers and non-$\frac{2\pi}{3}$-congruent numbers, obtained as products of primes which are congruent to 5 modulo 24, and to 13 modulo 24 respectively. Mokrani [39] used Monky matrices to construct families of non-$\frac{\pi}{3}$-congruent numbers and non-$\frac{2\pi}{3}$-congruent numbers over $\mathbb{Q}$.

A natural question arises whether existence of one $(K, \theta, n)$ triangle implies existence of infinitely many such triangles. The implication holds for the classical congruent numbers (for $K = \mathbb{Q}$). But the implication need not hold in general. For example, consider $n = 1$ over the real quadratic field $\mathbb{Q}(\sqrt{3})$ and let $\theta = \frac{2\pi}{3}$. Then $\cos\theta = \frac{s}{r}$ where $s = -1$, $r = 2$ and $\alpha_\theta = \sqrt{r^2 - s^2} = \sqrt{3}$. There is a $(\mathbb{Q}(\sqrt{3}), \frac{2\pi}{3}, 1)$-triangle with sides $(2, 2, \sqrt{3})$ and $\sqrt{3} \cdot 1$ as area. But one can verify that the elliptic curve $E_{1,\frac{2\pi}{3}}$ contains only finitely many points with coordinates in $\mathbb{Q}(\sqrt{3})$. Thus, 1 occurs as $\frac{2\pi}{3}$-congruent number for only finitely many triangles with sides in $\mathbb{Q}(\sqrt{3})$. This motivates us to define the following, which is analogous to the notion of *properly $K$-congruent numbers* defined in [30].

**Definition 1.2.4.** *We say that a $K$-congruent number $n$ is a properly $K$-congruent if there are infinitely many rational right triangle having area as $n$.*

It is easy to note that every $\mathbb{Q}$-congruent number is properly $\mathbb{Q}$-congruent number. Analogously we can define properly $(K, \theta)$-congruent number as follows.

**Definition 1.2.5.** *We say that a $(K, \theta)$-congruent number $n$ is a properly $(K, \theta)$-congruent if there exist infinitely many $(K, \theta, n)$ triangles, i.e., (1.3) has infinitely many solutions $u, v, w \in K$.*

The question whether $n$ is a properly $K$-congruent number (or a properly $(K, \theta)$-congruent number) is intimately connected with the size of the torsion subgroup of the corresponding congruent number elliptic curve $E_n$ (or $\theta$-congruent number elliptic curve $E_{n,\theta}$) over $K$. The following result due to Fujiwara ensures that a positive number $n \neq 1,\ 2,\ 3,\ 6$ is $(\mathbb{Q}, \theta)$-congruent number if and only if it is properly $(\mathbb{Q}, \theta)$-congruent number.

**Proposition 1.2.6** ( [19]). *For $n \neq 1, 2, 3, 6$, we have*

$$E_{n,\theta}(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Here, $E_{n,\theta}(\mathbb{Q})_{tors}$ is torsion part of $E_{n,\theta}(\mathbb{Q})$ (see section 2.3.1 for details).

In chapter 5, we show that a $(K, \theta)$ congruent number $n$ must be properly $(K, \theta)$-congruent for a large class of real number fields $K$. In particular, we consider the cases when (i) $K$ is a multi-quadratic field (Theorem 5.1.1), (ii) degree of $K/\mathbb{Q}$ is coprime to 6 (Theorem 5.1.2) and (iii) $K$ is a real cubic field (Theorem 5.1.3).

## 1.3 Connection with the Class Number of $\mathbb{Q}(\sqrt{-n})$

The class number of a number field $K$ measures how far the ring is from being a principal ideal domain, or equivalently in this context, a unique factorization domain. There are still many open questions concerning the class number of number fields. Most notable among them is perhaps the conjecture of Gauss that there are infinitely many real quadratic fields of class number 1. We briefly discuss the notion of class group and class number in section 2.2.3. It is natural to ask whether we can associate the property of an integer $n$ being congruent to the class number of some associated number field. Tunnell [54] and Kazalicki [32] examined the class number of $\mathbb{Q}(\sqrt{-p})$ for a prime number $p \equiv 1 \pmod 8$ when $p$ is congruent. They considered congruence between modular forms of half-integral weight to prove a divisibility result for the class number of $\mathbb{Q}(\sqrt{-p})$. In chapter 6, we prove a divisibility result (Theorem 6.1.1) for the class number of $\mathbb{Q}(\sqrt{-pq})$ where $p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$ are primes such that $pq$ is a congruent number.

## 1.4 Continued Fraction of Quadratic Irrationals

Every real number $\alpha$ can be expressed as a simple continued fraction, which turns out to be periodic when $\alpha$ is a quadratic irrational, i.e., $\alpha = \sqrt{n}$ for some integer $n > 0$. There are several open questions concerning the period of $\sqrt{n}$, such as the conjecture of Chowla and Chowla (see [10]) which states that there exist infinite many primes $p$ such that the length of the period of $\sqrt{p}$ is $k$ for any given integer $k \geq 1$. In section 2.2.2, we briefly discuss continued fractions. Mathematicians have tried to relate the congruent number problem for an integer $n$ to the continued fraction of certain associated quadratic irrationals. Steuding [50] and Komatsu [35] considered the continued fraction expansion of some special types of irrational numbers (such as $\sqrt{n^2+1}$ or $\sqrt{n^2+2}$), whose limit is related to rational right triangles of area close to some positive number. Keeping that perspective in mind, we examine the continued fraction of certain quadratic irrationals in chapter 7. In particular, we consider the continued fraction of $\sqrt{pq}$ where $p$ and $q$ are distinct primes congruent to 3 modulo 4. We prove a result concerning the length of the period of the continued fraction of $\sqrt{pq}$ (see Theorem 7.1.1). We further prove a result concerning the central term of the period of $\sqrt{pq}$ (see Theorem 7.1.2). However, we have not yet been able to link our findings to the question of $pq$ being congruent or not.

# CHAPTER 2

# PRELIMINARIES

## 2.1 Basic Notions from Algebra

In this chapter, we recall some of the standard definitions and results in algebra, number theory & elliptic curves that we need later. We also give a description of the complete 2-descent method for the Mordell-Weil group of an elliptic curve. The 2-descent method is central to our work in chapter 3 and chapter 6. The final section of this chapter provides a detailed discussion of Monsky matrices to be used later in chapter 4.

### 2.1.1 Finitely Generated Abelian Groups

We recall certain well-known definitions and results from abstract algebra (see [17]).

**Definition 2.1.1.** *An abelian group* $\mathbf{G}$ *equipped with a binary operation, denoted by* $+$*, is called a* ***finitely generated abelian group*** *if there exist finitely many elements* $g_1,\ g_2,\ \ldots, g_n \in G$ *such that every* $g \in G$ *can be written as*

$$g = a_1 g_1 + a_2 g_2 + \cdots + a_n g_n, \qquad a_1,\ a_2,\ \ldots,\ a_n \in \mathbb{Z}.$$

**Theorem 2.1.2** (**Structure Theorem of Finitely Generated Abelian Groups**)**.** *Every finitely generated abelian group* $(G, +)$ *is isomorphic to a direct sum of cyclic groups, i.e., we have*

$$G \cong \mathbb{Z}/p_1^{v_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{v_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{v_s}\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z},$$

*with* $r$ *copies of* $\mathbb{Z}$*, where each* $p_i$ *is a prime for* $1 \leq i \leq s$ $(v_i,\ r \in \mathbb{Z})$*. Here, the primes* $p_i$ *are not necessarily distinct and the indices* $v_i$ *are non-negative integers. The non-negative integer* $r$ *is called the rank of the abelian group* $G$*.*

### 2.1.2 Rank and Determinant of a Block Matrix

Here we recall some basic concepts and properties from linear algebra (see [27] and [38]).

**Definition 2.1.3.** *Suppose* $\mathbf{A}$ *is an* $m \times n$ *matrix. Then* ***rank*** *of* $\mathbf{A}$ *is defined to be the maximum number of linearly independent column vectors (or row vectors) of* $\mathbf{A}$*. The rank of* $\mathbf{A}$ *is denoted by* $rank(\mathbf{A})$*. Note that, the rank of a matrix is unaltered under row and column operations.*

**Theorem 2.1.4.** *Let* $\mathbf{A}$ *be an* $n \times n$ *square matrix, then* $\det \mathbf{A} \neq 0$ *if and only if* $rank(\mathbf{A}) = n$*. i.e., the matrix* $\mathbf{A}$ *is invertible if and only if* $rank(\mathbf{A}) = n$*.*

For a square matrix subdivided into four separate blocks, the following identities can be applied to compute its determinant (see [38]).

**Proposition 2.1.5.** *If* $\mathbf{A}$ *and* $\mathbf{D}$ *are square matrices, then*

$$\det\left(\begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{C} & \mathbf{D} \end{bmatrix}\right) = \det\left(\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{D} \end{bmatrix}\right) = \det \mathbf{A} \cdot \det \mathbf{D}.$$

**Lemma 2.1.6** (**Schur complement Lemma**)**.** *If* $\mathbf{A}$ *and* $\mathbf{D}$ *are square matrices, then*

$$\det\left(\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix}\right) = \begin{cases} \det(\mathbf{A}) \det(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}) & \text{when } \mathbf{A}^{-1} \text{ exists,} \\ \det(\mathbf{D}) \det(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C}) & \text{when } \mathbf{D}^{-1} \text{ exists.} \end{cases}$$

## 2.2 Basic Notions from Number Theory

### 2.2.1 Congruence and Residues

We mention some basic terminology and standard results from elementary number theory (see [6] and [37]).

**Definition 2.2.1.** *Let* $n$ *be a positive integer. If* $x$ *and* $y$ *are integers, we say that* $x$ *is congruent to* $y$ *modulo* $n$ *if* $n$ *divides* $(x - y)$*. In this case, we write,* $x \equiv y \pmod{n}$*.*

**Theorem 2.2.2** (**Chinese Remainder Theorem**)**.** *Let* $n_1, n_2, \ldots, n_r$ *be positive integers such that* $\gcd(n_i, n_j) = 1$ *for* $i \neq j$*. Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

*has a simultaneous solution, which is unique modulo the integer* $n_1 n_2 \cdots n_r$*.*

**Definition 2.2.3.** *If $n$ is a positive integer, we say that the integer $a$ is a quadratic residue modulo $n$ if $\gcd(a, n) = 1$ and the congruence $x^2 \equiv a \pmod{n}$ has a solution. Otherwise we say that $a$ is a quadratic nonresidue modulo $n$.*

**Definition 2.2.4.** *Let $p$ be an odd prime and $a$ be an integer not divisible by $p$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by*

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

For example, we have

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Note that if $a$ is divisible by $p$, then we will take $\left(\frac{a}{p}\right) = 0$. Some important properties for the Legendre symbol are stated below.

**Theorem 2.2.5.** *Let $p$ be an odd prime and let $a$ and $b$ be integers that are relatively prime to $p$. Then the Legendre symbol has the following properties:*

1. *If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{a^2}{p}\right) = 1$.*
3. *$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod{p}$.*
4. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

**Theorem 2.2.6 (Quadratic Reciprocity Law for Legendre Symbol).** *If $p$ and $q$ are distinct odd primes, then*

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

**Theorem 2.2.7.** *If $p$ is a odd prime then*

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

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

The Jacobi symbol, a generalization of the Legendre symbol, is defined as follows.

**Definition 2.2.8.** *For any integer $a$ and any positive odd integer $n$, the* ***Jacobi symbol*** $\left(\frac{a}{n}\right)_j$ *is defined as the product of the Legendre symbols corresponding to the prime factors of $n$ :*

$$\left(\frac{a}{n}\right)_j = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_t}\right)^{e_t},$$

*where $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ is the prime factorization of $n$.*

It is to be observed that when the lower argument is an odd prime, the Jacobi symbol is equal to the Legendre symbol.

**Theorem 2.2.9** (**Quadratic Reciprocity Law for Jacobi Symbol**)**.** *If $m$ and $n$ are odd positive numbers and mutually prime, then*

$$\left(\frac{m}{n}\right)_j\left(\frac{n}{m}\right)_j = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Suppose $p$ is a prime satisfying $p \equiv 1 \pmod 4$. Suppose $a$ is a integer with $\left(\frac{a}{p}\right) = 1$, i.e., $a$ is quadratic residue modulo $p$. Now a natural question is, does $x^4 \equiv a \pmod p$ has a solution or not. An affirmative answer to the above question leads us to define the following.

**Definition 2.2.10.** *Suppose $p$ is a prime satisfying $p \equiv 1 \pmod 4$. Suppose $a$ is an integer with $\left(\frac{a}{p}\right) = 1$, i.e., $a$ is a quadratic residue modulo $p$. Now we will call $a$* ***quartic*** *or* ***biquadratic residue*** *modulo $p$ if it is congruent to the fourth power of an integer modulo $p$. If $x^4 \equiv a \pmod p$ has (respectively does not have) an integer solution, $a$ is a quartic or biquadratic residue (respectively quartic or biquadratic nonresidue) modulo $p$ and we denote it as $\left(\frac{a}{p}\right)_4 = 1$ (respectively, $\left(\frac{a}{p}\right)_4 = -1$).*

**Theorem 2.2.11** (**Dirichlet's Theorem on Primes in Arithmetic Progressions**)**.** *Suppose that $a$ and $b$ are relatively prime positive integers. Then the arithmetic progression $an + b$, where $n$ is a positive integer, contains infinitely many primes.*

### 2.2.2 Continued Fractions

One can consider chapter IV of [13] as a reference for this section.

**Definition 2.2.12.** *A* ***continued fraction*** *is an expression obtained through an iterative process of representing a number as the sum of its integer part and the reciprocal of another number, then writing this other number as the sum of its integer part and another reciprocal, and so on. It is generally assumed that the numerator of all of the fractions is 1. This case is known as* ***simple*** *or* ***regular continued fraction****(RCF).*

A finite simple continued fraction is a simple continued fraction with only a finite number of terms. An infinite simple continued fraction is a simple continued fraction with an infinite number of terms. The RCF for a real number $x$ is written as

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}, \qquad a_0 = \lfloor x \rfloor.$$

Here $a_0, a_1, a_2, \ldots$ are known as terms or coefficients of the RCF of $x$ and in this case, we write $x = \langle a_0; a_1, a_2, a_3, \ldots \rangle$.

**Definition 2.2.13.** *The infinite simple continued fraction $\alpha = \langle a_0; a_1, a_2, a_3, \ldots \rangle$ is said to be periodic if there exist positive integers $n_0$ and $l$ such that for all $n \geq n_0$, we have $a_n = a_{n+l}$. If $l$ is the smallest integer with this property, then the $l$-tuple $(a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+l-1})$ is called the period of $\alpha$ and $l$ is called the length of the period of $\alpha$.*

The simplest and most familiar irrational numbers are the quadratic irrationals, that is, irrational numbers which arise as the solutions of quadratic equations with integral coefficients. For example, $\sqrt{2}$ has a periodic RCF given by

$$\sqrt{2} = \langle 1; 2, 2, 2, \ldots \rangle = \langle 1; \overline{2} \rangle.$$

It is classically known that the RCF of a quadratic irrational is periodic, and the converse holds too.

### 2.2.3 Number Fields

In this section we recall some well known notation and terminology from [51].

**Definition 2.2.14.** *A **number field** is a sub-field $K$ of $\mathbb{C}$ such that $[K : \mathbb{Q}]$ is finite. The **ring of integers** $\mathcal{O}_K$ of an algebraic number field $K$ is the ring of all elements of $K$ that are integral over $\mathbb{Z}$.*

For instance, $\mathbb{Q}(\sqrt{m})$ is a quadratic number field, and $\mathbb{Z}[\sqrt{m}]$ is the corresponding ring of integers, where $m$ is a square-free positive integer satisfying $m \equiv 2, 3 \pmod 4$.

The ring of integers $\mathcal{O}_K$ of a number field $K$ need not be a unique factorization domain, but unique factorization of a non-zero ideal into prime ideals does hold.

**Definition 2.2.15.** *A finitely generated $\mathcal{O}_K$-submodule $\Gamma$ of $K$ is called a fractional ideal of $\mathcal{O}_K$. Equivalently, an $\mathcal{O}_K$-submodule $\Gamma$ of $K$ is called a fractional ideal of $\mathcal{O}_K$ if there exists some non-zero $c \in \mathcal{O}_K$, such that $c\Gamma \subseteq \mathcal{O}_K$.*

The main idea of defining fractional ideals is to enlarge the set of ideals so that each ideal becomes invertible in the enlarged set, since the ideals in $\mathcal{O}_K$ clearly form a semigroup with the whole ring as identity where the existence of an inverse fails for all other ideals.

**Theorem 2.2.16.** *The non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication. Moreover, every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

The following notion measures how far prime factorization fails in $\mathcal{O}_K$, or equivalently, how far ideals of $\mathcal{O}_K$ are from being principal ideals.

**Definition 2.2.17.** *Let $\mathcal{F}$ be the group of fractional ideals under multiplication. The set of principal fractional ideals $\mathcal{P}$ is a subgroup of $\mathcal{F}$. The **ideal class group** of $\mathcal{O}_K$ is the quotient group*

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

*The **class number** $h = h(\mathcal{O}_K)$ is defined to be the order of $\mathcal{H}$.*

**Theorem 2.2.18.** *For a number field $K$, the ideal class group $\mathcal{H}$ is a finite abelian group.*

If $K$ is a number field then there exists an algebraic integer $\theta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$. The degree of the minimal polynomial of $\theta$ over $\mathbb{Q}$ is defined as the degree of the extension of $K$ over $\mathbb{Q}$. An embedding of $K$ is an injective ring homomorphisms $\sigma : K \to \mathbb{C}$. We call $\sigma : K \to \mathbb{C}$ a **real** embedding if $\sigma(K) \subset \mathbb{R}$ and **complex** embedding if $\sigma(K) \not\subset \mathbb{R}$.

**Theorem 2.2.19.** *Let $K = \mathbb{Q}(\theta)$ be a number field of degree $n$ over $\mathbb{Q}$. Then there are exactly $n$ distinct embeddings $\sigma_i : K \to \mathbb{C}$ $(i = 1, 2, \ldots, n)$. The element $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of $\theta$ over $\mathbb{Q}$.*

There is always an even number of complex embedding for a number field since the complex embeddings of $K$ occur in conjugate pairs $\sigma, \bar{\sigma}$, where $\bar{\sigma} : K \to \mathbb{C}$ takes $x$ to $\overline{\sigma(x)}$ for the embedding $\sigma$. If a number field $K$ of degree $n$ has $r$ real embeddings and $2s$ complex embeddings, then $r + 2s = n$ by Theorem 2.2.19. The collection of all invertible elements in the ring of integers $\mathcal{O}_K$ of a number field $K$ forms a group under multiplication, denoted by $\mathcal{O}_K^\times$.

**Theorem 2.2.20** (Dirichlet's Unit theorem)**.** *$\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$.*

It follows that $\mathcal{O}_K^\times$ for a real quadratic field $K$ is of rank 1, and the free part of $\mathcal{O}_K^\times$ has a unique generator bigger than 1. That unit is called the **fundamental unit.**

## 2.3 Elliptic Curves

Elliptic curves (see [48] and [49]) play a key role in the study of congruent numbers.

**Definition 2.3.1.** *An **elliptic curve** over a number field $K$ is a non-singular algebraic curve defined by an equation of the form*

$$y^2 = x^3 + ax + b, \tag{2.1}$$

*where $a, b \in K$. We denote it by $E/K$.*

Non-singularity of the curve is equivalent to non-vanishing of the discriminant

$$D = -(4a^3 + 27b^2). \tag{2.2}$$

The $K$-rational points on $E$ form an abelian group, denoted by $E(K)$, where the group operation is defined as follows.

### 2.3.1 Group Structure

It is convenient to consider $E/K$ as a projective curve which has a *point at infinity* denoted by $\mathcal{O}$ apart from its affine points. We homogenize the equation (2.1) by substituting $x = X/Z$ and $y = Y/Z$, which yields

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

The intersection of the homogenized cubic with the line at infinity $Z = 0$ gives $X^3 = 0$, which has a triple root $X = 0$. From the homogenized cubic, we find that $X = 0$ means $Z = 0$ and $Y$ can be taken as 1. The point $\mathcal{O} = [0 : 1 : 0]$ in homogenous coordinates is called the *point at infinity*, where the cubic meets the line at infinity thrice.

Suppose $P$ and $Q$ are two points in $E(K)$. A composition law known as *the chord and tangent method* is used to define $P + Q$ as follows. The straight line joining $P$ and $Q$ intersects the curve $E$ at a third point, denoted as $P * Q$. Then the line joining $\mathcal{O}$ and $P * Q$ (i.e., the vertical line through $P * Q$) intersects the curve again at a third point $(\mathcal{O} * (P * Q))$, which is defined to be $P + Q$. Under $+$, $E(K)$ is an abelian group with $\mathcal{O}$ as the identity element.

**Theorem 2.3.2** (**Mordell-Weil Theorem**)**.** *Let $E$ be an elliptic curve defined over a number field $K$. Then $E(K)$, the set of $K$-rational points on $E$, is a finitely generated abelian group.*

Consequently, we have (by Theorem 2.1.2)

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r, \tag{2.3}$$

where $E(K)_{tors}$ consists of all points of finite order in $E(K)$.

**Definition 2.3.3.** *The non-negative integer $r$ appearing in (2.3) is called the rank of $E(K)$.*

The rank of $E(K)$ is hard to determine, but the torsion part of $E(K)$ is far easier to compute especially when $K = \mathbb{Q}$. The following two results can be found in chapter II, [49]

**Theorem 2.3.4** (**Nagell-Lutz Theorem**). *Let $P = (x, y) \in E(\mathbb{Q})_{tors}$. Then $x$ and $y$ are integers, and either $y = 0$, in which case $P$ has order two, or else $y^2$ divides $D$, where $D$ is defined in (2.2).*

**Theorem 2.3.5** (**Mazur's Theorem**). *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is one of the following 15 groups:*

1. *$\mathbb{Z}/N\mathbb{Z}$: a cyclic group of order $N$, with $1 \leq N \leq 10$ or $N = 12$.*

2. *$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$: the product of a cyclic group of order 2 and a cyclic group of order $2N$, with $1 \leq N \leq 4$.*

For later work, we need the torsion structure of $E$ over more general number fields $K$. The torsion structure of $E(K)$ is better understood when $E$ has complex multiplication (CM) as defined below.

**Definition 2.3.6.** *An elliptic curve is said to have complex multiplication if its endomorphism ring End$(E)$ is strictly bigger than $\mathbb{Z}$.*

Note that End$(E)$ always contains $\mathbb{Z}$ as the map $m : E \longrightarrow E$, $P \mapsto mP$ is an endomorphism for any integer $m$. The elliptic curve $E_n$ given by (1.2) has CM as we have an endomorphism $i : E \longrightarrow E$, $(x, y) \mapsto (-x, iy)$ for $i = \sqrt{-1} \notin \mathbb{Z}$.

There are several open questions concerning the rank of $E(\mathbb{Q})$. The most prominent one is the Birch and Swinnerton-Dyer conjecture (BSD conjecture) which states that the rank of $E(\mathbb{Q})$ is equal to the order of vanishing of the Hasse-Weil $L$-function $L(E, s)$ of $E$ at $s = 1$ (see [3]). The conjecture further gives an interpretation for the first non-vanishing coefficient of $L(E, s)$ in terms of other arithmetic invariants associated with the elliptic curve $E$. The BSD conjecture has not yet been proved, though a lot of progress has been made due to the pioneering work of Coates-Wiles, Gross-Zagier, Kolyvagin and Rubin. Tunnell [54] gave a simple equivalent criterion for a natural number to be congruent assuming the BSD conjecture.

### 2.3.2 The Congruent Number Elliptic Curve

Suppose $n$ is a congruent number. It follows easily from (1.1) that the rational point $(\frac{c^2}{4}, \frac{c(a^2-b^2)}{8})$ obtained from the Pythagorean triple $(a, b, c)$ corresponding to $n$ lies on the congruent number elliptic curve $E_n$ given by equation (1.2). We have (see Proposition 17 in [34])

$$E_n(\mathbb{Q})_{tors} = E_n(\mathbb{Q})[2] = \{\mathcal{O},\ (0,0),\ (\pm n, 0)\}. \tag{2.4}$$

Since $a \neq b$, the point $(\frac{c^2}{4}, \frac{c(a^2-b^2)}{8})$ must be of infinite order.
Conversely, a point $P$ of infinite order on $E_n(\mathbb{Q})$ gives a rational point $2P = (x, y)$ where $x - n$, $x$ and $x + n$ are rational squares (see Proposition 5.2.2). Taking $a = \sqrt{x+n} - \sqrt{x-n}$, $b = \sqrt{x+n} + \sqrt{x-n}$, and $c = 2\sqrt{x}$, it can be easily checked that $n$ is congruent number from (1.1). This arguments leads to the following well-known criterion.

**Criterion 2.3.7.** *A positive integer $n$ is a congruent number if and only if $E_n(\mathbb{Q})$ has a point of infinite order, i.e., $rank(E_n(\mathbb{Q})) > 0$.*

## 2.4 The Method of Complete 2-Descent

We briefly recall a useful tool that in examining the rank of $E_n(\mathbb{Q})$. We use the standard notation in chapter X of [48].

**Theorem 2.4.1** (**Complete 2-Descent for $E_n$**). *Consider the elliptic curve $E_n$ for $n = 2^\epsilon p_1 p_2 \cdots p_k$ where $k$ is a positive integer, $p_1,\ p_2,\ \ldots,\ p_k$ are distinct odd primes and $\epsilon \in \{0, 1\}$. Let*

$$S = \{\infty, 2, p_1,\ \ldots,\ p_k\}$$

*be a finite subset of $M_\mathbb{Q}$, the set of all places of $\mathbb{Q}$. In addition, define*

$$\mathbb{Q}(S, 2) := \{c \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} |\quad v_p(c) \equiv 0 \pmod 2 \quad \forall p \in M_\mathbb{Q} \setminus S\},$$

*where $v_p(c)$ is the p-adic valuation of c. Then there exists an injective homomorphism*

$$b : E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \tag{2.5}$$

*defined by*

$$P = (x, y) \mapsto \begin{cases} (1, 1) & \text{if } P = \mathcal{O}, \\ (-1, -n) & \text{if } P = (0, 0), \\ (n, 2) & \text{if } P = (n, 0), \\ (x, x - n) & \text{if } P = (x, y) \neq \mathcal{O}, (0, 0), (n, 0). \end{cases}$$

*If* $(b_1, b_2) \in \mathbb{Q}(S,2)\times\mathbb{Q}(S,2)\setminus\{(1,1),(-1,-n),(n,2),(-n,-2n)\}$, *then* $(b_1,b_2) \in image(b)$ *if and only if there exist* $(z_1,z_2,z_3) \in (\mathbb{Q}^\times)^3$ *such that the following two equations simultaneously hold:*

$$b_1 z_1^2 - b_2 z_2^2 = n \tag{2.6}$$

$$b_1 z_1^2 - b_1 b_2 z_2^3 = -n. \tag{2.7}$$

*In this case,* $(b_1,b_2) = b(P)$ *for*

$$P = (b_1 z_1^2, b_1 b_2 z_1 z_2 z_3).$$

Let $r(n)$ denote the rank of $E_n(\mathbb{Q})$. By (2.4), we have

$$E_n(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^{r(n)}, \qquad E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r(n)+2}. \tag{2.8}$$

By Theorem 2.4.1, we can say that the rank $r(n)$ of $E_n(\mathbb{Q})$ is positive if and only if the system of equations (2.6) and (2.7) has a solution in $(\mathbb{Q}^\times)^3$ for some $(b_1,b_2) \in \mathbb{Q}(S,2)\times\mathbb{Q}(S,2)\setminus\{(1,1),(-1,-n),(n,2),(-n,-2n)\}$. In general, $\mathbb{Q}(S,2)$ is a finite abelian subgroup of $\mathbb{Q}^\times$, and is easily computable. With $n$ as in Theorem 2.4.1, we have

$$\mathbb{Q}(S,2) = \langle\, \{-1,\ 2,\ p_1,\ p_2,\ \ldots,\ p_k\} \,\rangle \cong (\mathbb{Z}/2\mathbb{Z})^{2+k},$$

where binary operation $*$ given by

$$a * b = \frac{ab}{\gcd(a,b)^2} \qquad \text{for } a,b \in \mathbb{Q}(S,2).$$

**Remark 2.4.2.** *A system of representatives of classes in* $\mathbb{Q}(S,2)$ *is given by*

$$R = \{(-1)^\alpha 2^\beta p_1^{\epsilon_1}\cdots p_k^{\epsilon_k} \mid \quad \alpha,\ \beta,\ \epsilon_1,\ \ldots,\ \epsilon_k = 0 \text{ or } 1\}.$$

In order to show that $n$ is a non-congruent number, it suffices to show that the system of equations (2.6) and (2.7) does not have a solution in $(\mathbb{Q}^\times)^3$. We use an integral version of this argument in chapter 3. The following proposition rules out simultaneous solutions of equations (2.6) and (2.7) for certain pairs in $\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$ (see [46]).

**Proposition 2.4.3** (Unsolvability Condition)**.** *Let*

$$n = 2^\epsilon p_1 p_2 \cdots p_k$$

*be a square-free positive integer where* $\epsilon \in \{0,1\}$, $k$ *is a natural number, and* $p_1$, $p_2$, ..., $p_k$ *are odd primes. Let* $(b_1,b_2) \in R \times R$, *where* $R$ *is as defined in Remark 2.4.2. The system of equations given by (2.6) and (2.7) has no solution* $(z_1,z_2,z_3) \in \mathbb{Q}^\times\times\mathbb{Q}^\times\times\mathbb{Q}^\times$

*in the following cases:*

*(a)* $b_1 b_2 < 0$ *or*

*(b)* $2 \nmid n$ *and* $2 \mid b_1$.

## 2.5 Monsky's Formula for 2-Selmer Rank

We briefly describe another useful method that provides a bound for the rank $r(n)$ of $E_n(\mathbb{Q})$ in terms of the 2-Selmer rank. We first recall the following result from chapter X of [48].

**Theorem 2.5.1.** *Let* $[2] : E_n \to E_n$ *be the map sending* $P$ *to* $2P$.

*(a) There is an exact sequence*

$$0 \to E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to S^{(2)}(E_n(\mathbb{Q})) \to Ш(E_n(\mathbb{Q}))[2].$$

*(b)* $S^{(2)}(E_n(\mathbb{Q}))$ *is finite.*

Here, $S^{(2)}(E_n(\mathbb{Q}))$ and $Ш(E_n(\mathbb{Q}))$ are known as the 2-Selmer group and Tate-Shafarevich group for the elliptic curve $E_n$, respectively. For details, one can refer to chapter X of [48]. Together with Corollary 4.4 and Example 4.5.1 in chapter X of [48], Theorem 2.5.1 implies

$$\begin{aligned} & E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \subset S^{(2)}(E_n(\mathbb{Q})) \subset \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \\ \implies & \#E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \leq \#S^{(2)}(E_n(\mathbb{Q})) \leq \#\left(\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)\right). \end{aligned} \tag{2.9}$$

Clearly, $\#S^{(2)}(E_n(\mathbb{Q}))$ is a power of 2, and will be a multiple of 4, on account of the rational points of order 2 on $E_n$. Therefore, we write $S^{(2)}(E_n(\mathbb{Q})) = 2^{2+s(n)}$. The exponent $s(n)$ is often referred to as the 'Selmer rank' or '2-Selmer rank' of the curve $E_n$. The fundamental inequality $r(n) \leq s(n)$ arising out of (2.9) provides a useful bound for $r(n)$. Monsky introduced certain matrices which are useful in determining $s(n)$ in the appendix of [26]. The form of these matrices, referred to as Monsky matrices henceforth, depend on the parity of $n$. We briefly discuss the form in some detail when $n$ is odd.

Let $n = p_1 p_2 \cdots p_m$, where $p_1,\ p_2,\ \ldots, p_m$ are odd and distinct primes. We will use notation of Theorem 2.4.1. We give the set $G$ of divisors of $n$ a group structure by defining

$$u * u' = \frac{uu'}{\gcd(u,u')^2}.$$

Clearly, $G$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$. Consider the following system of equations

$$uvx^2 - ny^2 = vw^2, \quad uvx^2 + ny^2 = uz^2 \qquad u, v \in G \times G. \tag{2.10}$$

**Lemma 2.5.2** ( [25]). *There are exactly $2^{r(n)}$ systems (2.10) with non-trivial integer solutions. Moreover, there are $2^{s(n)}$ systems (2.10) which are everywhere locally solvable.*

**Lemma 2.5.3** ( [25]). *If the system (2.10) has solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every odd prime $p$, then there are also solutions in $\mathbb{Q}_2$, where $\mathbb{Q}_p$ denotes the completion of $\mathbb{Q}$ under the $p$-adic metric for a prime $p$.*

Using Lemma 2.5.3, one can compute the Selmer rank by considering solvability of (2.10) in $\mathbb{Q}_p$ for all prime factors $p$ of $n$. For each prime factor $p$ of $n$, the condition for solvability in $\mathbb{Q}_p$ is as follows:

- $\left(\frac{u}{p}\right) = \left(\frac{v}{p}\right) = 1, \quad$ for $\quad p \nmid u,\ p \nmid v,$
- $\left(\frac{2n/u}{p}\right) = \left(\frac{2v}{p}\right) = 1, \quad$ for $\quad p \mid u,\ p \nmid v,$
- $\left(\frac{2u}{p}\right) = \left(\frac{-2n/v}{p}\right) = 1, \quad$ for $\quad p \nmid u,\ p \mid v,$
- $\left(\frac{n/u}{p}\right) = \left(\frac{-n/v}{p}\right) = 1, \quad$ for $\quad p \mid u,\ p \mid v.$

One can define a homomorphism $\phi_p : G \times G \to \{\pm 1\} \times \{\pm 1\}$ as

$$\begin{aligned} \phi_p(u, v) &= \left(\left(\frac{u}{p}\right), \left(\frac{v}{p}\right)\right), \quad \text{for } p \nmid uv \\ \phi_p(1, n) &= \left(\left(\frac{2}{p}\right), \left(\frac{-2}{p}\right)\right), \\ \phi_p(n, 1) &= \left(\left(\frac{2}{p}\right), \left(\frac{2}{p}\right)\right). \end{aligned}$$

Thus (2.10) is solvable in $\mathbb{Q}_p$ precisely when $(u, v)$ lies in the kernel of $\phi_p$. It follows that if $Z$ is the intersection of the kernels of the homomorphisms $\phi_p$, then $Z$ has size $2^{s(n)}$.

We transform this situation into one involving linear algebra over $(\mathbb{Z}/2\mathbb{Z})^{2m}$ by making the pair $(u, v)$ correspond to the vector $\bar{u} = (u_1, u_2, \ldots, u_{2m}) \in (\mathbb{Z}/2\mathbb{Z})^{2m}$. Here, we have $u_i = 1$ if and only if $p_i \mid u$, and $u_{m+i} = 1$ if and only if $p_i \mid v$ for $1 \leq i \leq m$. The co-domain of $\phi_p$ is $\{\pm 1\} \times \{\pm 1\} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Therefore, $\phi_p$ can be considered as a linear transformation from $(\mathbb{Z}/2\mathbb{Z})^{2m}$ to $(\mathbb{Z}/2\mathbb{Z})^2$ over $\mathbb{Z}/2\mathbb{Z}$ for each $p \in \{p_1, p_2, \ldots, p_m\}$. One can fix a standard basis $\{e_1, e_2, \ldots, e_{2m}\}$ of $(\mathbb{Z}/2\mathbb{Z})^{2m}$ over $\mathbb{Z}/2\mathbb{Z}$, where $e_i \in \mathbb{Z}/2\mathbb{Z}$ having only $i$-th entry non zero. One can take $\{(1, 0), (0, 1)\}$ as a basis of co-domain over $\mathbb{Z}/2\mathbb{Z}$.

For each $p_i$, we have

$$\begin{aligned}
\phi_{p_i}(e_j) &= \left(\left(\frac{p_j}{p_i}\right), 0\right) \text{ if } 1 \leq j \leq m, \text{ and } i \neq j, \\
\phi_{p_i}(e_j) &= \left(0, \left(\frac{p_j}{p_i}\right)\right) \text{ if } m+1 \leq j \leq 2m, \text{ and } m+i \neq j, \\
\phi_{p_i}(e_i) &= \left(\left(\frac{2}{p_i}\right) + \sum_{j:j\neq i} \left(\frac{p_j}{p_i}\right), \left(\frac{2}{p_i}\right)\right), \\
\phi_{p_i}(e_{i+m}) &= \left(\left(\frac{2}{p_i}\right), \left(\frac{-2}{p_i}\right) + \sum_{j:j\neq i} \left(\frac{p_j}{p_i}\right)\right).
\end{aligned}$$

The matrix representation $M_{p_i}$ of $\phi_{p_i}$ is a $2 \times 2m$ matrix. Let $M_{p_i}(R_j)$ denote the $j$-th row of $M_{p_i}$ for $j = 1, 2$. The Monsky's matrix $\mathbf{M}_o$ is a $2m \times 2m$ matrix whose $i$-th row is given by $M_{p_i}(R_1)$ and the $(m+i)$-th row is given by $M_{p_i}(R_2)$ for $1 \leq i \leq m$.

We define an $m \times m$ diagonal matrices $\mathbf{D}_l = [d_i]$ for $l \in \{-1, 2\}$, and an $m \times m$ matrix $\mathbf{A} = [a_{ij}]$ by

$$d_i = \begin{cases} 0 & if \left(\frac{l}{p_i}\right) = 1, \\ 1 & if \left(\frac{l}{p_i}\right) = -1, \end{cases} \quad a_{ij} = \begin{cases} 0 & if \left(\frac{p_j}{p_i}\right) = 1, \quad j \neq i, \\ 1 & if \left(\frac{p_j}{p_i}\right) = -1, \quad j \neq i, \end{cases} \quad a_{ii} = \sum_{j:j\neq i} a_{ij}. \tag{2.11}$$

Then, we have

$$\mathbf{M}_o = \begin{bmatrix} \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2 \\ \mathbf{A} + \mathbf{D}_{-2} & \mathbf{D}_2 \end{bmatrix}. \tag{2.12}$$

The kernel of the $2m \times 2m$ matrix $\mathbf{M}_o$ identifies with $Z$. Therefore, the 2-Selmer rank is given by

$$s(n) = 2m - rank_{\mathbb{F}_2}(\mathbf{M}_o). \tag{2.13}$$

Similarly, one can handle the case when $n$ is even. In that case, the 2-Selmer rank is given by

$$s(n) = 2m - rank_{\mathbb{F}_2}(\mathbf{M}_e), \tag{2.14}$$

where $\mathbf{M}_e$ is the $2m \times 2m$ matrix given by

$$\mathbf{M}_e = \begin{bmatrix} \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2 \\ \mathbf{A}^T + \mathbf{D}_2 & \mathbf{D}_{-1} \end{bmatrix}. \tag{2.15}$$

# CHAPTER 3

# NON-CONGRUENT FAMILIES BY 2-DESCENT

## 3.1 Introduction

In this chapter, we generalize the work of Lagrange [36] and Serf [46] on the construction of families of non-congruent composite numbers having at most 4 primes factors. We use the complete 2-descent method, which was used by Iskra [28] to construct families of non-congruent numbers having all its primes factors of the form $8k+3$. The method has been outlined in section 2.4. Our main results can be stated as follows.

**Theorem 3.1.1.** *Let $t$ be a positive integer. Suppose $p_1$, $p_2$, ..., $p_t$ and $q_1$, $q_2$, ..., $q_t$ are distinct primes such that all pairs $(p_j, q_j)$ are equivalent either to $(1,3)$ or to $(5,7)$ modulo 8. Suppose*

$$\left(\frac{q_j}{q_i}\right) = -1 \quad \text{if } i > j, \qquad \left(\frac{p_i}{p_j}\right) = 1 \quad \text{if } i \neq j, \quad \text{and}$$
$$\left(\frac{p_i}{q_j}\right) = \begin{cases} 1 & \text{if } i \neq j \\ -1 & \text{if } i = j, \end{cases} \tag{3.1}$$

*then $n = p_1q_1 \cdot p_2q_2 \cdot \cdots \cdot p_tq_t$ is a non-congruent number.*

**Theorem 3.1.2.** *Suppose $p_1, p_2, \ldots, p_t$ are distinct primes such that all of them are equivalent 3 modulo 8 and $q$ is a prime such that $q \equiv 7 \pmod 8$. Suppose*

$$\begin{cases} \left(\frac{p_i}{q}\right) & = -1 \text{ for all } 1 \leq i \leq t, \\ \left(\frac{p_i}{p_j}\right) & = -1 \text{ if } 1 \leq i < j \leq t. \end{cases} \tag{3.2}$$

*If $t$ is a odd integer then $n = 2p_1p_2 \cdots p_tq$ is a non-congruent number.*

The following proposition guarantees that for each positive integer $t$, we do have infinitely many pairs of primes $(p_1, q_1), \ldots, (p_t, q_t)$ satisfying the conditions of Theorem 3.1.1. The proposition is a consequence of Dirichlet's theorem on primes in arithmetic progressions.

**Proposition 3.1.3.** *Let $H_t$ denote the collection of positive integers with prime factorization $(p_1q_1)(p_2q_2)\cdots(p_tq_t)$, where all the pairs $(p_j, q_j)$ are equivalent to $(1, 3)$ modulo 8 and satisfy the conditions (3.1). For any natural number $t$, the set $H_t$ contains infinitely many elements. The analogous statement for pairs $(p_j, q_j) \equiv (5, 7) \pmod 8$ holds and also for collection of non-congruent numbers satisfying (3.2).*

## 3.2 An Equivalent Integral System

By Theorem 2.4.1, we need to rule out the existence of non-trivial rational solutions for the system of equations (2.6) and (2.7). We first reformulate the system in terms of integral solutions.

**Lemma 3.2.1.** *Let $(z_1, z_2, z_3) \in (\mathbb{Q}^\times)^3$ be a solution to equations (2.6) and (2.7). Then there exist a positive integer $d$ and integers $a_1$, $a_2$ and $a_3$ such that*

$$z_1 = \frac{a_1}{d}, \quad z_2 = \frac{a_2}{d}, \quad z_3 = \frac{a_3}{d}, \quad \text{and } \gcd(a_i, d) = 1.$$

*Moreover, if $n$ is odd then $a_1$, $a_2$ and $a_3$ are pairwise coprime.*

*Proof.* We write $z_i = \frac{a_i}{d_i}$ for $i = 1, 2, 3$ as fractions in irreducible form with $d_i > 0$. After clearing denominators, equation (2.6) becomes

$$b_1a_1^2d_2^2 - b_2a_2^2d_1^2 = nd_1^2d_2^2. \tag{3.3}$$

By simple inspection, we can say that $d_1^2 | b_1d_2^2$ and $d_2^2 | b_2d_1^2$. Since $b_1$ and $b_2$ are square-free, we must have $d_1 | d_2$ and $d_2 | d_1$, hence $d_1 = d_2$. We set $d := d_1 = d_2$. Now, after clearing denominators, equation (2.7) becomes

$$b_1a_1^2d_3^2 - b_1b_2a_3^2d^2 = -nd^2d_3^2. \tag{3.4}$$

It is easy to see $d^2 | b_1d_3^2$ and since $b_1$ is square-free, $d | d_3$. Thus we write $d_3 = md$. By dividing both sides by $d^2$ in equation (3.4), we get

$$b_1a_1^2m^2 - b_1b_2a_3^2 = -nd^2m^2. \tag{3.5}$$

Equation (3.5) gives us $m^2 | b_1b_2$, and since $b_1$ and $b_2$ are square-free, we have $m | b_1$ and $m | b_2$, and $m$ is also square-free. Our target is to show $m = 1$. It can be shown that $(m, nd) = 1$.

Suppose $p$ is a prime dividing $(m, nd)$, then $\nu_p(b_1a_1^2m^2) \geq 3$ and $\nu_p(b_1b_2a_3^2) = 2$ but $\nu_p(nm^2d^2) \geq 3$, a contradiction to equation (3.4). Now since $b_i \equiv 0 \pmod{m}$ for $i = 1, 2$, from equation (3.3) we get $m = 1$, hence $d_3 = d$.

Now, we can rewrite (2.6) and (2.7) as

$$b_1a_1^2 - b_2a_2^2 = nd^2, \tag{3.6}$$

$$b_1a_1^2 - b_1b_2a_3^2 = -nd^2. \tag{3.7}$$

By taking the sum and the difference of the pair of equations above, we further obtain

$$2b_1a_1^2 - b_2a_2^2 - b_1b_2a_3^2 = 0, \tag{3.8}$$

$$b_2a_2^2 - b_1b_2a_3^2 = -2nd^2. \tag{3.9}$$

Since $n$ is square-free and $(a_i, d) = 1$ for $i = 1,\ 2,\ 3$, we can easily deduce from above that $(a_1, a_2) = (a_1, a_3) = (a_2, a_3) = 1$, whenever $n$ is odd. □

**Corollary 3.2.2.** *If* $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \setminus Im\{\mathcal{O}, (0, 0), (\pm n, 0)\}$ *then* $(b_1, b_2) \in Im(b)$ *if and only if there exist integers* $a_1$, $a_2$, $a_3$ *and* $d$ *with* $\gcd(a_i, d) = 1$, *satisfying the system of equations (3.6) and (3.7), or equivalently, (3.8) and (3.9).*

## 3.3 Proof of Theorem 3.1.1

In order to prove that $n = (p_1q_1)(p_2q_2)\cdots(p_tq_t)$ is a non-congruent number as stated in Theorem 3.1.1, we need to use the Legendre symbols listed as follows.

**Remark 2.** $(a)$ Suppose $n = n'_jq_j = n''_jp_j$ for all $j \in \{1,\ 2,\ \ldots,\ t\}$. Then

$$\left(\frac{n'_j}{q_j}\right) = (-1)^j, \quad \text{and} \quad \left(\frac{n''_j}{p_j}\right) = -1. \tag{3.10}$$

Moreover,

$$\left(\frac{q_j}{q_i}\right) = -1 \quad \text{for } i > j \ \text{ implies } \ \left(\frac{q_j}{q_i}\right) = 1 \quad \text{for } j > i. \tag{3.11}$$

$(b)$ When all the prime pairs in the factorization of $n$ in Theorem 3.1.1 satisfy $(p_j, q_j) \equiv (5, 7) \pmod 8$, we have

$$\left(\frac{-1}{p_j}\right) = -\left(\frac{2}{p_j}\right) = 1, \qquad \left(\frac{-1}{q_j}\right) = -\left(\frac{2}{q_j}\right) = -1. \tag{3.12}$$

$(c)$ When all the prime pairs in the factorization of $n$ in Theorem 3.1.1 satisfy $(p_j, q_j) \equiv$

$(1,3) \pmod 8$, we have

$$\left(\frac{-1}{p_j}\right) = \left(\frac{2}{p_j}\right) = 1, \qquad \left(\frac{-1}{q_j}\right) = \left(\frac{2}{q_j}\right) = -1. \tag{3.13}$$

By Corollary 3.2.2, it suffices to show that the system of equations (3.6) and (3.7) or equivalently, (3.8) and (3.9), cannot simultaneously be solved for any pair

$$\begin{aligned} &(b_1, b_2) \in D := R \times R \ \setminus \ \{(1,1), (-1,-n), (n,2), (-n,-2n)\}, \\ &\text{with } R = \{\pm 2^{\epsilon} p_1^{\epsilon_1} \dots p_t^{\epsilon_t} q_1^{\mu_1} \cdots q_t^{\mu_t} \mid \epsilon, \epsilon_1, \dots, \epsilon_t, \mu_1, \dots, \mu_t \in \{0,1\}\}. \end{aligned} \tag{3.14}$$

By Proposition 2.4.3, we know that the equivalent system of equations (2.6) and (2.7) do not have a solution when $b_1 b_2 < 0$, or when $2 \nmid n$ and $2 | b_1$. Therefore, we only need to consider pairs $(b_1, b_2)$ for which $b_1 b_2 > 0$ and $2 \nmid b_1$. The following lemma shows that it is enough to consider pairs $(b_1, b_2)$ for which $b_2$ is positive and odd.

**Lemma 3.3.1.** *Let $(b_1, b_2) \in D$ represent an element in the image of the map $b$ given by (2.5). Then, there is a pair $(b_1^*, b_2^*)$ in $D$ representing an element in $Im(b)$ such that $b_2^*$ is positive and odd.*

*Proof.* Let us first assume that $b_2$ is positive and even. Then the set of points

$$L = \{(1,1), (-1,-n), (n,2), (-n,-2n), (b_1, b_2)\}$$

generates a subgroup of $Im(b)$ inside $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. By closure, the pair

$$(b_1, b_2) \cdot (n, 2) = (nb_1, 2b_2) \in Im(b).$$

By our assumption $2 | b_2$, hence we can write $2b_2 = 2^2 b_2^*$, where $b_2^* \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ and $2 \nmid b_2^*$. If we set $b_1^* = nb_1$, then we have

$$(nb_1, 2b_2) = (b_1^*, b_2^*) \in Im(b) \subset \mathbb{Q}(S,2) \times \mathbb{Q}(S,2),$$

where $b_2^*$ is odd.

Next, let us assume that $b_2$ is negative and odd. As before, we have

$$(b_1, b_2) \cdot (-n, -2n) = (-nb_1, -2b_2 n) = (b_1^*, b_2^*) \in Im(b),$$

where $b_2^* = -2b_2 n$ is positive and even. But it leads us to the previous case.

Finally, let $b_2$ be negative and even. Then the pair

$$(b_1, b_2) \cdot (-n, -2n) = (-b_1 n, -2b_2 n) \in Im(b)$$

as well. Equivalently, the pair

$$(b_1^*, b_2^*) \in Im(b) \subset \mathbb{Q}(S,2) \times \mathbb{Q}(S,2),$$

where $b_1^* = -b_1 n$, $-2b_2 n = 2^2 b_2^*$ with $b_2^*$ as positive and odd. □

By Corollary 3.2.2, (3.14) and Lemma 3.3.1, it now suffices to show that for a pair $(b_1, b_2)$ in $D$ with $b_2$ positive and odd, the system of equations (3.6), (3.7) has a solution only when $(b_1, b_2) = (1, 1)$. Since $b_1$, $b_2$ are factors of $n$, we next show that none of the $q_j$ divides $b_1 b_2$ in Lemma 3.3.2 and that none of the $p_j$ divides $b_1 b_2$ in Lemma 3.3.3. We extend the argument employed by Iskra in [28] that dealt with the case when $n$ has all its prime factors in the form $8k + 3$.

**Lemma 3.3.2.** *Let $(b_1, b_2)$ be an element of $R \times R$ such that $b_2$ is odd and positive. If $(b_1, b_2) \in Im(b)$, then $q_j$ does not divide $b_1 b_2$ for $j = 1,\ 2,\ \ldots, t$.*

*Proof.* We provide the argument when all pairs $(p_j, q_j) \equiv (5, 7) \pmod 8$. The proof is similar when all pairs $(p_j, q_j) \equiv (1, 3) \pmod 8$. Define

$$U = \{j : q_j | b_1 \text{ or } q_j | b_2\}.$$

It is enough to show that $U$ is the empty set. Suppose otherwise, and let $u$ be the least element of $U$. Let

$$b_i' = \begin{cases} \frac{b_i}{q_u}, & \text{if } q_u | b_i \\ b_i, & \text{if } q_u \nmid b_i \end{cases} \quad \text{and} \quad b_i'' = \begin{cases} \frac{b_i}{p_u}, & \text{if } p_u | b_i \\ b_i, & \text{if } p_u \nmid b_i \end{cases} \quad i = 1 \text{ or } 2.$$

By Remark 2,

$$\left(\frac{b_i'}{q_u}\right) = \begin{cases} -1, & \text{if } p_u | b_i \\ 1, & \text{if } p_u \nmid b_i, \end{cases} \text{ and } \left(\frac{b_i''}{p_u}\right) = \begin{cases} -1, & \text{if } q_u | b_i \\ 1, & \text{if } q_u \nmid b_i, \end{cases} \text{ for } i = 1,\ 2. \quad (3.15)$$

According to the definition of $u$, $q_u$ divides both $b_1$ and $b_2$ or exactly one of them. We consider these three cases separately.

**Case-1:** $q_u | b_1$ and $q_u | b_2$.
We have the following possibilities.

**Subcase-I:** $p_u \nmid b_1$ and $p_u \nmid b_2$.
From equation (3.7) we obtain $b_1 a_1^2 - b_1 b_2 a_3^2 \equiv 0 \pmod{p_u}$, i.e.,

$$a_1^2 \equiv b_2 a_3^2 \pmod{p_u}.$$

As $(a_1, a_3) = 1$, we have $\left(\frac{b_2}{p_u}\right) = 1$. But it is not possible, since $q_u$ is a divisor of $b_2$.

**Subcase-II:** $p_u \mid b_1$ and $p_u \mid b_2$.
Dividing both sides of equation (3.9) by $p_u$, we obtain $b_2''a_2^2 - b_1b_2''a_3^2 = -2n_u''d^2$, i.e.,

$$b_2''a_2^2 \equiv -2n_u''d^2 \pmod{p_u}.$$

Since $(a_2, d) = 1$, we have $\left(\frac{-2n_u''b_2''}{p_u}\right) = 1$. Consequently, $\left(\frac{b_2''}{p_u}\right) = 1$. It is not possible, since $q_u$ is a divisor of $b_2''$.

**Subcase-III:** $p_u | b_1$ but $p_u \nmid b_2$.
In this case,

$$\left(\frac{b_2'}{q_u}\right) = -\left(\frac{b_1'}{q_u}\right) = 1.$$

Dividing both sides of equation (3.7) by $q_u$, we obtain $b_1'a_1^2 - b_1'b_2a_3^2 = -n_u'd^2$. Hence,

$$b_1'a_1^2 \equiv -n_u'd^2 \pmod{q_u}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_u'b_1'}{q_u}\right) = \left(\frac{-1}{q_u}\right)\left(\frac{n_u'}{q_u}\right)\left(\frac{b_1'}{q_u}\right) = 1$. It follows that

$$\left(\frac{n_u'}{q_u}\right) = 1. \tag{3.16}$$

On the other hand, division of both sides of (3.9) by $q_u$ yields $b_2'a_2^2 - b_1b_2'a_3^2 = -2n_u'd^2$. Hence,

$$b_2'a_2^2 \equiv -2n_u'd^2 \pmod{q_u}.$$

As $(a_2, d) = 1$, we have $\left(\frac{-2n_u'b_2'}{q_u}\right) = \left(\frac{-1}{q_u}\right)\left(\frac{2}{q_u}\right)\left(\frac{b_2'}{q_u}\right)\left(\frac{n_u'}{q_u}\right) = 1$. It follows that $\left(\frac{n_u'}{q_u}\right) = -1$, which contradicts (3.16).

**Subcase-IV:** $p_u \nmid b_1$ and $p_u | b_2$.
This case can be ruled out in a similar way as above.

**Case-2:** $q_u | b_1$ and $q_u \nmid b_2$.
As before, we consider the following subcases.

**Subcase-I:** $p_u \nmid b_1$ and $p_u \nmid b_2$.
From equation (3.6) we have

$$b_1a_1^2 \equiv b_2a_2^2 \pmod{p_u}.$$

Since $(a_1, a_2) = 1$, we have $\left(\frac{b_1b_2}{p_u}\right) = 1$, which is impossible, since $q_u | b_1$ but not $b_2$.

**Subcase-II:** $p_u | b_1$ and $p_u \mid b_2$.
Equation (3.6) gives us $b_2a_2^2 \equiv 0 \pmod{q_u}$. It follows that $a_2$ is divisible by $q_u$, and $\frac{a_2^2}{q_u}$ is divisible by $q_u$. Dividing both sides of equation (3.8) by $q_u$, we obtain $2b_1'a_1^2 - b_2\frac{a_2^2}{q_u} - b_1'b_2a_3^2 =$

0 and consequently,

$$2a_1^2 \equiv b_2 a_3^2 \pmod{q_u}.$$

Now, $(a_1, a_3) = 1$ implies $\left(\frac{2b_2}{q_u}\right) = 1$, which is a contradiction since $p_u$ divides $b_2$.

**Subcase-III:** $p_u | b_1$ and $p_u \nmid b_2$.
Equation (3.6) gives us $a_2$ is divisible by $p_u$. Now dividing both sides of equation (3.9) by $p_u$, we obtain $b_2 \frac{a_2^2}{p_u} - b_1'' b_2 a_3^2 = -2n_u'' d^2$, i.e.,

$$b_1'' b_2 a_3^2 \equiv 2n_u'' d^2 \pmod{p_u}. \tag{3.17}$$

Since $(a_3, d) = 1$, it follows that $\left(\frac{2n_u'' b_1'' b_2}{p_u}\right) = 1$. But

$$\left(\frac{2n_u'' b_1'' b_2}{p_u}\right) = \left(\frac{2}{p_u}\right)\left(\frac{n_u''}{p_u}\right)\left(\frac{b_1''}{p_u}\right)\left(\frac{b_2}{p_u}\right) = (-1)\cdot(-1)\cdot(-1)\cdot 1 = -1,$$

a contradiction to (3.17).

**Subcase-IV:** $p_u \nmid b_1$ and $p_u \mid b_2$.
The argument is similar to the previous one.

**Case-3:** $q_u \nmid b_1$ and $q_u \mid b_2$.
We consider following subcases.

**Subcase-I:** $p_u \nmid b_1$.
Equation (3.6) gives us $b_1 a_1^2 \equiv 0 \pmod{q_u}$. It follows that $a_1$ is divisible by $q_u$, and $\frac{a_1^2}{q_u}$ is divisible by $q_u$. Dividing both sides of equation (3.8) by $q_u$, we obtain $2b_1 \frac{a_1^2}{q_u} - b_2' a_2^2 - b_1 b_2' a_3^2 = 0$ and consequently,

$$a_2^2 \equiv -b_1 a_3^2 \pmod{q_u}.$$

Now, $(a_2, a_3) = 1$ implies $\left(\frac{-b_1}{q_u}\right) = 1$, which is a contradiction because $p_u$ does not divide $b_1$.

**Subcase-II:** $p_u \mid b_1$ and $p_u \mid b_2$.
From equation (3.7) we have

$$b_1'' a_1^2 \equiv -n_u'' d^2 \pmod{p_u}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_u'' b_1''}{p_u}\right) = 1$, which is impossible since $q_u \nmid b_1$.

**Subcase-III:** $p_u | b_1$ and $p_u \nmid b_2$.
Equation (3.6) gives us $a_2$ is divisible by $p_u$. Dividing both sides of equation (3.6) by $p_u$, we obtain $b_1'' a_1^2 - b_2 \frac{a_2^2}{p_u} = n_u'' d^2$. Clearly,

$$b_1'' a_1^2 \equiv n_u'' d^2 \pmod{p_u}. \tag{3.18}$$

Since $(a_1, d) = 1$, $\left(\frac{n_u'' b_1''}{p_u}\right) = 1$. But

$$\left(\frac{n_u'' b_1''}{p_u}\right) = \left(\frac{n_u''}{p_u}\right)\left(\frac{b_1''}{p_u}\right) = (-1) \cdot 1 = -1,$$

a contradiction to (3.18).

Therefore, we can conclude that $u = \min U$ does not exist, i.e., $U$ is empty. So, none of the prime factors $q_j$ of $n$ divides $b_1 b_2$. □

**Lemma 3.3.3.** *Let $(b_1, b_2)$ be an element of $R \times R$ such that $b_2$ is odd and positive. If $(b_1, b_2) \in Im(b)$, then $p_j$ does not divide $b_1 b_2$ for $j = 1, 2, \ldots, t$.*

*Proof.* We provide the argument when all prime pairs in the factorization of $n$ satisfy $(p_j, q_j) \equiv (5, 7) \pmod 8$. The proof is similar when all pairs $(p_j, q_j) \equiv (1, 3) \pmod 8$. Let us define

$$V = \{j : p_j | b_1 \text{ or } p_j | b_2\}.$$

It suffices to show that $V$ is empty. If possible, let $V$ be non-empty and $v$ be the least element of $V$. Let

$$b_{i,v} = \begin{cases} \frac{b_i}{p_v}, & \text{if } p_v | b_i \\ b_i, & \text{if } p_v \nmid b_i \end{cases} \qquad i = 1, 2.$$

Since $q_j \nmid b_1 b_2$, for all $j \in \{1, 2, \ldots, t\}$, we have

$$\left(\frac{b_{1,v}}{p_v}\right) = \left(\frac{b_{2,v}}{p_v}\right) = 1.$$

We need to consider the following three cases.

**Case-A:** $p_v | b_1$ and $p_v | b_2$.
Dividing equation (3.7) by $p_v$, we have $b_{1,v} a_1^2 - b_{1,v} b_2 a_3^2 = -n_v'' d^2$. Clearly,

$$b_{1,v} a_1^2 \equiv -n_v'' d^2 \pmod{p_v}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_v'' b_{1,v}}{p_v}\right) = 1$. It follows that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (3.10).

**Case-B:** $p_v | b_1$ and $p_v \nmid b_2$.
From equation (3.6) we have $a_2 \equiv 0 \pmod{p_v}$. Therefore, $b_{1,v} a_1^2 - b_2 \frac{a_2^2}{p_v} = n_v'' d^2$, and

$$b_{1,v} a_1^2 \equiv n_v'' d^2 \pmod{p_v}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{n_v'' b_{1,v}}{p_v}\right) = 1$. It follows that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (3.10).

**Case-C:** $p_v \nmid b_1$ and $p_v \mid b_2$.

From equation (3.6) we have $a_1 \equiv 0$ in modulo $p_v$. Therefore, $b_1\frac{a_1^2}{p_v} - b_{2,v}a_2^2 = n_v''d^2$ and

$$-b_{2,v}a_2^2 \equiv n_v''d^2 \pmod{p_v}.$$

Since $(a_2, d) = 1$, we have $\left(\frac{-n_v''b_{2,v}}{p_v}\right) = 1$. But it implies that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (3.10). □

By Lemmas 3.3.2 and 3.3.3, we can conclude that if $(b_1, b_2) \in Im(b)$ with $b_1b_2 > 0$ and $b_2$ odd as well as positive, then $b_2 = 1 = b_1$. Hence, Theorem 3.1.1 follows from Theorem 2.4.1 and Proposition 2.4.3, and Corollary 3.2.2.

## 3.4 Proof of Theorem 3.1.2

Let the 2-adic valuation of a rational number $c$ by $v_2(c)$. Then following Remark will help us to proof Theorem 3.1.2

**Remark 3.4.1.** *By Theorem 2.4.1, Remark 2.4.2 and Lemma 3.2.1, $n$ is non-congruent if the system of Diophantine equations (3.6) and (3.7), or equivalently (3.8) and (3.9), does not have solution $(a_1, a_2, a_3, d)$ in $(\mathbb{Z}^\times)^4$ where $(a_i, d) = 1$ for all $i = 1, 2, 3$ and*

$$(b_1, b_2) \in D := R \times R \ \setminus \ \{(1, 1),\ (-1, -n),\ (n, 2),\ (-n, -2n)\},$$

*where*

$$R = \{\pm 2^{\epsilon}p_1^{\epsilon_1} \dots p_t^{\epsilon_t}q^{\mu} \ \mid \ \epsilon,\ \epsilon_1,\ \dots,\ \epsilon_t,\ \mu \in \{0, 1\}\}.$$

*Furthermore, it is enough to rule out solutions when $b_1$, $b_2$ are both positive and $(v_2(b_1), v_2(b_2))$ is either $(0, 0)$ or $(1, 0)$ by Proposition 2.4.3 and Lemma 3.3.1.*

*Proof of Theorem 3.1.2.* In view of Remark 3.4.1, we need to consider following two cases.
**Case:** $(v_2(b_1), v_2(b_2)) = (0, 0)$
Suppose there exists some $p_i$ that divides $b_1b_2$. Let

$$u = \min\{i : p_i | b_1b_2\}.$$

Define

$$b_i' = \begin{cases} b_i & \text{if } p_u \nmid b_i \\ \frac{b_i}{p_u} & \text{if } p_u \mid b_i \end{cases}$$

for $i = 1, 2$. Under the given conditions, we have

$$\left(\frac{b_1'}{p_u}\right) = \left(\frac{b_2'}{p_u}\right) = 1. \tag{3.19}$$

First, suppose $p_u|b_1$ and $p_u|b_2$. Then by (3.8), $\left(\frac{2b_1'b_2'}{p_u}\right) = 1$ which contradicts (3.19). Secondly, if $p_u|b_1$ and $p_u \nmid b_2$ then by equation (3.6) we have $p_u \mid a_2$, $p_u \nmid a_1$, whereas $p_u \nmid a_3$ by equation (3.9). Consequently, by equation (3.8) we have $\left(\frac{2b_2'}{p_u}\right) = 1$ which contradicts (3.19). The case $p_u \nmid b_1$ and $p_u \mid b_2$ can be ruled out in similar fashion. From equations (3.6)-(3.9), it is clear that $(b_1, b_2)$ is either equivalent to $(1, 1)$ or $(5, 3)$ modulo 8. Therefore, $q \nmid b_1b_2$ if $p_i$ does not divide $b_1b_2$. Thus $b_1 = b_2 = 1$, which is a contradiction.

**Case:** $(v_2(b_1), v_2(b_2)) = (1, 0)$
From equations (3.6) and (3.8), $a_2$ and $a_3$ are even but $a_1$ is odd. By equation (3.9), $a_2 \equiv 2 \pmod 4$. Let $b_{12} = \frac{b_1}{2}$. If $a_3 \equiv 2 \pmod 4$ then from equations (3.7) and (3.8) we have $b_{12} \equiv 7b_2 \equiv 7 \pmod 8$. If $a_3 \equiv 0 \pmod 4$ then $b_{12} \equiv 3 \pmod 8$ by (3.7) and then, $b_2 \equiv 3 \pmod 8$ by equation (3.9). Therefore,

$$(b_1, b_2) = (2b_{12}, b_2) \equiv \begin{cases} (2 \cdot 7, 1) \pmod 8 & \text{if } a_3 \equiv 2 \pmod 4, \\ (2 \cdot 3, 3) \pmod 8 & \text{if } a_3 \equiv 0 \pmod 4. \end{cases}$$

Let us define

$$b_i'' = \begin{cases} b_i & \text{if } q \nmid b_i \\ \frac{b_i}{q} & \text{if } q \mid b_i, \end{cases} \quad \text{and } n_q = \frac{n}{q}.$$

Suppose $(b_1, b_2) \equiv (2 \cdot 7, 1) \pmod 8$, then $q \mid b_1$, $q \nmid b_2$ and an even number of $p_i$'s divide $b_1$. By (3.6), $q \mid a_2$ and

$$\left(\frac{b_1''}{q}\right) = -\left(\frac{n_q}{q}\right) = 1. \tag{3.20}$$

But from equation (3.6) we have $\left(\frac{n_q b_1''}{q}\right) = 1$, which contradicts (3.20).

Now suppose $(b_1, b_2) \equiv (2 \cdot 3, 3) \pmod 8$, then $q \nmid b_1b_2$, and an odd number of $p_i$'s divide $b_1$. Therefore,

$$\left(\frac{b_1}{q}\right) = -1. \tag{3.21}$$

But from equation (3.9) we have $\left(\frac{b_1}{q}\right) = 1$, which contradicts (3.21). We are done. □

## 3.5 Infinitude of the Families

In this section, we show that Theorem 3.1.1 and 3.1.2 provides infinitely many families of non-congruent numbers and each family has infinitely many members by proving Proposition 3.1.3.

*Proof of Proposition 3.1.3.* We use Dirichlet's theorem on primes in arithmetic progres-

sion and apply induction on $t$. The case when $t = 1$ is trivial, since we can take any $q_1 \equiv 3 \pmod 8$ and $p_1 \equiv 1 \pmod 8$, $p_1 \equiv 2 \pmod{q_1}$. Suppose $t > 1$. By the induction hypothesis, we know that there exists an integer $n_{t-1} = (p_1q_1)(p_2q_2)\cdots(p_{t-1}q_{t-1})$ where $p_1, p_2, \ldots, p_{t-1}$ and $q_1, q_2, \ldots, q_{t-1}$ are distinct primes such that $p_j \equiv 1 \pmod 8$ and $q_j \equiv 3 \pmod 8$ for all $1 \leq j \leq t-1$ satisfying (3.1).

It is enough if we can choose primes $p_t$ and $q_t$ satisfying

$$q_t \equiv \begin{cases} 3 & \pmod 8, \\ \alpha & \pmod{n_{t-1}}, \end{cases} \tag{3.22}$$

and

$$p_t \equiv \begin{cases} 1 & \pmod 8, \\ \beta & \pmod{n_{t-1}}, \\ \gamma & \pmod{q_t}, \end{cases} \tag{3.23}$$

where $\alpha$, $\beta$ is any quadratic residue modulo $n_{t-1}$ and $\gamma$ is any quadratic non-residue modulo $q_t$, e.g., $\alpha = 1 = \beta$, $\gamma = 2$. The Chinese Remainder Theorem guarantees that both the systems of congruences (3.22) and (3.23) have a solution. By applying this theorem in conjunction with Dirichlet's theorem on primes in arithmetic progression and quadratic reciprocity, we can conclude that there exist infinitely many primes $p_t$ and $q_t$ satisfying the system of congruences given by (3.23) and (3.22), respectively.

The analogous statement, when all the prime pairs $(p_j, q_j)$ in the factorization of $n$ are equivalent to $(5, 7)$ modulo 8, can be proved similarly. □

The infinitude of the families in Theorem 3.1.2 follows similarly.

## 3.6 Examples

**Example 1.** Consider $n = (17 \cdot 3) \cdot (409 \cdot 19) \cdot (3697 \cdot 859)$, where each pair of prime factors is equivalent to $(1, 3)$ modulo 8 and satisfy the hypotheses (3.1) of Theorem 3.1.1. Using MAGMA [4], we verify that the rank of the elliptic curve $y^2 = x^3 - n^2x$ is 0, hence $n$ is non-congruent. We further verify that $(17 \cdot 3) \cdot (409 \cdot 19)$, $(17 \cdot 3) \cdot (3697 \cdot 859)$ and $(409 \cdot 19) \cdot (3697 \cdot 859)$ are non-congruent too, as implied by Theorem 3.1.1.

**Example 2.** Consider $n = (5 \cdot 7) \cdot (29 \cdot 79) \cdot (821 \cdot 151)$ where each pair of prime factors is equivalent to $(5, 7)$ modulo 8 and satisfy the hypotheses (3.1) of Theorem 3.1.1. Using MAGMA [4], we verify that the rank of the elliptic curve $y^2 = x^3 - n^2x$ is 0, hence $n$ is non-congruent. We further verify that $(5 \cdot 7) \cdot (29 \cdot 79)$, $(5 \cdot 7) \cdot (821 \cdot 151)$ and $(29 \cdot 79) \cdot (821 \cdot 151)$ are non-congruent too, as implied by Theorem 3.1.1.

**Example 3.** $n = 2(3 \cdot 19 \cdot 139) \cdot 7$ satisfy the hypotheses (3.2) of Theorem 3.1.2. Using MAGMA [4], we verify that the rank of the elliptic curve $y^2 = x^3 - n^2x$ is 0, hence $n$ is non-congruent.

# CHAPTER 4

# NON-CONGRUENT FAMILIES BY MONSKY MATRICES

## 4.1 Introduction

In this chapter, we use Monsky matrices (see 2.5) to construct infinitely many new families of non-congruent numbers. Monksy matrices have been used by Reinholz, Spearman & Yang [43], [44], [45] to construct new families of non-congruent numbers which have arbitrarily many prime factors in a certain congruence class modulo 8 together with at most 3 odd prime factors in different congruence classes modulo 8. Similarly, Cheng & Guo [9] constructed families of non-congruent numbers with arbitrarily many prime factors of the form $8k+3$. We construct infinite families of non-congruent numbers containing arbitrarily many triplets of prime factors. From now on, $t$ denotes a positive integer. The main results of this chapter can be stated as follows.

**Theorem 4.1.1.** *Let $p_1, p_2, \ldots, p_t$; $q_1, q_2, \ldots, q_t$ and $r_1, r_2, \ldots, r_t$ be distinct primes such that all triples $(p_j, q_j, r_j)$ are equivalent to $(1,3,3)$ modulo 8. Assume that*

$$\begin{aligned}
&\left\{\left(\left(\frac{p_i}{p_j}\right),\left(\frac{q_i}{q_j}\right),\left(\frac{r_i}{r_j}\right)\right) : i<j\right\} \text{ is a singleton subset of } \{(1,\pm 1,\pm 1)\},\\
&\left(\frac{p_i}{q_j}\right)=\left(\frac{p_i}{r_j}\right)=1 \quad \text{if } i\neq j \text{ and } \left(\frac{q_i}{r_j}\right)=1 \text{ for all } i,j,\\
&\left(\frac{p_i}{q_i}\right)=-\left(\frac{p_i}{r_i}\right) \text{ for all } i.
\end{aligned} \tag{4.1}$$

*Then $n=(p_1q_1r_1)(p_2q_2r_2)\cdots(p_tq_tr_t)$ and $2n$ are non-congruent numbers.*

**Theorem 4.1.2.** *Let $p_1, p_2, \ldots, p_t$; $q_1, q_2, \ldots, q_t$ and $r_1, r_2, \ldots, r_t$ be distinct primes such*

*that all triples* $(p_j, q_j, r_j)$ *are equivalent to* $(5, 7, 7)$ *modulo* 8. *Assume that*

$$\begin{aligned} \left(\frac{p_i}{p_j}\right) = \left(\frac{p_i}{q_j}\right) = \left(\frac{p_i}{r_j}\right) = \left(\frac{q_i}{r_j}\right) = 1 \quad \textit{for all } i \neq j \\ \left(\frac{p_i}{q_i}\right) = -\left(\frac{p_i}{r_i}\right) = \left(\frac{q_i}{r_i}\right) = -1 \quad \textit{for all } i. \end{aligned} \tag{4.2}$$

*Then* $n = 2(p_1q_1r_1)(p_2q_2r_2)\cdots(p_tq_tr_t)$ *is a non-congruent number.*

We prove these results in the next section by showing that the corresponding Monsky matrices have non-vanishing determinant.

## 4.2 Proof of Theorems 4.1.1-4.1.2

The following notation simplifies the description of Monsky matrices that we are about to consider.

$\mathbf{O}$ : $t \times t$ zero matrix,
$\mathbf{I}$ : $t \times t$ identitity matrix,
$\mathbf{N}$ : $t \times t$ matrix having all the entries 1,
$\mathbf{R}$ : $t \times t$ matrix satisfying $\mathbf{R} = \mathbf{N} - \mathbf{I}$,
$\mathbf{U}_f$ : $t \times t$ upper-triangular matrix with all diagonal entries $(t-i)+f$, and all upper-diagonal entries 1,
$\mathbf{L}_f$ : $t \times t$ lower-triangular matrix with all diagonal entries $f+(i-1)$, and all lower-diagonal entries 1.

$$\mathbf{T}_{l,f} = \begin{cases} \mathbf{L}_f & \text{if } \left(\frac{l_i}{l_j}\right) = -1 \text{ for all } i < j, \\ \mathbf{U}_f & \text{if } \left(\frac{l_i}{l_j}\right) = 1 \text{ for all } i < j, \end{cases}$$

where $l \in \{p, q, r\}$. For any matrix, we denote $m$-th row by $R_m$ and $m$-th column by $C_m$. The following lemma is immediate.

**Lemma 4.2.1.** *With* $\mathbf{T}_{l,f}$ *defined as above, we have*

*(a)* $\mathbf{T}_{l,f}\mathbf{T}_{l,f+1} \equiv \mathbf{O} \pmod 2$,

*(b)* $\mathbf{T}_{l,f}\mathbf{T}_{l,f}^T \equiv f\mathbf{N} \pmod 2$,

*(c)* $\mathbf{T}_{l,f}^T\mathbf{T}_{l,f} \equiv (t-1+f)\mathbf{N} \pmod 2$.

Theorems 4.1.1-4.1.2 are proven by forming the Monsky matrix $\mathbf{M}_o$ and $\mathbf{M}_e$ corresponding to $n$ and computing its determinant. Since it is enough to show non-vanishing

of the determinant of the Monsky matrices in $\mathbb{F}_2$, we often write equality instead of equivalence modulo 2 by a slight abuse of notation.

*Proof of Theorem 4.1.1*: We write $n$ as $2^{\epsilon}(p_1p_2\cdots p_t)(q_1q_2\cdots q_t)(r_1r_2\cdots r_t)$, where $\epsilon \in \{0,1\}$. As $p_i \equiv 1 \pmod 8$ and $q_i \equiv r_i \equiv 3 \pmod 8$, we have

$$\mathbf{D}_2 = \mathbf{D}_{-1} = \left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{I} \end{array}\right], \quad \mathbf{D}_{-2} = \left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \end{array}\right], \quad \text{and}$$
$$\mathbf{A} = \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{D}_{pq} & \mathbf{T}_{q,t} + \mathbf{D}_{pq} & \mathbf{N} \\ \hline \mathbf{D}_{pr} & \mathbf{O} & \mathbf{T}_{r,0} + \mathbf{D}_{pr} \end{array}\right], \tag{4.3}$$

where $\mathbf{D}_{lk}$ is a diagonal matrix with

$$\mathbf{D}_{lk}(i,i) = \begin{cases} 0 & \text{if } \left(\frac{k_i}{l_i}\right) = 1, \\ 1 & \text{if } \left(\frac{k_i}{l_i}\right) = -1, \end{cases} \qquad \text{for all } l,k \in \{p,q,r\}.$$

It is easy to notice that by the given conditions we obtain

$$\mathbf{D}_{pq} + \mathbf{D}_{pr} = \mathbf{I}, \quad \mathbf{D}_{pq}\mathbf{D}_{pr} = \mathbf{O}, \quad \mathbf{D}_{pq}^2 = \mathbf{D}_{pq} \text{ and } \mathbf{D}_{pr}^2 = \mathbf{D}_{pr}. \tag{4.4}$$

(a) Now by (2.12)

$$\mathbf{M}_o = \left[\begin{array}{c|c|c|c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{D}_{pq} & \mathbf{T}_{q,t+1} + \mathbf{D}_{pq} & \mathbf{N} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{D}_{pr} & \mathbf{O} & \mathbf{T}_{r,1} + \mathbf{D}_{pr} \\ \hline \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{D}_{pq} & \mathbf{T}_{q,t} + \mathbf{D}_{pq} & \mathbf{N} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{D}_{pr} & \mathbf{O} & \mathbf{T}_{r,0} + \mathbf{D}_{pr} & \mathbf{O} & \mathbf{O} & \mathbf{I} \end{array}\right].$$

By swapping of rows ($R_i$ with $R_{3t+i}$ for $1 \le i \le t$), and applying Lemmas 2.1.6, 4.2.1 together with (4.4), we find that $\mathbf{M}_o$ is invertible if and only if

$$\mathbf{M}_o' = \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{T}_{q,t}\mathbf{D}_{pq} + \mathbf{N}\mathbf{D}_{pr} & \mathbf{T}_{q,t}\mathbf{D}_{pq} + \mathbf{I} & \mathbf{T}_{q,t}\mathbf{N} + \mathbf{N}(\mathbf{T}_{r,1} + \mathbf{D}_{pr}) \\ \hline \mathbf{T}_{r,0}\mathbf{D}_{pr} & \mathbf{O} & \mathbf{T}_{r,0}\mathbf{D}_{pr} + \mathbf{I} \end{array}\right]$$

is invertible over $\mathbb{F}_2$. Column operation $C_{2t+i} \to C_i + C_{2t+i}$ on $\mathbf{M}_o'$ for all $1 \le i \le t$ followed

by Lemma 2.1.6 and (4.4) gives $\det \mathbf{M}'_o$ modulo 2 as

$$\det\left(\left[\begin{array}{c} \mathbf{T}_{q,t}\mathbf{D}_{pq}+\mathbf{N}\mathbf{D}_{pr} \\ \hline \mathbf{T}_{r,0}\mathbf{D}_{pr} \end{array}\right]\left[\begin{array}{c|c} \mathbf{D}_{pq} & \mathbf{D}_{pq} \end{array}\right]+\left[\begin{array}{c|c} \mathbf{T}_{q,t}\mathbf{D}_{pq}+\mathbf{I} & \mathbf{T}_{q,t}(\mathbf{N}+\mathbf{D}_{pq})+\mathbf{N}\mathbf{T}_{r,1} \\ \hline \mathbf{O} & \mathbf{I} \end{array}\right]\right)$$
$$\equiv \det\left[\begin{array}{c|c} \mathbf{I} & \bigstar \\ \hline \mathbf{O} & \mathbf{I} \end{array}\right] \equiv 1.$$

(b) By (2.12)

$$\mathbf{M}_e = \left[\begin{array}{c|c|c|c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{D}_{pq} & \mathbf{T}_{q,t+1}+\mathbf{D}_{pq} & \mathbf{N} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{D}_{pr} & \mathbf{O} & \mathbf{T}_{r,1}+\mathbf{D}_{pr} \\ \hline \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{D}_{pq} & \mathbf{T}^T_{q,t+1}+\mathbf{D}_{pq} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{D}_{pr} & \mathbf{N} & \mathbf{T}^T_{r,1}+\mathbf{D}_{pr} & \mathbf{O} & \mathbf{O} & \mathbf{I} \end{array}\right].$$

Swapping rows ($R_i$ with $R_{3t+i}$ for $1 \le i \le t$) and applying Lemma 2.1.6, 4.2.1 together with (4.4) ensure that $\mathbf{M}_e$ is invertible if and only if

$$\mathbf{M}'_e = \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{T}^T_{q,t+1}\mathbf{D}_{pq} & \mathbf{T}^T_{q,t+1}\mathbf{D}_{pq}+\mathbf{I} & \mathbf{T}^T_{q,t+1}\mathbf{N} \\ \hline \mathbf{N}\mathbf{D}_{pq}+\mathbf{T}^T_{r,1}\mathbf{D}_{pr} & \mathbf{N}(\mathbf{T}_{q,t+1}+\mathbf{D}_{pq}) & \mathbf{T}^T_{r,1}\mathbf{D}_{pr}+\mathbf{I} \end{array}\right]$$

is invertible over $\mathbb{F}_2$. Column operation $C_{t+i} \to C_i + C_{t+i}$ on $\mathbf{M}'_e$ for all $1 \le i \le t$ followed by Lemma 2.1.6 and (4.4) we find that $\mathbf{M}'_e$ is invertible as

$$\left[\begin{array}{c|c} \mathbf{N}\mathbf{D}_{pq}+\mathbf{T}^T_{r,1}\mathbf{D}_{pr} & \mathbf{N}\mathbf{T}_{q,t+1}+\mathbf{T}^T_{r,1}\mathbf{D}_{pr} \end{array}\right]\left[\begin{array}{c|c} \mathbf{I}+\mathbf{D}_{pr}\mathbf{T}^T_{q,t+1}\mathbf{D}_{pq} & \mathbf{D}_{pr} \\ \hline \mathbf{T}^T_{q,t+1}\mathbf{D}_{pq} & \mathbf{I} \end{array}\right]\left[\begin{array}{c} \mathbf{D}_{pr} \\ \hline \mathbf{T}^T_{q,t+1}\mathbf{N} \end{array}\right]$$
$$+\left[\mathbf{I}+\mathbf{T}^T_{r,1}\mathbf{D}_{pr}\right]$$

is equivalent to the identity matrix modulo 2.

*Proof of Theorem 4.1.2*: We write $n$ as $2^\epsilon(p_1p_2\cdots p_t)(q_1q_2\cdots q_t)(r_1r_2\cdots r_t)$. By (2.11), we have

$$\mathbf{D}_2 = \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \end{array}\right], \quad \mathbf{D}_{-1} = \left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{I} \end{array}\right], \text{ and } \mathbf{A} = \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{I} & \mathbf{X}_q+t\mathbf{I} & \mathbf{R} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{X}_r+I \end{array}\right],$$

where

$$\mathbf{X}_l(i,j) = \begin{cases} 0 & \text{if } \left(\frac{l_j}{l_i}\right) = 1, \\ 1 & \text{if } \left(\frac{l_j}{l_i}\right) = -1, \end{cases} \qquad \text{for all } l \in \{p,q,r\}.$$

By (2.12), we have

$$\mathbf{M}_e = \left[\begin{array}{c|c|c|c|c|c} \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{X}_q + t\mathbf{I} & \mathbf{R} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{X}_r + \mathbf{I} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{I} & \mathbf{X}_q^T + t\mathbf{I} & \mathbf{I} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{R} & \mathbf{X}_r^T + \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{I} \end{array}\right].$$

By swapping rows ($R_{t+i}$ with $R_{3t+i}$ for $1 \le i \le t$) and applying Lemma 2.1.6, we find that the non-singularity of $\mathbf{M}_e$ follows from that of

$$\left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{X}_r + \mathbf{I} \end{array}\right] \left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{I} & \mathbf{X}_q^T + t\mathbf{I} & \mathbf{I} \\ \hline \mathbf{O} & \mathbf{R} & \mathbf{X}_r + \mathbf{I} \end{array}\right] + \left[\begin{array}{c|c|c} \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{O} \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{O} & \mathbf{X}_q^T + t\mathbf{I} & \mathbf{I} \\ \hline \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \hline \mathbf{I} & \bigstar_1 & \bigstar_2 \end{array}\right].$$

## 4.3 Infinitude of the Families and Examples

**Remark 4.3.1.** *One can show here exist infinitely many triplets of primes that satisfy the hypotheses of Theorems 4.1.1 and 4.1.2. The proof essentially follows from Dirichlet's theorem on primes in arithmetic progression together with the Chinese remainder theorem, just like the proof of Proposition 3.1.3 in the previous chapter.*

We conclude by furnishing some examples that illustrate our results.

| Theorem | Hypothesis | $t$ | Non-congruent number |
|---|---|---|---|
| Theorem 4.1.1 | (4.1) | $t = 2$, odd case | $(17 \cdot 19 \cdot 3)(457 \cdot 67 \cdot 179)$ |
| | | $t = 2$, even case | $2 \cdot (17 \cdot 19 \cdot 3) \cdot (457 \cdot 67 \cdot 179)$ |
| Theorem 4.1.2 | (4.2) | $t = 2$ | $2 \cdot (5 \cdot 19 \cdot 71) \cdot (29 \cdot 79 \cdot 439)$ |

# CHAPTER 5

# $\theta$-CONGRUENT NUMBER OVER NUMBER FIELDS

## 5.1 Introduction

In this chapter, we prove a criterion for a natural number $n$ to be $\theta$-congruent over certain classes of real number fields $K$. In particular, we show that any triangle with sides in $K$ corresponding to a $\theta$-congruent number $n$ over $K$ arises from a non-torsion point on the $\theta$-congruent number elliptic curve $E_{n,\theta}(K)$ (see section 1.2). Thus, our results in this chapter imply that existence of one such triangle guarantees existence of infinitely many such triangles. Examining the torsion part of $E_{n,\theta}(K)$ is crucial for this chapter. Much progress has been made concerning the torsion of elliptic curves over number fields, especially when the degree of the number field is small (see [23], [24], [22], [12]). When the elliptic curve has complex multiplication (CM), more information is available for the torsion group over number fields (e.g., see [41]). The congruent number elliptic curve has complex multiplication. But we find that the $\theta$-congruent number elliptic curve (given by (1.4)) does not have CM for $\theta \neq \frac{\pi}{2}$ (Proposition 5.3.1). Hence the study of the torsion subgroup of the latter requires somewhat more care. Motivated by [30], this chapter provides a criterion for determining whether a square-free positive integer $n$ is $\theta$-congruent number over certain classes of real number fields (Theorems 5.1.1, 5.1.2 and 5.1.3).

Let $K_{2,d}$ denotes the real number field of type $(2, \ldots, 2)$, i.e.,

$$K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_d}),$$

where $m_i$ are distinct square-free natural numbers such that any two distinct $m_i$, $m_j$ do not divide one another. It follows that $[K_{2,d} : \mathbb{Q}] = 2^d$. We prove the following analogue of Criterion 2.3.7 for $\theta$-congruent number over $K_{2,d}$.

**Theorem 5.1.1.** *Assume that $n \neq 1, 2, 3, 6$ is a square free natural number and $2r(r-s)$ is not a square in $K_{2,d}$. Then $n$ is $\theta$-congruent number over $K_{2,d}$ if and only if $E_{n,\theta}(K_{2,d})$ has a point of infinite order.*

Following two Theorems are analogues of Theorem 5.1.1 for real number fields $K$ other than multi-quadratic fields under certain restrictions.

**Theorem 5.1.2.** *Suppose $n$ is a square free natural number other than 1, 2, 3 or 6. Let $K$ be a real number field such that $[K : \mathbb{Q}]$ is coprime to 6 and is not divisible by 55. Then $n$ is a $\theta$-congruent number over $K$ if and only if $E_{n,\theta}(K)$ has a point of infinite order.*

**Theorem 5.1.3.** *Suppose $n$ is a square free natural number other than 1, 2, 3 or 6. Let $K$ be a real cubic number field. Suppose $s$ is divisible by 5 or $(r, s) \equiv (\pm 2, \pm 1)$ or $\equiv (\pm 1, \pm 2) \pmod 5$. Then $n$ is a $\theta$-congruent number over $K$ if and only if $E_{n,\theta}(K)$ has a point of infinite order.*

In the following sections, we closely examine the torsion structure of the $\theta$-congruent number elliptic curve over these three types of number fields in order to prove the theorems.

## 5.2 Real Multi-Quadratic Fields

We need the following lemma to establish our results.

**Lemma 5.2.1.** *For every sub-field $K$ of $\mathbb{R}$, a natural number $n$ is $\theta$-congruent number over $K$ if and only if $E_{n,\theta}(K) \setminus E_{n,\theta}(K)[2] \neq \varnothing$.*

The essential argument for the proof of the lemma above is contained in Tada (Theorem 1 in [52]) who considered the case $\theta = \frac{\pi}{2}$ for real quadratic fields $K$. The analogue for real quadratic fields with $\theta$ of any rational cosine in [29] adopts the same approach as in [52]. In the case of real multiquadratic fields too, the proof similarly follows from a well-known result on elliptic curves stated below.

**Proposition 5.2.2.** *[33] Let $E$ be an elliptic curve over a field $k$ (char $k \neq 2, 3$) given by*

$$E : y^2 = (x - a_1)(x - a_2)(x - a_3) \text{ with } a_1, a_2, a_3 \in k.$$

*Let $(x_0, y_0)$ be a $k$-rational point of $E \setminus \{\mathcal{O}\}$. Then there exists a $k$-rational point $(x_1, y_1)$ of $E$ with $2(x_1, y_1) = (x_0, y_0)$ if and only if $x_0 - a_1$, $x_0 - a_2$ and $x_0 - a_3$ are squares in $k$.*

*Proof of Lemma 5.2.1.* Let $K$ be a real number field. For a positive integer $n$ and $\theta$ such that $\cos\theta = \frac{s}{r}$ with $s, r \in \mathbb{Z}$, Consider the two sets

$$S = \{(u, v, w) \in K^3 : 0 < u \leq v < w, \quad uv = 2rn, \quad u^2 + v^2 - 2uv.\frac{s}{r} = w^2\},$$

and

$$T = \{(x, y) \in 2E_{n,\theta}(K) \setminus \{\mathcal{O}\} : y \geq 0\}.$$

Define

$$\phi : S \to T, \qquad (u, v, w) \mapsto \Big(\frac{w^2}{4}, \frac{w(v^2 - u^2)}{8}\Big),$$

and $\psi : T \to S$ be the map sending $(x, y)$ to the tuple

$$(\sqrt{x + (r+s)n} - \sqrt{x - (r-s)n},\ \sqrt{x + (r+s)n} + \sqrt{x - (r-s)n},\ 2\sqrt{x}).$$

Using Proposition 5.2.2 it is easy to observe that the maps $\phi$ and $\psi$ are well defined, $\phi \circ \psi = 1_T$ and $\psi \circ \phi = 1_S$. It follows that $n$ is $\theta$-congruent over $K$ if and only if $T$ is nonempty. □

The following corollary is immediate from Lemma 5.2.1.

**Corollary 5.2.3.** *Assume that $E_{n,\theta}(K)_{tors} = E_{n,\theta}(K)[2]$ for any real number field $K$. Then $n$ is a $\theta$-congruent number over $K$ if and only if $E_{n,\theta}(K)$ has positive rank.*

**Lemma 5.2.4.** *$E_{n,\theta}(K_{2,d})_{tors}$ is a 2-group for $n \neq 1,\ 2,\ 3,\ 6$.*

*Proof.* Observe that the quadratic $m_i$-twist of the $\theta$-congruent number elliptic curve is given by

$$E^{m_i}_{n,\theta} : y^2 = x(x - m_i n(r - s))(x + m_i n(r + s)). \tag{5.1}$$

Thus $E^{m_i}_{n,\theta}$ is isomorphic to $E_{nm_i,\theta}$. By Proposition 1.2.6,

$$E^{m_i}_{n,\theta}(\mathbb{Q}) \cong E_{nm_i,\theta}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Hence due to the remark below Theorem 2 and Lemma 3 in [42], we can conclude that $E_{n,\theta}(K_{2,d})_{tors}$ is a 2-group. □

We are interested in showing that any point $(x, y) \in E_{n,\theta}(K_{2,d})$ with $y \neq 0$ is a point of infinite order. The points $(x, y)$ with $y = 0$ are precisely the 2-torsion points on $E_{n,\theta}$. While Lemma 5.2.4 rules out torsion points of odd order, we still need to rule out torsion points of order 4 or higher power of 2 in $E_{n,\theta}(K_{2,d})$.

**Lemma 5.2.5.** *Assume that $n$ is not a divisor of 6 and $2r(r-s)$ is not square in $K_{2,d}$, then $E_{n,\theta}(K_{2,d})_{tors} = E_{n,\theta}(K_{2,d})[2]$.*

*Proof.* It is enough to show that $E_{n,\theta}(K_{2,d})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since we know that there are exactly 3 elements of order 2 and $E_{n,\theta}(K_{2,d})_{tors}$ is a 2-group by Lemma 5.2.4, it suffices to show that $E_{n,\theta}(K_{2,d})_{tors}$ has no point of order 4.

Suppose, if possible, $P$ has order 4. Then $2P$ has order 2 and

$$2P \in \{(0,0),\ (-(r+s)n, 0),\ ((r-s)n,\ 0)\}.$$

By Proposition 5.2.2,

1. $2P = (0,0) \iff$ both $-(r+s)n,\ (r-s)n$ are squares in $K_{2,d}$, which is not possible because $K_{2,d}$ is a real sub-field.

2. $2P = (-(r+s)n, 0) \iff$ both $-(r+s)n,\ -2rn$ are squares in $K_{2,d}$, which is not possible for same reason as above.

3. $2P = ((r-s)n, 0) \iff$ both $(r-s)n,\ 2rn$ are squares in $K_{2,d}$. Then $2r(r-s)$ is a square in $K_{2,d}$, contrary to our assumption. □

Theorem 5.1.1 follows immediately from Corollary 5.2.3 and Lemma 5.2.5. We have the following consequences of Theorem 5.1.1.

**Corollary 5.2.6.** *Assume that $n$ is not a divisor of 6 and $2r(r-s)$ is not square in $K_{2,d}$. Then $n$ is a $\theta$-congruent number over $K_{2,d}$ if and only if at least one of the $2^d$ numbers $nm_1^{e_1}\cdots m_d^{e_d}$ $(e_i = 0, 1)$ is a $\theta$-congruent number over $\mathbb{Q}$.*

We require the following well known result to establish the corollary above.

**Proposition 5.2.7.** *[11] Suppose $E$ is elliptic curves over number field $k$. Let $D \in k \setminus k^2$ and $E^D$ be the quadratic $D$-twist of $E$. Then*

$$rank(E(k)) + rank(E^D(k)) = rank(E(k(\sqrt{D}))). \tag{5.2}$$

*Proof of Corollary 5.2.6.* Using (5.2) inductively and noting that $E_{n,\theta}^{m_i}$ is isomorphic to $E_{nm_i,\theta}$, we obtain

$$rank(E_{n,\theta}(K_{2,d})) = \sum rank(E_{nm_1^{e_1}\cdots m_d^{e_d},\theta}(\mathbb{Q})),$$

where summation is over all $d$-tuples $e_i \in \{0,1\}$. By Theorem 5.1.1 and Criterion 1.2.2, if $n$ is a $\theta$-congruent number then

$$rank(E_{n,\theta}(K_{2,d})) > 0 \iff rank(E_{nm_1^{e_1}\cdots m_d^{e_d},\theta}(\mathbb{Q})) > 0 \quad \text{for some } (e_1,\ldots,e_d),$$

which proves the corollary. □

**Corollary 5.2.8.** *$n$ is a $\theta$-congruent number over $K_{2,d}$, if and only if $n$ is a $\theta$-congruent number over $\mathbb{Q}$ or over some real quadratic field $\mathbb{Q}(\sqrt{m_1^{e_1}\cdots m_d^{e_d}})$ contained in $K_{2,d}$.*

*Proof.* Suppose $n$ is not a $\theta$-congruent number over $\mathbb{Q}$. By corollary 5.2.6, one of the $2^d$ numbers $nm_1^{e_1}\cdots m_d^{e_d}$, say $nr$ $(\neq n)$ is a $\theta$-congruent number over $\mathbb{Q}$. Then

$$rank(E_{nr,\theta}(\mathbb{Q})) > 0 \implies rank(E^r_{n,\theta}(\mathbb{Q})) > 0 \implies rank(E_{n,\theta}(\mathbb{Q}(\sqrt{r}))) > 0$$

by (5.1) and (5.2). Thus, $n$ is $\theta$-congruent number over $\mathbb{Q}(\sqrt{r})$. □

## 5.3 Real Number Fields of Degree Coprime to 6

We need to ensure that the torsion group $E_{n,\theta}(K)_{tors}$ does not grow bigger than $E_{n,\theta}(\mathbb{Q})_{tors}$. When the degree of $K$ over $\mathbb{Q}$ is not divisible by small primes, it is possible to restrict the torsion and obtain similar criteria for $\theta$-congruent numbers over $K$ as stated in Theorem 5.1.2 below.

In [30], it has been proved that $n$ is a congruent number over $K$ if and only if $E_n(K)$ has a point of infinite order, under the assumptions that (i) $K$ is a real number field such that $[K:\mathbb{Q}]$ is odd or $2p$, where $p$ is prime; and (ii) $\sqrt{2}, \sqrt{3}$ and $\sqrt{5} \notin K$. The proof depends crucially on the fact that congruent number elliptic curves have complex multiplication, hence their torsion groups over such number fields are well understood due to work of Silverberg [47], Prasad and Yogananda [41]. But the torsion of a $\theta$-congruent number elliptic curve poses somewhat more difficulty due to the proposition below.

**Proposition 5.3.1.** *The $\theta$-congruent number elliptic curve $E_{n,\theta}$ does not have complex multiplication for $\theta \neq \frac{\pi}{2}$.*

*Proof.* Given any number field $F$, there are only finitely many $\mathbb{C}$-isomorphism classes of elliptic curves over $F$ with complex multiplication, and each isomorphism class has a distinct $j$-invariant which must be an algebraic integer in $F$. By using SAGE, one can show that the $j$-invariant of a rational elliptic curve with complex multiplication must be one of the 13 integers $-262537412640768000$, $-147197952000$, $-884736000$, $-12288000$,

$-884736$, $-32768$, $-3375$, 0, 1728, 8000, 54000, 287496 or 16581375. The $j$-invariant of the elliptic curve $E_{n,\theta}$ given by the equation (1.4) is

$$j(E_{n,\theta}) = 2^6 \frac{(3r^2+s^2)^3}{r^2(r^2-s^2)^2}.$$

It is clear that $j(E_{n,\theta}) > 0$. By considering the numerator of $j(E_{n,\theta})$ modulo 5, we find that it is not divisible by 5 and hence it cannot be 8000, 54000 or 16581375 for any two coprime integers $r$ and $s$. By considering the numerator of $j(E_{n,\theta})$ modulo 11, we find that that it is not divisible by 11 either and hence it cannot be 287496 for any two coprime integers $r$ and $s$. Finally, $j(E_{n,\theta}) = 1728$ if and only if $s = 0$, i.e., $\theta = \frac{\pi}{2}$. □

Exploiting following work of González-Jiménez and Najman [23] on torsion subgroup of rational elliptic curves, we will prove Theorem 5.1.2.

**Proposition 5.3.2** ( Theorem 7.2 of [23]). *Let $B$ be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree $d$, where the smallest prime divisor of $d$ is $\geq B$. Let $E(K)[p^\infty]$ denote the $p$-primary torsion subgroup of $E(K)_{tors}$, that is, the $p$-Sylow subgroup of $E(K)$. Then*

*(i). If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*(ii). If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

*(iii). If $B \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5,\ 7,\ 11$.*

*(iv). If $B > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 19,\ 43,\ 67,\ 163$.*

*Proof of Theorem 5.1.2.* By Proposition 1.2.6, we have $E_{n,\theta}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Suppose $K$ is a real number field satisfying the assumptions of Theorem 5.1.2. By Proposition 5.3.2 (*iii*), we need only rule out torsion points of order $5, 7$ or 11 in $E_{n,\theta}(K)_{tors}$. We consider the following cases.

**5-torsion:** Suppose, if possible, $R = (x, y)$ be a point of order 5 in $E_{n,\theta}(K)_{tors}$. We consider the possibilities for the degree of the sub-extension $\mathbb{Q}(R)$ of $K$ over $\mathbb{Q}$. The Galois group of the normal closure of $\mathbb{Q}(R)$ can be identified with a subgroup of $GL_2(\mathbb{F}_5)$, the general linear group over finite field of order 5. By the fundamental theorem of Galois theory, $[\mathbb{Q}(R) : \mathbb{Q}]$ must divide $\#GL_2(\mathbb{F}_5) = 2^5 \cdot 3 \cdot 5$. By assumption, $[K : \mathbb{Q}]$ is coprime to 6. As $\mathbb{Q}(R) \subset K$, $[\mathbb{Q}(R) : \mathbb{Q}]$ must divide 5. Since $E_{n,\theta}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $[\mathbb{Q}(R) : \mathbb{Q}] \neq 1$. Therefore, $\mathbb{Q}(R)$ is a quintic extension over $\mathbb{Q}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ is a subgroup of $E_{n,\theta}(\mathbb{Q}(R))_{tors}$. But González-Jiménez showed that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot

appear as a torsion subgroup of a rational elliptic curve over a quintic field (Theorem 2 of [22]). Therefore, 5-torsion cannot occur over $K$.

**7-torsion:** Suppose $E_{n,\theta}(K)_{tors}$ contains a point of order 7, say $R = (x, y)$. By a similar argument as above, we find that $[\mathbb{Q}(R) : \mathbb{Q}] = 7$. It follows that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ appears as a subgroup of $E_{n,\theta}(\mathbb{Q}(R))_{tors}$. But González-Jiménez and Najman showed that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ cannot appear as a torsion subgroup of a rational elliptic curve over a number field of degree 7 (Proposition 7.1 of [23]). Therefore, 7-torsion cannot occur over $K$.

**11-torsion:** Suppose $E_{n,\theta}(K)_{tors}$ contains a point of order 11, say $R = (x, y)$. By arguing as before, we find that $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $5^2 \cdot 11$. Theorem 5.8 of [23] provides a complete list possibilities for the degree of a number field generated by an 11-torsion of a rational elliptic curve, and that list does not include $5^2 \cdot 11$. So we must have either $[\mathbb{Q}(R) : \mathbb{Q}] = 5$ or $[\mathbb{Q}(R) : \mathbb{Q}] = 55$. If $[\mathbb{Q}(R) : \mathbb{Q}] = 5$ then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$ would appear as a subgroup of $E_{n,\theta}(\mathbb{Q}(R))_{tors}$. But González-Jiménez has shown that a quintic field cannot have $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$ as a subgroup of the torsion of a rational elliptic curve (Theorem 2 in [22]). Finally, we can't have $[\mathbb{Q}(R) : \mathbb{Q}] = 55$ since $[K : \mathbb{Q}]$ is not divisible by 55.

Thus we can conclude that $E_{n,\theta}(K)_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The theorem now follows from Lemma 5.2.3. □

## 5.4 Real Cubic Fields

After $\theta = \frac{\pi}{2}$, the next natural values to be considered are $\theta = \frac{\pi}{3}$ or $\frac{2\pi}{3}$, since they are rational multiples of $\pi$ with rational cosine. Fujiwara [19] proved that a prime $p$ is not $\frac{\pi}{3}$-congruent if $p \equiv 5,\ 7,\ 19 \pmod{24}$. Kan [31] showed that a prime $p$ is not $\frac{2\pi}{3}$-congruent if $p \equiv 7,\ 11,\ 13 \pmod{24}$ and that the primes $p \equiv 23 \pmod{24}$ are $\frac{\pi}{3}$- and $\frac{2\pi}{3}$-congruent over $\mathbb{Q}$. In this subsection, we consider angles $\theta$ where $\cos\theta = \frac{s}{r}$, and $r$, $s$ belong to certain congruence classes modulo 5 and obtain the following criterion over real cubic fields.

In order to prove Theorem 5.1.3 above, we need to consider the growth of torsion upon base change from $\mathbb{Q}$ to a cubic field $K$. Let $d$ be a positive integer. Let $\Phi(d)$ be the set of possible torsion structures $E(K)_{tors}$, where $K$ runs through all number fields $K$ of degree $d$ and $E$ runs through all elliptic curves over $K$. Mazur established that

$$\Phi(1) = \{\mathcal{C}_n \mid n = 1, \ldots, 10, 12\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 1, \ldots, 4\},$$

where $\mathcal{C}_n$ denotes the cyclic group of order $n$. Let $\Phi_{\mathbb{Q}}(d)$ be the set of possible torsion structures over a number field of degree $d$ of an elliptic curve defined over $\mathbb{Q}$. Clearly,

$\Phi_{\mathbb{Q}}(1) = \Phi(1)$. For each $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ denote the set

$$\{E(K)_{tors} : E/\mathbb{Q} \text{ is an elliptic curve }, \ \ E(\mathbb{Q})_{tors} \simeq G, \ \ [K : \mathbb{Q}] = d\}.$$

In order to identify $\theta$-congruent numbers over a number field of degree $d$, we need to examine $\Phi_{\mathbb{Q}}(d, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$. For cubic extension of $\mathbb{Q}$, we have the following result.

**Proposition 5.4.1.** *[24] For $G = \mathcal{C}_2 \times \mathcal{C}_2$, we have*

$$\Phi_{\mathbb{Q}}(3, G) = \{\mathcal{C}_2 \times \mathcal{C}_2, \ \mathcal{C}_2 \times \mathcal{C}_6\}.$$

*Proof of Theorem 5.1.3.* The Weierstrass form of a $\theta$-congruent number elliptic curve $E_{n,\theta}$ is given by

$$y^2 = x^3 - 3^3(3r^2 + s^2)n^2x + 2 \cdot 3^3n^3s(9r^2 - s^2), \text{ where } \cos\theta = \frac{s}{r}.$$

For a cubic number field $K$, we have

$$E_{n,\theta}(K)_{tors} \simeq \mathcal{C}_2 \times \mathcal{C}_2 \text{ or } E_{n,\theta}(K)_{tors} \simeq \mathcal{C}_2 \times \mathcal{C}_6$$

by Proposition 5.4.1. Our objective is to rule out $E_{n,\theta}(K)_{tors} \simeq \mathcal{C}_2 \times \mathcal{C}_6$ under the assumptions on $r$, $s$ in the theorem. Suppose, if possible, $E_{n,\theta}(K)_{tors} \simeq \mathcal{C}_2 \times \mathcal{C}_6$. Then there is an element in $E_{n,\theta}(K)$ of order 3, say $P = (X, Y)$. Then $X$ is a root of the 3-rd division polynomial given by

$$\phi(X) = 3X^4 - 162n^2(3r^2 + s^2)X^2 + 648n^3s(9r^2 - s^2)X - 729n^4(3r^2 + s^2)^2. \tag{5.3}$$

It is not difficult to observe that $\phi(3nX) = 3^5 \cdot n^4 f(X)$, where

$$f(x) = x^4 - 6(3r^2 + s^2)x^2 + 8s(9r^2 - s^2)x - 3(3r^2 + s^2)^2 \in \mathbb{Z}[x].$$

Hence $\phi(X)$ has a solution in $K$ if and only if equation $f(x)$ has a solution in $K$. Reducing the polynomial $f(x)$ modulo 5, we find that

$$f(x) \equiv \begin{cases} x^4 + 2x^2 + 3 \pmod 5 & \text{if } (r, s) \equiv (\pm 1, 0) \text{ or } (\pm 2, \pm 1) \pmod 5 \\ x^4 + 3x^2 + 3 \pmod 5 & \text{if } (r, s) \equiv (\pm 2, 0) \text{ or } (\pm 1, \pm 2) \pmod 5. \end{cases}$$

One can check that $x^4 + 2x^2 + 3$ and $x^4 + 3x^2 + 3$ are irreducible polynomials over $\mathbb{Z}/5\mathbb{Z}$. Therefore $f(x)$ is irreducible over $\mathbb{Q}$, hence equation (5.3) does not possess a solution in $K$ as 4 does not divide $[K : \mathbb{Q}]$. The theorem now follows from Corollary 5.2.3. □

**Example.** To illustrate the theorem above, let us take $\cos\theta = \frac{5}{6}$ where $r = 6$ and $s = 5 \equiv 0 \pmod 5$. The corresponding $\theta$-congruent number curve with $n = 7$ is

$$E_{7,\theta} : y^2 = x^3 + 70x^2 - 539x.$$

We can verify by using MAGMA that the rank of $E_{7,\theta}(\mathbb{Q})$ is 0, therefore 7 is not a $\theta$-congruent number over $\mathbb{Q}$. By putting $y = 1$, we find that the polynomial $x^3 + 70x^2 - 539x - 1$ has 3 real roots. If we denote the largest real root by $\alpha \approx 7.0017$, then $K = \mathbb{Q}(\alpha)$ is a real cubic field. The point $(\alpha, 1) \in E_{7,\theta}(K)$ is clearly not a 2-torsion point, and hence 7 is $\theta$-congruent over $K$. By Proposition 5.4.1,

$$E_{7,\theta}(K)_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ or } E_{7,\theta}(K)_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Theorem 5.4.1 rules out the latter possibility which we directly verify now. Clearly,

$$E_{7,\theta}(K)[2] = E_{7,\theta}(\mathbb{Q}) = \{(0,0),\ (7,0),\ (-77,0),\ \mathcal{O}\}.$$

If the point $(\alpha, 1)$ were a 6-torsion point, then one of $P = (\alpha, 1)$, $Q = (\alpha, 1) + (0, 0)$, $R = (\alpha, 1) + (-77, 0)$ or $S = (\alpha, 1) + (7, 0)$ must be a 3-torsion point. By considering the $x$-coordinates of the points, it can be easily checked that

$$\begin{aligned} &x(2P) > 208 > x(-P) = \alpha, \\ &x(2Q) = x(2P) > 208 > 0 > x(-Q), \\ &x(2R) = x(2P) > 208 > 0 > x(-R), \\ &x(2S) = x(2P) < 303 < 24000 < x(-S). \end{aligned}$$

Therefore, $2P \neq -P$, $2Q \neq -Q$, $2R \neq -R$ or $2S \neq -S$, and none of $P$, $Q$, $R$ or $S$ is a 3-torsion point. Therefore, $P = (\alpha, 1)$ cannot be a 6-torsion on $E_{7,\theta}(K)$ and it must have have infinite order.

**Remark 5.4.2.** *Suppose $K$ is a real sextic field. It has been conjectured in [12] that $\Phi_{\mathbb{Q}}(6,\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$ is a subset of*

$$\{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2t\mathbb{Z} \mid t = 1,\ 2,\ 3,\ 4,\ 6\} \cup \{\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}\}.$$

*If we put restrictions on $(r, s)$ such that $2r(r - s)$ is not a square element in $K$, we can rule out 4-torsion point on $E_{n,\theta}(K)_{tors}$ by Lemma 5.2.5. if we further assume that $s$ is divisible by 5 or $(r, s) \equiv (\pm 2, \pm 1)$ or $(\pm 1, \pm 2) \pmod 5$, we can rule out 3-torsion point on $E_{n,\theta}(K)_{tors}$ as in Theorem 5.1.3 noting that 4 does not divide $[K : \mathbb{Q}]$ in this case*

*too. Therefore, we have* $E_{n,\theta}(K)_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*, and by Lemma 5.2.3 a square free integer* $n \neq 1, 2, 3, 6$ *will be* $\theta$*-congruent number over real sextic field* $K$ *under the above restrictions over* $r, s$ *if and only if* $E_{n,\theta}(K)$ *has positive rank assuming the conjecture.*

**Corollary 5.4.3.** *If a real number field satisfies the assumptions of Theorem 5.1.1, 5.1.3 or 5.1.2 then a number* $n$ *is* $(K, \theta)$*-congruent if and only if* $n$ *is properly* $(K, \theta)$*-congruent.*

*Proof.* For such fields $K$ a number $n$ is $(K, \theta)$-congruent if and only if $rank(E_{n,\theta}(K))$ is positive. Once again, $n$ is properly $(K, \theta)$-congruent if and only if $E_{n,\theta}$ has a point of infinite order. These two correspondences conclude this corollary. □

# CHAPTER 6

# THE CLASS NUMBER OF $\mathbb{Q}(\sqrt{-pq})$

## 6.1 Introduction

In this chapter, we establish a divisibility result for the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ when $n$ is a square-free congruent number with two prime factors $p \equiv 5$ modulo 8 and $q \equiv 7$ modulo 8. Let us denote the ideal class number of imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ by $h(-n)$. Using modular forms of half-integral weight, Tunnell [54] proved a divisibility result for the 2-part of $h(-p)$ for a prime $p \equiv 1$ modulo 8 when $p$ is a congruent number. A prototypical example of half-integral weight modular forms is the theta function. A classical result of Gauss states that the coefficients of Fourier series representation of the theta function is related to the Hurwitz class number, and hence to the class number $h(-n)$. Assuming the BSD Conjecture, Kazalicki [32] related the 2-part of $h(-p)$ for a prime $p \equiv 1$ modulo 8 to $p$ being a congruent number by considering theta function.

Here we prove a necessary condition for $pq$ to be congruent in terms of the 2-part of the $h(-pq)$ where $p$ and $q$ are primes as specified above. Rather than considering modular forms, we rely on the method of complete 2-descent. We do not need the full force of the BSD Conjecture, but we assume a weaker conjecture known as the Parity Conjecture. We know that a natural number $n$ is a congruent number if and only if the congruent number elliptic curve $E_n$ given by (1.2) has positive Mordell–Weil rank $r(n)$. Let $w(n)$ denote the order of vanishing at $s = 1$ for the Hasse-Weil $L$-function $L(E_n, s)$ of the elliptic curve $E_n$. The Parity Conjecture predicts that $r(n)$ and $w(n)$ must have the same parity, whereas the first part of the Birch and Swinnerton-Dyer Conjecture predicts that the rank $r(n)$ of $E_n(\mathbb{Q})$ is equal to $w(n)$ (see [25]). The second part of the BSD Conjecture predicts that the Shafarevich-Tate group of $E_n/\mathbb{Q}$ is finite, and hence $r(n)$ must also be the rank $s_p(n)$

of the $p^\infty$-Selmer group of $E_n$. T. Dokchitser and V. Dokchitser [14] proved that $w(n)$ and $s_p(n)$ have the same parity for a large class of primes $p$.

Our result concerning the class number can be stated as follows.

**Theorem 6.1.1.** *Let $n = pq$, where $p$ and $q$ are distinct primes satisfying $(p, q) \equiv (5, 7) \pmod 8$. Suppose the Parity Conjecture holds for $E_n/\mathbb{Q}$. If $n$ is a congruent number, then $h(-n)$ is divisible by 8.*

We prove our result by employing a criterion of Brown [5] for divisibility of $h(-pq)$ by 8 in terms of the quartic reside symbol $\left(\frac{-q}{p}\right)_4$. In order to investigate the quartic residue symbol, we show that certain Diophantine equations have non-trivial integral solutions. We obtain these Diophantine equations by considering the complete 2-descent method. In section 6.2, we briefly discuss how 2-descent combing with Proposition 2.4.3 for certain Diophantine equations that eventually help in restricting our search for the desired Diophantine equations with non-trivial integral solutions. In section 6.3, we use the Parity Conjecture to show that there exist non-trivial integral solutions to certain Diophantine equations leading us to the desired value of the quartic residue symbol.

## 6.2 The Size of the Image $b(E_n(\mathbb{Q})/2E_n(\mathbb{Q}))$

In this section we first recall the key aspects of the method of complete 2-descent that we need. The method of 2-descent is an algorithm used for computing the rank of an elliptic curve (for details, see section 2.4 of chapter 2 ).

**Remark 6.2.1.** *Suppose $n = pq$ as given in Theorem 6.1.1, then a system of representatives of classes in $\mathbb{Q}(S, 2)$ is given by (see Remark 2.4.2)*

$$R = \{(-1)^\alpha 2^\beta p^{\epsilon_1} q^{\epsilon_2} \mid \quad \alpha,\ \beta,\ \epsilon_1,\ \epsilon_2 = 0 \text{ or } 1\}. \tag{6.1}$$

The image of $E_n(\mathbb{Q})_{tors}$ under the map $b$ in (2.5) is represented by

$$\mathcal{A} = \{(1, 1),\ (-1, -n),\ (n, 2),\ (-n, -2n)\} \subset R \times R. \tag{6.2}$$

Clearly, $\mathcal{A}$ can also be considered as a subgroup $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$. For $n$ to be a congruent number, we require that $r(n) > 0$. In other words, there needs to be a pair $(b_1, b_2) \in (R \times R) \setminus \mathcal{A}$ such that the system of equations given by (2.6) and (2.7) possesses a solution in $(\mathbb{Q}^\times)^3$.

Proposition 2.4.3 helps us to rule out certain pairs of elements $(b_1, b_2) \in (R \times R)$ which can not have preimage in the Mordell-Weil group under the map $b$ defined in (2.5). For example, rather than considering rational solutions for the system of equations (2.6) and

(2.7), it is convenient to consider integral solutions of an equivalent system of equations as stated in Lemma 3.2.1 and corollary 3.2.2. Here, we examine the image of $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ under the embedding $b$ defined in (2.5) in Theorem 2.4.1 of chapter 2. From now onward, we assume that $n = pq$, as defined in Theorem 6.1.1. The following lemma restricts the possibilities for the image of a non-torsion point $E_n(\mathbb{Q})$ under the map $b$. Recall that $\mathcal{A} = b(E_n(\mathbb{Q})_{tors})$.

**Lemma 6.2.2.** *Suppose $P = (x, y)$ is a non-torsion point of $E_n(\mathbb{Q})$. Modulo $\mathcal{A}$, the image $b(P)$ is represented by a pair $(b_1, b_2) \in R' \times R'$ where $R' = \{1, p, q, pq\}$.*

*Proof.* The idea of the proof can be taken from proof of Lemma 3.3.1 of chapter 3. □

By a slight abuse of notation, we just write equality for the representatives whenever they represent the same equivalence classes in

$$(\mathbb{Q}(S,2) \times \mathbb{Q}(S,2))/\mathcal{A}.$$

The following lemma further restricts the possible images of non-torsion points of $E_n(\mathbb{Q})$ under the map $b$ in (2.5).

**Lemma 6.2.3.** *Let $p$ and $q$ be distinct primes satisfying $(p, q) \equiv (5, 7) \pmod 8$ such that $pq$ is a congruent number. If the system of equations (3.6) and (3.7) has a solution $(a_1, a_2, a_3, d) \in (\mathbb{Z}^\times)^4$ for some $(b_1, b_2) \in R' \times R'$, then*

$$(b_1, b_2) \in \{(1, p), (q, 1), (q, p), (1, 1)\}.$$

In order to prove the lemma, we first state the following result due to Lagrange [36].

**Proposition 6.2.4.** *Let $p$ and $q$ be distinct primes satisfying $(p, q) \equiv (5, 7) \pmod 8$. If $\left(\frac{q}{p}\right) = -1$, then $pq$ is not a congruent number.*

**Remark 6.2.5.** *Under our assumption in Theorem 6.1.1, $n = pq$ is a congruent number. Therefore, $\left(\frac{q}{p}\right) = 1$ in view of Proposition 6.2.4.*

*Proof of Lemma 6.2.3.* We need to show that the system of equations (3.6) and (3.7) does not have a non-trivial integral solution for

$$(b_1, b_2) \in (R' \times R') \setminus \{(1, p), (q, 1), (q, p), (1, 1)\}.$$

Consider the pair $(b_1, b_2) = (p, 1) \in R' \times R'$. If possible, let $(a_1, a_2, a_3, d) \in (\mathbb{Z}^\times)^4$ be a solution for the system of Diophantine equations

$$pa_1^2 - a_2^2 = pqd^2, \qquad pa_1^2 - pa_3^2 = -pqd^2.$$

From the first equation, $a_2 \equiv 0 \pmod{p}$. As $a_1$, $a_2$, $a_3$ and $d$ are pairwise coprime by Lemma 3.2.1, $a_1$ and $a_3$ are coprime to $p$. Replacing $a_2 = pa_2^{'}$ followed by taking sum of the resulting equations leads to

$$2a_1^2 - pa_2'^2 - a_3^2 = 0,$$

which gives us $\left(\frac{2}{p}\right) = 1$. But this is not possible, since $p \equiv 5 \pmod{8}$. Similar argument rules out non-trivial solutions for pairs $(p, p)$, $(pq, 1)$, $(pq, pq)$ in $R' \times R'$.

Now, consider the pair $(1, pq) \in R' \times R'$. If possible, let $(a_1, a_2, a_3, d) \in (\mathbb{Z}^\times)^4$ be a solution for the system of Diophantine equations

$$a_1^2 - pqa_2^2 = pqd^2,$$
$$a_1^2 - pqa_3^2 = -pqd^2.$$

Clearly, $a_1$ is divisible by $p$ and $q$. By Lemma 3.2.1, $a_2$ is coprime to $pq$. Substituting $a_1 = pqa_1'$ with $a_1' \in \mathbb{Z}^\times$ in the first equation yields

$$pqa_1'^2 - a_2^2 = d^2.$$

It follows that $\left(\frac{-1}{q}\right) = 1$, which is absurd as $q \equiv 7 \pmod{8}$. Similar argument rules out the pairs $(p, pq)$, $(pq, pq)$, and $(pq, q)$.

Next, consider the pair $(pq, p)$. If possible, let $(a_1, a_2, a_3, d) \in (\mathbb{Z}^\times)^4$ be a solution for the system of Diophantine equations

$$pqa_1^2 - pa_2^2 = pqd^2,$$
$$pqa_1^2 - p^2qa_3^2 = -pqd^2.$$

Clearly, $a_2$ is divisible by $q$. Substituting $a_2 = qa_2'$ and then adding the resulting equations leads to

$$2a_1^2 - qa_2'^2 - pa_3^2 = 0. \tag{6.3}$$

Clearly, $p \mid a_1 \Leftrightarrow p \mid a_2' \Leftrightarrow p \mid a_2$. Since $(a_1, a_2) = 1$, we must have $a_1a_2'$ coprime to $p$. It follows from (6.3) that $\left(\frac{2q}{p}\right) = 1$. Since $p \equiv 5 \pmod{8}$, we have $\left(\frac{q}{p}\right) = -1$. By Proposition 6.2.4, $pq$ must be a non-congruent number, which contradicts our assumption. Similarly, we can rule out the remaining pairs $(p, q)$, $(q, q)$, and $(q, pq)$ by using the fact that the Legendre symbol $\left(\frac{q}{p}\right)$ must be 1 for a congruent number $pq$. □

**Corollary 6.2.6.** *Let $p$ and $q$ be distinct primes satisfying $(p, q) \equiv (5, 7) \pmod{8}$. If $n = pq$ is a congruent number, then the system of equations (3.6) and (3.7) must have a*

*solution* $(a_1, a_2, a_3, d) \in (\mathbb{Z}^\times)^4$ *for each pair*

$$(b_1, b_2) \in \{(1, p), (q, 1), (q, p), (1, 1)\} \subset R' \times R'$$

*if we assume the Parity Conjecture.*

*Proof.* It is well-known that $w(n)$, the order of vanishing of $L(E_n, s)$ at $s = 1$ is even when $n \equiv 1, 2, 3 \pmod 8$ (see [34], page 84). By the Parity Conjecture, the rank $r(n)$ of $E_n(\mathbb{Q})$ must be even too (see [25]). Consequently, $r(n)$ must be at least 2 if $n$ is congruent. By (2.8), the image of $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$ under the map $b$ in (2.5) has order $2^4$. Since the image $\mathcal{A}$ of the torsion points under $b$ has cardinality 4, the system of equations (3.6) and (3.7) must have non-trivial integral solutions for each of the coset representatives

$$(b_1, b_2) \in \{(1, p), (q, 1), (q, p), (1, 1)\} \subset R' \times R'. \qquad \square$$

In the following remark, we make certain observations concerning the non-integral solutions that correspond to one particular pair of representatives out of the four in the previous corollary.

**Remark 6.2.7.** *By Corollary 6.2.6,* $(q, 1)$ *is represents a coset in the image of the map* $b$*. Thus, there exist pairwise coprime integers* $a_1$*,* $a_2$*,* $a_3$ *and* $d$ *such that*

$$qa_1^2 - a_2^2 = pqd^2,$$
$$qa_1^2 - qa_3^2 = -pqd^2.$$

*From the first equation it is clear that* $a_2$ *is divisible by* $q$*. Hence* $a_1$*,* $a_3$ *and* $d$ *are coprime to* $q$*. Substituting* $a_2 = qa_2'$ *in above equations, we obtain*

$$a_1^2 - qa_2'^2 = pd^2, \tag{6.4}$$

$$a_1^2 - a_3^2 = -pd^2. \tag{6.5}$$

*Observe that* $p$ *does not divide* $a_2'$*,* $a_1$ *or* $a_3$*, otherwise these integers would no longer be pairwise coprime.*

## 6.3 Divisibility of the Class Number

In order to relate the class number of $\mathbb{Q}(\sqrt{-pq})$ to the existence of non-trivial solutions of the system of Diophantine equations (3.6) and (3.7), we need the following result due to Brown [5].

**Proposition 6.3.1.** *If $p \equiv -q \equiv 1 \pmod 4$ are primes with $\left(\frac{q}{p}\right) = 1$ then $h(-pq)$ is divisible by 8 if and only if $\left(\frac{-q}{p}\right)_4 = 1$, i.e., $-q$ is a quartic residue modulo $p$.*

Our next step is to reduce the computation of the quartic residue symbol $\left(\frac{-q}{p}\right)_4$ to a computation of certain Jacobi symbol.

**Lemma 6.3.2.** *Under the assumptions in Theorem 6.1.1,*

$$\left(\frac{-q}{p}\right)_4 = \left(\frac{a_2'}{p}\right),$$

*where $a_2'$ is the odd number coprime to $p$ as given in Remark 6.2.7.*

*Proof.* There exist pairwise coprime positive integers $a_1$, $a_2$, $a_3$ and $d$ satisfying the simultaneous equations (6.4) and (6.5) corresponding to the pair $(q, 1)$, as mentioned in Remark 6.2.7. Since $(p, q) \equiv (5, 7) \pmod 8$, we must have $a_2' \equiv a_3 \equiv d \equiv a_1 + 1 \equiv 1 \pmod 2$. By (6.5), we have

$$(a_3 + a_1)(a_3 - a_1) = pd^2.$$

The numbers $(a_3 + a_1)$ and $(a_3 - a_1)$ are mutually co prime as $a_3$ and $a_1$ are coprime with different parity. Therefore, we can write

$$\begin{aligned} a_3 + a_1 &= \pm pe^2, \qquad a_3 - a_1 = \pm f^2; \qquad \text{or} \\ a_3 + a_1 &= \pm e^2, \qquad a_3 - a_1 = \pm pf^2, \end{aligned}$$

where $d = ef$ and $(e, f) = 1$. The first possibility leads to

$$a_3 = \pm\frac{pe^2 + f^2}{2}, \qquad a_1 = \pm\frac{pe^2 - f^2}{2} \tag{6.6}$$

Note that $f$ is not divisible by $p$, since $(a_1, d) = 1$. By equation (6.4),

$$\begin{aligned} 4qa_2'^2 &= 4(a_1^2 - pd^2) \\ &\equiv (pe^2 - f^2)^2 \pmod p \\ &\equiv f^4 \pmod p \\ \implies \left(\frac{4qa_2'^2}{p}\right)_4 &= 1. \end{aligned} \tag{6.7}$$

It is easily observed that $\left(\frac{-1}{p}\right)_4 = \left(\frac{2}{p}\right)$ for a prime $p \equiv 1 \pmod 4$. Therefore,

$$\left(\frac{4}{p}\right)_4 = \left(\frac{2^2}{p}\right)_4 = \left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)_4.$$

It follows from (6.7) that

$$\left(\frac{-q}{p}\right)_4 = \left(\frac{a_2'^2}{p}\right)_4 = \left(\frac{a_2'}{p}\right).$$

The argument for the second possibility for the values of $a_3$ and $a_1$ works out exactly the same way. □

Our final step is to compute the Legendre symbol $\left(\frac{a_2'}{p}\right)$ appearing in the preceding lemma.

*Proof of Theorem 6.1.1.* Recall that $a_2'$ is odd and coprime to $p$. Since $p \equiv 5 \pmod 8$, it follows from Lemma 6.3.2 and Jacobi's reciprocity law that

$$\left(\frac{-q}{p}\right)_4 = 1 \Leftrightarrow \left(\frac{a_2'}{p}\right) = \left(\frac{|a_2'|}{p}\right) = \left(\frac{p}{|a_2'|}\right)_j = 1. \tag{6.8}$$

Here, $\left(\frac{k}{l}\right)_j$ denotes the Jacobi symbol for any integer $k$ coprime to the odd natural number $l$. Taking the sum and difference of equations (6.4) and (6.5), we have

$$a_3^2 - 2a_1^2 = -qa_2'^2, \tag{6.9}$$

$$a_3^2 - qa_2'^2 = 2pd^2. \tag{6.10}$$

Since $a_1$, $a_2 = qa_2'$, $a_3$ and $d$ are pairwise coprime, it follows from (6.9) and (6.10) that

$$\left(\frac{2}{|a_2'|}\right)_j = 1, \quad \left(\frac{2p}{|a_2'|}\right)_j = 1.$$

Therefore,

$$\left(\frac{a_2'}{p}\right) = \left(\frac{p}{|a_2'|}\right)_j = \left(\frac{2}{|a_2'|}\right)_j \left(\frac{2p}{|a_2'|}\right)_j = 1.$$

By Proposition 6.3.1 and Lemma 6.3.2, we can now conclude that the class number of $\mathbb{Q}(\sqrt{-pq})$ is divisible by 8. □

We provide a few examples to illustrate our main result.

| $p \equiv 5 \pmod 8$ | $q \equiv 7 \pmod 8$ | Rank $r(pq)$ | Class number $h(-pq)$ |
|---|---|---|---|
| 5 | 79 | 2 | 8 |
| 13 | 103 | 2 | 8 |
| 29 | 631 | 2 | 48 |
| 37 | 751 | 2 | 16 |

The converse of Theorem 6.1.1 is not true. For example, $n = 13 \cdot 23$ is a non-congruent number but $h(-13 \cdot 23) = 8$.

# CHAPTER 7

# THE CONTINUED FRACTION OF $\sqrt{pq}$

## 7.1 Introduction

In this chapter, we examine the regular continued fraction (RCF) of certain quadratic irrationals $\sqrt{n}$ where $n$ is a square-free rational number. There have been attempts to relate the continued fraction of quadratic irrational to the congruent number problem (e.g. see [50] and [35]). But there are several interesting questions concerning the RCF of quadratic irrationals that are still open. A conjecture of Chowla and Chowla (see [10]) predicts that for any natural number $k$ there exist infinitely many primes $p$ such that the RCF of $\sqrt{p}$ has period length $k$. While their conjecture is still open, it has been proved in [18] that there exists infinitely many square-free natural numbers $d$ such that the RCF of $\sqrt{d}$ has period $k$ for any natural number $k$. The density of square-free integers $d$ with no prime factor congruent to 3 modulo 4 such that $\sqrt{d}$ has period of odd length has been studied in [15] and [16]. Golubeva ( [21]) proved that the period length of the RCF $\sqrt{p}$ is divisible by 4 when $p$ is a prime congruent to 7 modulo 8 and is of the form $4k+2$ when $p$ is a prime congruent to 3 modulo 8. Golubeva further showed that the central term of the period of the RCF $\sqrt{p}$ is odd for a prime congruent to 3 modulo 4. In this chapter, we examine the period of the RCF of $\sqrt{pq}$ where $p < q$ are two primes congruent to 3 modulo 4.

The RCF of $\sqrt{pq}$ can be written as

$$\sqrt{pq} = n + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{l-1} + \cfrac{1}{2n + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}}}}}, \quad \text{where } n = \lfloor \sqrt{pq} \rfloor.$$

We denote it as $\sqrt{pq} = \langle n, \overline{a_1, a_2, \ldots, a_{l-1}, 2n} \rangle$. It is well-known that the first $l-1$ terms

$a_1, a_2, \ldots, a_{l-1}$ of the period $(a_1, a_2, \ldots, a_{l-1}, 2n)$ form a palindrome (e.g. [13]). It can be easily seen that the length $l$ of the period of $\sqrt{pq}$ is even when at least one of $p$ and $q$ is congruent to 3 modulo 4 (see Proposition 7.2.1). In this chapter, we prove a closer relation between the congruence properties of the length of the period of the RCF of $\sqrt{pq}$ and the interplay between the primes $p$ and $q$ in terms of quadratic congruence.
We begin by observing the period of the RCF of $\sqrt{pq}$ when $q$ is a quadratic residue modulo $p$ in the table below.

Table 7.1: $(\frac{q}{p}) = 1$

| $p$ | $q$ | $\sqrt{pq} = \langle n, \overline{a_1, a_2, \ldots, a_{l-1}, 2n} \rangle$ | $l$ | $a_{\frac{l}{2}}$ |
|---|---|---|---|---|
| 3 | 7 | $\sqrt{21} = \langle 4, \overline{1, 1, 2, 1, 1, 8} \rangle$ | 6 | 2 |
| 3 | 19 | $\sqrt{57} = \langle 7, \overline{1, 1, 4, 1, 1, 14} \rangle$ | 6 | 4 |
| 7 | 11 | $\sqrt{77} = \langle 8, \overline{1, 3, 2, 3, 1, 16} \rangle$ | 6 | 2 |
| 3 | 43 | $\sqrt{129} = \langle 11, \overline{2, 1, 3, 1, 6, 1, 3, 1, 2, 22} \rangle$ | 10 | 6 |
| 7 | 23 | $\sqrt{161} = \langle 12, \overline{1, 2, 4, 1, 2, 1, 4, 2, 1, 24} \rangle$ | 10 | 2 |

We find that the length of the period is of the form $4k + 2$, and the central term $a_{\frac{l}{2}}$ of the palindromic part of the period is an even integer. Then we consider the period of the RCF of $\sqrt{pq}$ when $q$ is a quadratic non-residue modulo $p$ in the following table.

Table 7.2: $(\frac{q}{p}) = -1$

| $p$ | $q$ | $\sqrt{pq} = \langle n, \overline{a_1, a_2, \ldots, a_{l-1}, 2n} \rangle$ | $l$ | $a_{\frac{l}{2}}$ |
|---|---|---|---|---|
| 3 | 11 | $\sqrt{33} = \langle 5, \overline{1, 2, 1, 10} \rangle$ | 4 | 2 |
| 3 | 47 | $\sqrt{141} = \langle 11, \overline{1, 6, 1, 22} \rangle$ | 4 | 6 |
| 3 | 59 | $\sqrt{177} = \langle 13, \overline{3, 3, 2, 8, 2, 3, 3, 26} \rangle$ | 8 | 8 |
| 11 | 19 | $\sqrt{209} = \langle 14, \overline{2, 5, 3, 2, 3, 5, 2, 28} \rangle$ | 8 | 2 |
| 11 | 43 | $\sqrt{473} = \langle 21, \overline{1, 2, 1, 42} \rangle$ | 4 | 2 |

We find that the length $l$ of the RCF of $\sqrt{pq}$ is divisible by 4, and the central term $a_{\frac{l}{2}}$ of the palindromic part of the period is even as before. In this chapter, we prove that the period of the RCF of $\sqrt{pq}$ always exhibits this behavior. The main results of this chapter can be stated as follows.

**Theorem 7.1.1.** *Let $p < q$ be two primes congruent to 3 modulo 4 and $l$ be the length of the period of the regular continued fraction of $\sqrt{pq}$. Then $l$ is of the form $4k + 2$ if $q$ is a quadratic residue modulo $p$, and $l$ is divisible by 4 if $q$ is a quadratic non-residue modulo $p$.*

**Theorem 7.1.2.** *The central term in the palindromic part of the period of* $\sqrt{pq}$ *is even in either of the following cases:*
*(i) if* $q$ *is a quadratic non-residue modulo* $p$*, or*
*(ii) if* $q$ *is a quadratic residue modulo* $p$ *and* $p$ *is congruent to* 3 *modulo* 8*.*

We prove the theorems above by examining the convergents of the RCF of $\sqrt{pq}$ closely. In particular, we establish some implications of the congruence property of the period length of the RCF of $\sqrt{pq}$ for certain convergents. Then we relate those specific convergents to the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{pq})$ and show that they are solutions of certain Diophantine equations. As a consequence, we can prove the behavior of the length and the central term as stated in Theorems 7.1.1 and 7.1.2.

## 7.2 The Convergents of $\sqrt{pq}$

In this section we establish certain relations involving convergents of the continued fraction of $\sqrt{pq}$ where $p$ and $q$ are primes congruent to 3 modulo 4. As before, let

$$\sqrt{pq} = \langle n, \overline{a_1, a_2, \ldots, a_{l-1}, 2n}\rangle, \qquad n = \lfloor \sqrt{pq} \rfloor, \qquad a_i = a_{l-i}.$$

The $i$-th convergent of the continued fraction of $\sqrt{pq}$ is given by

$$\frac{k_i}{h_i} = n + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_i}}}}. \tag{7.1}$$

We can write the first few convergents as

$$\begin{aligned} &h_0 = 1, \quad k_0 = n; && h_1 = a_1, \quad k_1 = na_1 + 1; \\ &h_2 = 1 + a_1a_2, && k_2 = na_1a_2 + n + a_2. \end{aligned} \tag{7.2}$$

By convention, we take

$$h_{-1} = 0, \qquad k_{-1} = 1.$$

It can be readily verified (see [13]) that

$$h_{i+1} = a_{i+1}h_i + h_{i-1}, \qquad k_{i+1} = a_{i+1}k_i + k_{i-1} \quad \text{for} \quad i \geq 2, \tag{7.3}$$

$$k_{l-1} = nh_{l-1} + h_{l-2}, \tag{7.4}$$

$$k_ih_{i-1} - k_{i-1}h_i = (-1)^{i-1} \qquad \text{for } i \geq 0,$$

$$(nh_{l-1} + h_{l-2})^2 - pqh_{l-1}^2 = (-1)^{l-2}. \tag{7.5}$$

The next proposition is immediate from the last equality.

**Proposition 7.2.1.** *The period $l$ of the RCF of $\sqrt{pq}$ must be even.*

*Proof.* If $l$ were odd, $-1$ would be a quadratic residue modulo $p$ by (7.5). But it is not possible since $p$ is a prime congruent to 3 modulo 4. □

We need the following proposition for our subsequent results. We use the following notation for brevity:

$$c_{\frac{l}{2}-1} = h_{\frac{l}{2}} + h_{\frac{l}{2}-2}.$$

**Proposition 7.2.2.** *Let $l$ denote the length of the period of $\sqrt{pq}$. Then*

$$h_{l-1} = h_{\frac{l}{2}-1}\left(h_{\frac{l}{2}} + h_{\frac{l}{2}-2}\right) = h_{\frac{l}{2}-1}c_{\frac{l}{2}-1}. \tag{7.6}$$

The proof is similar to that of Proposition 2.1 in [7]. We just briefly mention the argument. By (7.3), we have

$$\begin{aligned} h_{l-1} &= a_{l-1}h_{l-2} + h_{l-3} = a_1h_{l-2} + h_{l-3} = h_1h_{l-2} + h_0h_{l-3}, \\ h_{l-1} &= a_1(a_{l-2}h_{l-3} + h_{l-4}) + h_{l-3} = a_1(a_2h_{l-3} + h_{l-4}) + h_{l-3} \\ &= (1 + a_1a_2)h_{l-3} + a_1h_{l-4} = h_2h_{l-3} + h_1h_{l-4}. \end{aligned}$$

Continuing in this way, we find that

$$h_{l-1} = h_ih_{l-1-i} + h_{i-1}h_{l-2-i} \text{ for } 0 \le i \le l-2.$$

In particular, putting $i = \frac{l-2}{2}$ we obtain (7.6).
The following lemma concerning $c_{\frac{l}{2}-1}$ and $h_{\frac{l}{2}-1}$ is needed later.

**Lemma 7.2.3.** *With the notation as above, $c_{\frac{l}{2}-1} = 2h_i$ or $h_{\frac{l}{2}-1} = 2h_i$ for any convergent $\frac{k_i}{h_i}$ of the RCF of $\sqrt{pq}$ only if $i = 0$.*

*Proof.* First consider $c_{\frac{l}{2}-1}$. Clearly,

$$\begin{aligned} \text{for } i \le \frac{l}{2} - 2, \qquad & 2h_i \le 2h_{\frac{l}{2}-2} < h_{\frac{l}{2}} + h_{\frac{l}{2}-2} = c_{\frac{l}{2}-1}, \\ \text{for } i \ge \frac{l}{2}, \qquad & 2h_i \ge 2h_{\frac{l}{2}} > h_{\frac{l}{2}} + h_{\frac{l}{2}-2} = c_{\frac{l}{2}-1}. \end{aligned}$$

The remaining possibility is $i = \frac{l}{2} - 1$. We consider the two cases $a_{\frac{l}{2}} = 1$ and $a_{\frac{l}{2}} \ge 2$ separately in the relation $h_{\frac{l}{2}} = a_{\frac{l}{2}}h_{\frac{l}{2}-1} + h_{\frac{l}{2}-2}$. When $a_{\frac{l}{2}} \ge 2$, we have

$$2h_{\frac{l}{2}-1} \le a_{\frac{l}{2}-1}h_{\frac{l}{2}-1} + 2h_{\frac{l}{2}-2} = c_{\frac{l}{2}-1}.$$

Here, the equality holds only when $h_{\frac{l}{2}-2} = 0$ and $a_{\frac{l}{2}} = 2$. In that case, we have

$$c_{\frac{l}{2}-1} = 2h_0.$$

For $a_{\frac{l}{2}} = 1$, the equality $c_{\frac{l}{2}-1} = 2h_{\frac{l}{2}-1}$ implies

$$(h_{\frac{l}{2}-1} + h_{\frac{l}{2}-2}) + h_{\frac{l}{2}-2} = 2h_{\frac{l}{2}-1}.$$

It follows that

$$2h_{\frac{l}{2}-2} = h_{\frac{l}{2}-1} = a_{\frac{l}{2}-1}h_{\frac{l}{2}-2} + h_{\frac{l}{2}-3},$$

which is possible only when $a_{\frac{l}{2}-1} = 2$ and $h_{\frac{l}{2}-3} = 0$. In that case, we obtain

$$c_{\frac{l}{2}-1} = 2h_{\frac{l}{2}-2} = 2h_0.$$

Now consider $h_{\frac{l}{2}-1}$. Clearly, for $i \leq \frac{l}{2} - 3$

$$2h_i \leq 2h_{\frac{l}{2}-3} \leq a_{\frac{l}{2}-1}h_{\frac{l}{2}-2} + h_{\frac{l}{2}-3} = h_{\frac{l}{2}-1},$$

and equality is not possible even when $h_{\frac{l}{2}-2} = 0$.
For $i = \frac{l}{2} - 2$, we have $2h_i = 2h_{\frac{l}{2}-2} > h_{\frac{l}{2}-2} + h_{\frac{l}{2}-3} = h_{\frac{l}{2}-1}$ if $a_{\frac{l}{2}-1} = 1$, and

$$2h_i = 2h_{\frac{l}{2}-2} \leq a_{\frac{l}{2}-1}h_{\frac{l}{2}-2} + h_{\frac{l}{2}-3} = h_{\frac{l}{2}-1}.$$

Therefore, the equality $2h_{\frac{l}{2}-2} = h_{\frac{l}{2}-1}$ holds only when $h_{\frac{l}{2}-3} = 0$ and $a_{\frac{l}{2}-1} = 2$. In that case, we have

$$h_{\frac{l}{2}-1} = 2h_{\frac{l}{2}-2} = 2h_0.$$

□

**Lemma 7.2.4.** *Let* $\frac{k_i}{h_i}$ *denote the* $i$*-th convergent of* $\langle n; \overline{a_1, a_2, ..., a_{l-1}, 2n}\rangle$. *Suppose* $l$ *is divisible by* 4. *Let* $t$ *be a divisor of* $h_{l-1}$.
(*i*) *If* $t \mid h_{\frac{l}{2}-1}$, *then* $h_{l-2} \equiv 1 \pmod{t}$.
(*ii*) *If* $t \mid c_{\frac{l}{2}-1}$, *then* $h_{l-2} \equiv -1 \pmod{t}$.

*Proof.* (*i*) Let $t$ be a divisor of $h_{l-1}$ that also divides $h_{\frac{l}{2}-1}$. By using (7.3), we have

$$\begin{aligned}
h_{\frac{l}{2}} &= a_{\frac{l}{2}}h_{\frac{l}{2}-1} + h_{\frac{l}{2}-2} \equiv h_{\frac{l}{2}-2} \pmod{t},\\
h_{\frac{l}{2}+1} &= a_{\frac{l}{2}+1}h_{\frac{l}{2}} + h_{\frac{l}{2}-1} = a_{\frac{l}{2}-1}h_{\frac{l}{2}} + h_{\frac{l}{2}-1}\\
&\equiv a_{\frac{l}{2}-1}h_{\frac{l}{2}-2} - h_{\frac{l}{2}-1} = -h_{\frac{l}{2}-3} \pmod{t}\\
h_{\frac{l}{2}+2} &= a_{\frac{l}{2}+2}h_{\frac{l}{2}+1} + h_{\frac{l}{2}} \equiv -a_{\frac{l}{2}-2}h_{\frac{l}{2}-3} + h_{\frac{l}{2}-2} = h_{\frac{l}{2}-4} \pmod{t}. \qquad (7.7)
\end{aligned}$$

Observing that the positive sign on the right hand side of the congruence precisely when the index on the left hand side is even, we can conclude that

$$h_{l-2} \equiv h_0 = 1 \pmod{t}.$$

(*ii*) Let $t$ be a divisor of $h_{l-1}$ that divides $c_{\frac{l}{2}-1}$, i.e., $h_{\frac{l}{2}} \equiv -h_{\frac{l}{2}-2} \pmod{t}$. Using (7.3), we find

$$\begin{aligned} h_{\frac{l}{2}+1} &= a_{\frac{l}{2}+1}h_{\frac{l}{2}} + h_{\frac{l}{2}-1} \\ &\equiv -a_{\frac{l}{2}-1}h_{\frac{l}{2}-2} + h_{\frac{l}{2}-1} \pmod{t} \qquad (\text{since } a_{\frac{l}{2}+1} = a_{\frac{l}{2}-1}) \\ &= h_{\frac{l}{2}-3}, \\ h_{\frac{l}{2}+2} &= a_{\frac{l}{2}+2}h_{\frac{l}{2}+1} + h_{\frac{l}{2}} \\ &\equiv a_{\frac{l}{2}-2}h_{\frac{l}{2}-3} - h_{\frac{l}{2}-2} \pmod{t} \qquad (\text{since } a_{\frac{l}{2}+2} = a_{\frac{l}{2}-2}) \\ &= -h_{\frac{l}{2}-4} \pmod{t}. \end{aligned}$$

Thus we have,

$$h_{\frac{l}{2}+1} \equiv h_{\frac{l}{2}-3} \pmod{t}, \qquad h_{\frac{l}{2}+2} \equiv -h_{\frac{l}{2}-4} \pmod{t}, \tag{7.8}$$

and so on. Observing that the positive sign on the right hand side of the congruence precisely when the index on the left hand side is odd, we can conclude that

$$h_{l-2} \equiv -h_0 = -1 \pmod{t}.$$

**Lemma 7.2.5.** *Let $\frac{k_i}{h_i}$ be the $i$-th convergent of $\langle n; \overline{a_1, a_2, ..., a_{l-1}, 2n}\rangle$. Suppose $l$ is congruent to 2 modulo 4. Let $t$ be a divisor of $h_{l-1}$.*
(*i*) *If $t \mid h_{\frac{l}{2}-1}$, then $h_{l-2} \equiv -1 \pmod{t}$.*
(*ii*) *If $t \mid c_{\frac{l}{2}-1}$, then $h_{l-2} \equiv 1 \pmod{t}$.*

The proof is very similar to the previous one.

**Proposition 7.2.6.** *Let $\frac{k_i}{h_i}$ be the $i$-th convergent of the continued fraction of $\sqrt{pq}$ where $p < q$ are primes congruent to 3 modulo 4. Suppose $l$ is the length of the period of $\sqrt{pq}$. Then the greatest common divisor of $h_{\frac{l}{2}-1}$ and $c_{\frac{l}{2}-1}$ is 1 or 2.*

*Proof.* Let $t$ be a common divisor of $h_{\frac{l}{2}-1}$ and $c_{\frac{l}{2}-1}$. By Lemmas 7.2.4 and 7.2.5, we must have $h_{l-2} \equiv 1 \equiv -1 \pmod{t}$ in any case. Therefore, $t$ must divide 2. □

## 7.3 The Fundamental Unit of $\mathbb{Q}(\sqrt{pq})$

The RCF of $\sqrt{pq}$ is related to the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{pq})$. We denote the fundamental unit of $\mathbb{Q}(\sqrt{pq})$ by $\eta$. In this section, we establish a closer relation between certain convergents of $\sqrt{pq}$ and $\eta$. It is well known that when $pq$ is congruent to 1 modulo 8, $\eta$ belong to $\mathbb{Z}[\sqrt{pq}]$. Though $\eta$ may not belong to $\mathbb{Z}[\sqrt{pq}]$ when $pq$ is congruent to 5 modulo 8, $\eta^3$ does. Let $x + y\sqrt{pq}$ denote the smallest unit $> 1$ contained in $\mathbb{Z}[\sqrt{pq}]$. Thus $x+y\sqrt{pq} = \eta$ unless $\eta \notin \mathbb{Z}[\sqrt{pq}]$, in which case $x+y\sqrt{pq} = \eta^3$. It is well known that (e.g., see page 76 of [2]).

$$x + y\sqrt{pq} = k_{l-1} + h_{l-1}\sqrt{pq} = nh_{l-1} + h_{l-2} + h_{l-1}\sqrt{pq}. \tag{7.9}$$

The following lemma is crucial for our subsequent work.

**Proposition 7.3.1.** *Let $p$ and $q$ are primes congruent to 3 modulo 4. Then we have $x = \frac{a^2+pqb^2}{p} = \frac{c^2+pqd^2}{q}$ and $y = \frac{2ab}{p} = \frac{2cd}{q}$ for integers $a, b, c$ and $d$ such that $(a, b) = (c, d) = 1$. Moreover $a^2 - pqb^2 = -p$ and $c^2 - pqd^2 = q$ when $(\frac{q}{p}) = 1$, and $a^2 - pqb^2 = p$ and $c^2 - pqd^2 = -q$ when $(\frac{q}{p}) = -1$.*

*Proof.* As $p$ ramifies in the extension $K$, $p\mathcal{O}_K = \mathfrak{p}^2$. It is well-known that $\mathbb{Q}(\sqrt{pq})$ has odd class number when $p$ and $q$ are primes congruent to 3 modulo 4. Since the ideal class of $\mathfrak{p}$ has order dividing 2, $\mathfrak{p}$ has to be a principal ideal. Therefore, there exists an algebraic integer $\alpha \in \mathcal{O}_K$ and a rational integer $j$ that

$$p\eta^j = \alpha^2.$$

Here as $pq$ is congruent to 1 in modulo 4, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{pq}}{2}]$. So a typical element $\alpha$ of $\mathcal{O}_K$ is in form $\frac{a+b\sqrt{pq}}{2}$, where $a, b \in \mathbb{Z}$. Therefore, we have

$$p\eta^j = \Big(\frac{a + b\sqrt{pq}}{2}\Big)^2. \tag{7.10}$$

If $j$ were even, (7.10) would imply that $\sqrt{p} \in \mathbb{Q}(\sqrt{pq})$. Hence $j$ has to be odd, and we can take $j = 1$ or 3 by absorbing the even powers of the unit $\eta$ on the right hand side of (7.10). Thus,

$$p(x + y\sqrt{pq}) = \Big(\frac{a + b\sqrt{pq}}{2}\Big)^2 \implies 4px = a^2 + pqb^2, \qquad y = \frac{ab}{2p}. \tag{7.11}$$

Now $4px = a^2 + pqb^2$ implies that $a^2 + b^2$ is congruent to 0 in modulo 4, and it is possible

only if $a$ and $b$ both are even. So, we can consider $\alpha = a + b\sqrt{pq}$, where $a, b \in \mathbb{Z}$. Then,

$$p(x + y\sqrt{pq}) = (a + b\sqrt{pq})^2 \implies x = \frac{a^2 + pqb^2}{p}, \qquad y = \frac{2ab}{p}. \tag{7.12}$$

Since $x + y\sqrt{pq}$ is a unit, $a$ and $b$ have to be coprime.
As $-1$ is not a quadratic residue of $p$, the norm of $x + y\sqrt{pq}$ can not be $-1$, i.e.,

$$x^2 - pqy^2 = 1. \tag{7.13}$$

Substituting $x$ and $y$ from (7.12), we obtain

$$\Big(\frac{a^2 + pqb^2}{p}\Big)^2 - 4pqa^2b^2 = 1 \implies a^2 - pqb^2 = \pm p.$$

When $(\frac{q}{p}) = 1$ i.e., $p$ is not a quadratic residue of $q$ and hence

$$a^2 - pqb^2 = -p. \tag{7.14}$$

When $(\frac{q}{p}) = -1$, then $-p$ is not a quadratic residue of $q$ and hence

$$a^2 - pqb^2 = p. \tag{7.15}$$

Now as $q$ is a rational prime which ramifies in $K$, so in similar fashion we can show that there exist mutually coprime integers $c, d \in \mathbb{Z}$ such that

$$q\eta = (c + d\sqrt{pq})^2 \implies x = \frac{c^2 + pqd^2}{q}, \qquad y = \frac{2cd}{q}. \tag{7.16}$$

Substituting $x$ and $y$ from (7.16), we obtain

$$\Big(\frac{c^2 + pqd^2}{q}\Big)^2 - 4pqc^2d^2 = 1 \implies c^2 - pqd^2 = \pm q.$$

When $(\frac{q}{p}) = 1$ i.e., $-q$ is not a quadratic residue of $p$ and hence

$$c^2 - pqd^2 = q. \tag{7.17}$$

When $(\frac{q}{p}) = -1$, then $q$ is not a quadratic residue of $p$ and hence

$$c^2 - pqd^2 = -q. \tag{7.18}$$

□

**Remark 7.3.2.** *When* $(\frac{q}{p}) = 1$, $a^2+3b^2 \equiv 1 \pmod 4$ *by (7.14), and* $c^2+3d^2 \equiv 3 \pmod 4$ *by (7.17). Therefore, a, d must be odd and b, c must be even. By adding and subtracting the pair of equations (7.12) and (7.14), and the pair of equations (7.16) and (7.17), we find that*

$$\begin{aligned} x-1 = \frac{2a^2}{p} = 2pd^2 \quad &\Longrightarrow \quad a = pd, \\ x+1 = 2qb^2 = \frac{2c^2}{q} \quad &\Longrightarrow \quad c = qb. \end{aligned} \tag{7.19}$$

**Remark 7.3.3.** *When* $(\frac{q}{p}) = -1$, *we similarly have a, d as even, and b, c as odd integers. By adding and subtracting the pair of equations (7.12) and (7.15), and the pair of equations (7.16) and (7.18), we find that*

$$\begin{aligned} x+1 = \frac{2a^2}{p} = 2pd^2 \quad &\Longrightarrow \quad a = pd, \\ x-1 = 2qb^2 = \frac{2c^2}{q} \quad &\Longrightarrow \quad c = qb. \end{aligned} \tag{7.20}$$

**Remark 7.3.4.** *In both cases above,* $y = \frac{2ab}{p} = \frac{2cd}{q} = 2bd$.

The following corollaries of Proposition 7.3.1 are needed later.

**Corollary 7.3.5.** *Let p and q are primes congruent to 3 modulo 4 and* $(\frac{q}{p}) = 1$. *Let t be an odd prime factor of* $h_{l-1}$. *Then,*
*(i)* $h_{l-2} \equiv 1 \pmod t$ *if and only if* $t \mid d$.
*(ii)* $h_{l-2} \equiv -1 \pmod t$ *if and only if* $t \mid b$.

*Proof.* By (7.9) and Remark 7.3.4, we have

$$\begin{aligned} y = h_{l-1} = 2bd, \qquad & x-1 = nh_{l-1} + h_{l-2} - 1 = 2d^2p, \\ & x+1 = nh_{l-1} + h_{l-2} + 1 = 2b^2q. \end{aligned} \tag{7.21}$$

If $t$ is an odd prime dividing $h_{l-1} = \frac{2cd}{q}$, then by (7.21) $h_{l-2} \equiv 1 \pmod t$ if and only if $2d^2p \equiv 0 \pmod t$. If $t$ does not divide $d$ then $t = p$. As $p$ divides $h_{l-1}$ so $p$ has to divide $c$ and it leads to contradiction to (7.17). So, $t$ divides $d$. The other implication is trivial from (7.21).

If $t$ is an odd prime dividing $b$, it is evident from (7.21) that $h_{l-2} \equiv -1 \pmod t$. If $h_{l-2} \equiv -1 \pmod t$, then $2b^2q \equiv 0 \pmod t$ by (7.21). Also, $t \mid \frac{2ab}{p} = h_{l-1}$ by Remark 7.3.4. If $t$ does not divide $b$, $t$ has to divide $q$ as well as $a$, which would contradict $a^2 - pqb^2 = -p$. Therefore the converse holds. □

**Corollary 7.3.6.** *Let $p$ and $q$ are primes congruent to 3 modulo 4 and $(\frac{q}{p}) = -1$. Let $t$ be an odd prime factor of $h_{l-1}$. Then,*
*(i)* $h_{l-2} \equiv 1 \pmod{t}$ *if and only if* $t \mid b$.
*(ii)* $h_{l-2} \equiv -1 \pmod{t}$ *if and only if* $t \mid d$.

The argument for the proof runs similar to that of the previous corollary.

## 7.4 The Length of the Period

In this section we prove our theorem concerning the length of the period of the RCF of $\sqrt{pq}$. First we consider the case when $q$ is a quadratic non-residue modulo $p$ in the following proposition.

**Proposition 7.4.1.** *Let $p$ and $q$ are primes congruent to 3 modulo 4 and $l$ denote the length of the period of $\sqrt{pq}$. Suppose $(\frac{q}{p}) = -1$. Then $l$ must be divisible by 4.*

*Proof.* By (7.6) and Remark 7.3.4, we have $y = 2bd = h_{\frac{l}{2}-1}c_{\frac{l}{2}-1}$. If possible, let $l \equiv 2 \pmod 4$. If $t$ is a prime factor of $b$, then by Corollary 7.3.6 $h_{l-2} \equiv 1 \pmod t$ and by Lemma 7.2.5 $t$ is a factor of $c_{\frac{l}{2}-1}$. But $gcd(h_{\frac{l}{2}-1}, c_{\frac{l}{2}-1}) = 1$ or 2 by Proposition 7.2.6, and $b$ is odd by Remark 7.3.3. It follows that $c_{\frac{l}{2}-1} = 2^k b$. Since $2bd = h_{\frac{l}{2}-1}c_{\frac{l}{2}-1}$, we must have $h_{\frac{l}{2}-1} = \frac{d}{2^{k-1}}$.
If $k = 0$, then $c_{\frac{l}{2}-1}$ is odd and $h_{\frac{l}{2}-1}$ is even. Then, the predecessor $h_{\frac{l}{2}-2}$ and successor $h_{\frac{l}{2}}$ must both be odd, and consequently their sum $c_{\frac{l}{2}-1}$ must be even, a contradiction.
If $k \geq 2$, then $c_{\frac{l}{2}-1} \equiv 0 \pmod 4$. Then $h_{l-2} \equiv 1 \pmod 4$ by (ii) of Lemma 7.2.5. Now from (7.21) and Remark 7.3.3, it is clear that, $h_{l-1} \equiv 0 \pmod 4$, since $d$ is even. Therefore, from (7.21) we have $2b^2q \equiv 0 \pmod 4$ which is absurd.
If $k = 1$, we have $c_{\frac{l}{2}-1} = 2b$. As $a^2 - pqb^2 = p$ and $\mid p \mid < \sqrt{pq}$, $\frac{a}{b} = \frac{k_i}{h_i}$ for some $i$. Then $c_{\frac{l}{2}-1} = 2h_i$. By Lemma 7.2.3, $i = 0$ and $b = h_0 = 1$. Then $(k_0 = n, h_0 = 1)$ must satisfy $n^2 - pq = p$, which leads to a contradiction $p + pq = n^2 < pq$.
Therefore, we can conclude that $l$ divisible by 4. □

Next we consider the case when $q$ is a quadratic residue modulo $p$.

**Proposition 7.4.2.** *Let $p$ and $q$ are primes congruent to 3 modulo 4 and $l$ denote the length of the period of $\sqrt{pq}$ with $(\frac{q}{p}) = 1$. Then the continued fraction of $\sqrt{pq}$ has period of length $l \equiv 2$ modulo 4.*

*Proof.* If possible, let $l \equiv 0 \pmod 4$. If $t$ is a prime factor of $d$, then by Corollary 7.3.5 $h_{l-2} \equiv 1 \pmod t$ and by Lemma 7.2.4, $t$ is a factor of $h_{\frac{l}{2}-1}$. But $gcd(h_{\frac{l}{2}-1}, c_{\frac{l}{2}-1}) = 1$ or 2 by Proposition 7.2.6, and $d$ is odd by Remark 7.3.2. It follows that $h_{\frac{l}{2}-1} = 2^k d$. Since $y = 2bd = h_{\frac{l}{2}-1}c_{\frac{l}{2}-1}$, we must have $c_{\frac{l}{2}-1} = \frac{b}{2^{k-1}}$.

If $k = 0$, then $c_{\frac{l}{2}-1} = 2b$. Being a solution of $a^2 - pab^2 = -p$ where $| -p | < \sqrt{pq}$, $(a, b) = (k_i, h_i)$ for some $i$. By Lemma 7.2.3, $i = 0$ and $b = h_0 = 1$. Then $(k_0 = n, h_0 = 1)$ must satisfy $n^2 - pq = -p$, which leads to $n^2 = p(q-1) \equiv 2 \pmod 4$ which is absurd.
If $k \geq 2$, then $h_{\frac{l}{2}-1} \equiv 0 \pmod 4$ implies $h_{l-2} \equiv 1 \pmod 4$ by Lemma 7.2.4, and consequently by (7.21), $nh_{l-1} + h_{l-2} + 1 = 2d^2p \equiv 0 \pmod 4$, which is absurd.
If $k = 1$, we have $c_{\frac{l}{2}-1} = b$. As $a^2 - pab^2 = -p$ and $| -p | < \sqrt{pq}$, $\frac{a}{b} = \frac{k_i}{h_i}$ for some $i$. Then $h_i = c_{\frac{l}{2}-1} = h_{\frac{l}{2}} + h_{\frac{l}{2}-2}$ implies $i > \frac{l}{2}$. But

$$h_i \geq h_{\frac{l}{2}+1} \geq h_{\frac{l}{2}} + h_{\frac{l}{2}-1} > h_{\frac{l}{2}} + h_{\frac{l}{2}-2} \quad \text{for } i > \frac{l}{2}.$$

Therefore, we must have $l \equiv 2 \pmod 4$. □

The Propositions 7.4.1 and 7.4.2 complete the proof of Theorem 7.1.1.

## 7.5 Parity of the Central Term

In this section, we examine the parity of the central term $a_{\frac{l}{2}}$ of the RCF of $\sqrt{pq}$. When $q$ is a quadratic non-residue modulo $p$, we can determine the parity by the following proposition.

**Proposition 7.5.1.** *Let $(\frac{q}{p}) = -1$. Then the central term $a_{\frac{l}{2}}$ in the palindromic part of the period of the RCF of $\sqrt{pq}$ is even.*

However, when $q$ is a quadratic residue modulo $p$ we can conclude about the parity of $a_{\frac{l}{2}}$ only when $p$ is congruent to 3 modulo 8 as stated below.

**Proposition 7.5.2.** *Let $(\frac{q}{p}) = 1$ and $p \equiv 3 \pmod 8$. Then the central term $a_{\frac{l}{2}}$ in the palindromic part of the period of the RCF of $\sqrt{pq}$ is even.*

In order to prove the propositions above, we establish the following lemma.

**Lemma 7.5.3.** *With the notation used previously, $h_{\frac{l}{2}-1} = b$ and $c_{\frac{l}{2}-1} = 2d$.*

*Proof.* First assume that $(\frac{q}{p}) = -1$. By Proposition 7.4.1, the length $l$ of the RCF of $\sqrt{pq}$ is divisible by 4. If $t$ is a prime factor of $b$, then $h_{l-2} \equiv 1 \pmod t$ by Corollary 7.3.6, and $t \mid h_{\frac{l}{2}-1}$ by Lemma 7.2.4. But $gcd(h_{\frac{l}{2}-1}, c_{\frac{l}{2}-1}) = 1$ or 2 by Proposition 7.2.6 and $b$, $c$ are odd by Remark 7.3.3. It follows that $h_{\frac{l}{2}-1} = 2^k b$ and $c_{\frac{l}{2}-1} = \frac{d}{2^{k-1}}$.
If $k \geq 2$, then $h_{\frac{l}{2}-1} \equiv 0 \pmod 4$ implies $h_{l-2} \equiv 1 \pmod 4$ by Lemma 7.2.4, and $nh_{l-1} + h_{l-2} - 1 = \frac{2c^2}{q} \equiv 0 \pmod 4$, which is absurd as $c$ is odd.
If $k = 1$, we have $h_{\frac{l}{2}-1} = 2b$. As $a^2 - pqb^2 = p$ and $| p | < \sqrt{pq}$, $\frac{a}{b} = \frac{k_i}{h_i}$ for some $i$. By Lemma 7.2.3, $i = 0$ and $(k_0 = n, h_0 = 1)$ satisfies $n^2 - pq = p$, which leads to the contradiction $p + pq = n^2 < pq$.

Therefore, $k = 0$ and $h_{\frac{l}{2}-1} = b$. Consequently $c_{\frac{l}{2}-1} = 2d$.

Next assume that $(\frac{q}{p}) = 1$. By Proposition 7.4.2, the length $l$ of the RCF of $\sqrt{pq}$ is congruent to 2 modulo 4, and $a, d$ are odd, $b$, $c$ even. If $t$ is a prime factor of $d$, then $h_{l-2} \equiv 1 \pmod{t}$ by Corollary 7.3.5, and $t \mid c_{\frac{l}{2}-1}$ by Lemma 7.2.5. As $gcd(h_{\frac{l}{2}-1}, c_{\frac{l}{2}-1}) = 1$ or 2 and $d$ is odd, we must have $c_{\frac{l}{2}-1} = 2^k d$. Consequently $h_{\frac{l}{2}-1} = \frac{b}{2^{k-1}}$.
If $k \geq 2$, then $c_{\frac{l}{2}-1} \equiv 0 \pmod{4}$ implies $h_{l-2} \equiv 1 \pmod{4}$ by Lemma 7.2.5, and consequently by (7.21), $nh_{l-1} + h_{l-2} - 1 = 2d^2p \equiv 0 \pmod{4}$, which is absurd.
If $k = 0$, we have $h_{\frac{l}{2}-1} = 2b$. As $a^2 - pqb^2 = -p$ and $\mid -p \mid < \sqrt{pq}$, $\frac{a}{b} = \frac{k_i}{h_i}$ for some $i$. As before, it leads to $n^2 = p(q-1) \equiv 2 \pmod{4}$ which is absurd.
Therefore, $k = 1$ and $c_{\frac{l}{2}-1} = 2d$. Consequently $h_{\frac{l}{2}-1} = b$. □

*Proof of Proposition 7.5.1.* We have

$$\begin{aligned} & a_{\frac{l}{2}} h_{\frac{l}{2}-1} + h_{\frac{l}{2}-2} = h_{\frac{l}{2}} \\ \implies & a_{\frac{l}{2}} h_{\frac{l}{2}-1} + 2h_{\frac{l}{2}-2} = h_{\frac{l}{2}} + h_{\frac{l}{2}-2} = c_{\frac{l}{2}-1} \\ \implies & a_{\frac{l}{2}} b + 2h_{\frac{l}{2}-2} = 2d \qquad \text{(by Lemma 7.5.3).} \end{aligned}$$

When $(\frac{q}{p}) = -1$, $b$ is odd as observed in Remark 7.3.3. Therefore, $a_{\frac{l}{2}}$ must be even. □
*Proof of Proposition 7.5.2*: As before, we have

$$a_{\frac{l}{2}} b + 2h_{\frac{l}{2}-2} = 2d. \tag{7.22}$$

When $(\frac{q}{p}) = 1$, $b$ is even as observed in Remark 7.3.2, and $d$ is odd. Since $h_{\frac{l}{2}-1} = b$ is even, its predecessor $h_{\frac{l}{2}-2}$ is odd. When $p \equiv 3 \pmod{8}$, it follows from (7.19) that $x - 1 \equiv 6 \pmod{16}$ and $2qb^2 = x + 1 \equiv 8 \pmod{16}$ . Consequently $b \equiv 2 \pmod{4}$. By (7.22), we have $2a_{\frac{l}{2}} + 2 \equiv 2 \pmod{4}$, which implies that $a_{\frac{l}{2}}$ must be even. □

Finally, Propositions 7.5.1 and 7.5.2 together imply Theorem 7.1.2.

# CHAPTER 8

# FUTURE PLAN

1. Tada [52] obtained certain necessary and sufficient conditions for a positive square-free number $n$ to be congruent over real quadratic fields $\mathbb{Q}(\sqrt{m})$ and classified the corresponding right-triangles according to the types of their sides. We would like to explore such classification on the basis of the sides of the corresponding triangles over more general number fields.

2. Steuding [50] and Komatsu [35] examined the relation between the continued fraction expansion of some special types of irrational numbers (such as $\sqrt{n^2+1}$ or $\sqrt{n^2+2}$) to rational right triangles of area close to certain natural numbers. We would like to explore and establish such connection for more general quadratic irrationals.

3. Girard, Lalín and Nair [20] have constructed families of non-$\theta$-congruent numbers with arbitrarily many prime factors of special types. Mokrani [39] used Monky matrices to construct new families of non-$\frac{\pi}{3}$-congruent numbers and non-$\frac{2\pi}{3}$-congruent numbers. We would like to construct families of $\frac{\pi}{3}$- or $\frac{2\pi}{3}$-non-congruent numbers with arbitrarily many prime factors of types not yet covered in the literature. In order to obtain stronger results concerning non-congruent (resp. non-$\frac{\pi}{3}$- or non-$\frac{2\pi}{3}$-congruent) numbers, we would like to use 2-Selmer group of congruent number elliptic curve (resp. $\frac{\pi}{3}$- and $\frac{2\pi}{3}$-congruent number elliptic curves).

# LIST OF PUBLICATIONS FROM THE THESIS

- S. Das, D. Chakraborty and A. Saikia. *On the continued fraction of* $\sqrt{pq}$, Acta Arithmetica 196 (2020), no. 3, 291–302.

- S. Das and A. Saikia. *Families of non-congruent numbers with arbitrarily many pairs of prime factors*, Integers 20 (2020), Paper No. A55, 12 pp.

- S. Das and A. Saikia. *On* $\theta$*-congruent numbers over real number fields*, Bulletin of Australian Mathematical Society 103 (2021), no. 2, 218–229.

- S. Das and A. Saikia. *Families of even non-congruent numbers with arbitrarily many pairs of prime factors*, accepted for publication in Rocky Mountain Journal of Mathematics.

- S. Das and A. Saikia. *Families of highly composite non-congruent numbers*, communicated.

- S. Das. and A. Saikia. *On the class number of* $\mathbb{Q}(\sqrt{-pq})$ *when* $pq$ *is congruent for primes* $p \equiv 5 \pmod 8$ *and* $q \equiv 7 \pmod 8$, communicated.

# BIBLIOGRAPHY


[1] R. Alter. Research Problems: The Congruent Number Problem. *Amer. Math. Monthly*, 87(1):43–45, 1980.

[2] A. Baker. *A concise introduction to the theory of numbers*. Cambridge University Press, Cambridge, 1984.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[5] E. Brown. The class-number of $\mathbb{Q}(\sqrt{-pq})$, for $p \equiv -q \equiv 1 \pmod 4$ primes. *Houston J. Math.*, 7(4):497–505, 1981.

[6] D. M. Burton. *Elementary number theory*. W. C. Brown Publishers, Dubuque, IA, second edition, 1989.

[7] D. Chakraborty and A. Saikia. On a conjecture of Mordell. *Rocky Mountain J. Math.*, 49(8):2545–2556, 2019.

[8] W. Cheng and X. Guo. The non-congruent numbers via Monsky's formula. *Int. J. Number Theory*, 15(4):677–711, 2019.

[9] W. Cheng and X. Guo. Some new families of non-congruent numbers. *J. Number Theory*, 196:291–305, 2019.

[10] P. Chowla and S. Chowla. Problems on periodic simple continued fractions. *Proc. Nat. Acad. Sci. U.S.A.*, 69:3745, 1972.

[11] J. E. Cremona and P. Serf. Computing the rank of elliptic curves over real quadratic number fields of class number 1. *Math. Comp.*, 68(227):1187–1200, 1999.

[12] H. B. Daniels and E. González-Jiménez. On the torsion of rational elliptic curves over sextic fields. *Math. Comp.*, 89(321):411–435, 2020.

[13] H. Davenport. *The higher arithmetic.* Cambridge University Press, Cambridge, seventh edition, 1999. An introduction to the theory of numbers, Chapter VIII by J. H. Davenport.

[14] T. Dokchitser and V. Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1):567–596, 2010.

[15] E. Fouvry and J. Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.

[16] E. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, 101(2):337–391, 2010.

[17] J. B. Fraleigh. *A first course in abstract algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[18] C. Friesen. On continued fractions of given period. *Proc. Amer. Math. Soc.*, 103(1):9–14, 1988.

[19] M. Fujiwara. $\theta$-congruent numbers. In *Number Theory (Eger, 1996)*, pages 235–241. de Gruyter, Berlin, 1998.

[20] V. Girard, M. N. Lalín, and S. C. Nair. Families of non-$\theta$-congruent numbers with arbitrarily many prime factors. *Colloq. Math.*, 152(2):255–271, 2018.

[21] E. P. Golubeva. Quadratic irrationalities with a fixed length of the period of continued fraction expansion. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 196(Modul. Funktsii Kvadrat. Formy. 2):5–30, 172, 1991.

[22] E. González-Jiménez. Complete classification of the torsion structures of rational elliptic curves over quintic number fields. *J. Algebra*, 478:484–505, 2017.

[23] E. González-Jiménez and F. Najman. Growth of torsion groups of elliptic curves upon base change. *Math. Comp.*, 89(323):1457–1485, 2020.

[24] E. González-Jiménez, F. Najman, and J. M. Tornero. Torsion of rational elliptic curves over cubic fields. *Rocky Mountain J. Math.*, 46(6):1899–1917, 2016.

[25] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

[26] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[27] K. Hoffman and R. Kunze. *Linear algebra*. Second edition. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1971.

[28] B. Iskra. Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(7):168–169, 1996.

[29] A. S. Janfada and S. Salami. On $\theta$-congruent numbers on real quadratic number fields. *Kodai Math. J.*, 38(2):352–364, 2015.

[30] T. Jędrzejak. Congruent numbers over real number fields. *Colloq. Math.*, 128(2):179–186, 2012.

[31] M. Kan. $\theta$-congruent numbers and elliptic curves. *Acta Arith.*, 94(2):153–160, 2000.

[32] M. Kazalicki. Congruent numbers and congruences between half-integral weight modular forms. *J. Number Theory*, 133(4):1079–1085, 2013.

[33] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[34] N. Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.

[35] T. Komatsu. Congruent numbers and continued fractions. *Fibonacci Quart.*, 50(3):222–226, 2012.

[36] J. Lagrange. Nombres congruents et courbes elliptiques. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 16(1), 1974-1975. talk:16.

[37] F. Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[38] C. Meyer. *Matrix analysis and applied linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2000. With 1 CD-ROM (Windows, Macintosh and UNIX) and a solutions manual (iv+171 pp.).

[39] Y. Mokrani. Adaptation of Monsky matrices for $\theta$-congruent numbers. *Int. J. Number Theory*, 16(2):377–396, 2020.

[40] P. Monsky. Mock Heegner points and congruent numbers. *Math. Z.*, 204(1):45–67, 1990.

[41] D. Prasad and C. S. Yogananda. Bounding the torsion in CM elliptic curves. *C. R. Math. Acad. Sci. Soc. R. Can.*, 23(1):1–5, 2001.

[42] D. Qiu and X. Zhang. Elliptic curves and their torsion subgroups over number fields of type $(2, 2, \ldots, 2)$. *Sci. China Ser. A*, 44(2):159–167, 2001.

[43] L. Reinholz, B. K. Spearman, and Q. Yang. On the prime factors of non-congruent numbers. *Colloq. Math.*, 138(2):271–282, 2015.

[44] L. Reinholz, B. K. Spearman, and Q. Yang. An extension theorem for generating new families of non-congruent numbers. *Funct. Approx. Comment. Math.*, 58(1):69–77, 2018.

[45] L. Reinholz, B. K. Spearman, and Q. Yang. Families of even non-congruent numbers with prime factors in each odd congruence class modulo eight. *Int. J. Number Theory*, 14(3):669–692, 2018.

[46] P. Serf. Congruent numbers and elliptic curves. In *Computational number theory (Debrecen, 1989)*, pages 227–238. de Gruyter, Berlin, 1991.

[47] A. Silverberg. Points of finite order on abelian varieties. In *p-adic methods in number theory and algebraic geometry*, volume 133 of *Contemp. Math.*, pages 175–193. Amer. Math. Soc., Providence, RI, 1992.

[48] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[49] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[50] J. Steuding. What Fibonacci numbers have to do with congruent numbers? *Fibonacci Quart.*, 49(4):330–333, 2011.

[51] I. Stewart and D. Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.

[52] M. Tada. Congruent numbers over real quadratic fields. *Hiroshima Math. J.*, 31(2):331–343, 2001.

[53] Y. Tian. Congruent numbers and Heegner points. *Camb. J. Math.*, 2(1):117–161, 2014.

[54] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.