# A Study of Torsion of Elliptic Curves and Fundamental Units over Number Fields

Naba Kanta Sarma


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

September, 2018.

# A Study of Torsion of Elliptic Curves and Fundamental Units over Number Fields

*A thesis submitted*

*in partial fulfillment of the requirements*

*for the degree of*

**DOCTOR OF PHILOSOPHY**

by

**Naba Kanta Sarma**

(Roll No.: 126123007)

to

**Department of Mathematics**

**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI**

**September, 2018.**

*To*

*My Father*

# Declaration

This is to certify that the thesis entitled "**A Study of Torsion of Elliptic Curves and Fundamental Units over Number Fields**", submitted by me to *Indian Institute of Technology Guwahati*, for award of the degree of Doctor of Philosophy, is a bona fide work carried out by me under the supervision of Prof. Anupam Saikia. The contents of this thesis, in full or in parts, have not been submitted to any other University or Institute for award of any degree or diploma. I also wish to state that, to the best of my knowledge and understanding, nothing in this report amounts to plagiarism.

September 2018

Naba Kanta Sarma
Roll no. 126123007
Department of Mathematics
Indian Institute of Technology Guwahati

# Certificate

This is to certify that the thesis entitled "**A Study of Torsion of Elliptic Curves and Fundamental Units over Number Fields**", submitted by Mr. Naba Kanta Sarma to *Indian Institute of Technology Guwahati*, for award of the degree of Doctor of Philosophy, is a record of the original bona fide research work carried out by him under my supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The contents of this thesis, in full or in parts, have not been submitted to any other University or Institute for award of any degree or diploma. I also wish to state, that to the best of my knowledge and understanding, nothing in this report amounts to plagiarism.

September 2018

Prof. Anupam Saikia
Thesis Supervisor
Department of Mathematics
Indian Institute of Technology Guwahati

# Acknowledgements

I would like to take this opportunity to express my gratitude and appreciation to the contribution of everyone who has influenced in the outcome of this thesis.

First of all, I offer my gratitude to my thesis supervisor Prof. Anupam Saikia for his valuable inputs and suggestions during the entire period. His motivating words during difficult phases of this journey have been invaluable. Whenever I have looked up to him for his inputs, he was ever ready and willing to discuss my doubts. I am grateful to him for reviewing my thesis carefully and suggesting improvements from time to time. I am grateful to Prof. Filip Najman for his valuable e-mails that helped me enormously in the first half of my work. I am indebted to Dr. Debopam Chakraborty of Tezpur University for his valuable suggestions in the later half of my work in this thesis.

I would like to extend my gratitude to my doctoral committee members Prof. Bhaba Kumar Sarma, Dr. PAS Sreekrishna and Dr. Shyamashree Upadhyaya for reviewing my work every year and suggesting improvements each time which immensely improved my work. I humbly acknowledge the facilities provided at Indian Institute of Technology Guwahati (IITG) to carry out my research. I am also grateful to Assam university, Silchar, where I have been an assistant professor since 2008, for granting me three years of study leave without which I could not have fulfilled my dream of completing my research at Indian Institute of Technology Guwahati. On this occasion, I thank all the research scholars, teaching as well as non-teaching staffs of both these institutes for their overwhelming support.

I have been motivated by a few excellent teachers throughout my academic life. Special mention must be made to Prof. S. Kumaresan and Prof. Rajat Tandon of the University of Hyderabad, Prof. J.K. Verma, IIT Bombay, Dr. Anjan Chakraborty, IIT Guwahati and Prof. Tarun Sirkar and Prof. Biswajit Bhagawati of Cotton College, Guwahati, who all have a special place in my heart for their dedication to teaching. I am also thankful to Dhiren da and Uday for their ever-willing interest to discuss anything. I owe a great deal to my school teachers for what I am today. I take this opportunity to appreciate their influence in my life and wish them all good health in the final stage

of their lives.

I am lucky to have made a few real friends throughout my life and to add a few more here at IITG to this list during my thesis work. From my school days, I made some never-failing friends in Sachindra, Amal and Bhaskar. I owe a great deal to Chiku and Hamidul, who supported me by providing books and study materials during my college and university education. I thank Jayanta, Ankur, Sougata, Swapnendu, Ashish, Ramesh, Ranjan, Maneesh, Barun, Himadri, Murali, Dishari, Saloni, Abhishek, Anirban and many others with whom I shared some of the best moments of my life during my thesis work at IITG.

It is not possible for me to express in words my gratitude towards my parents for everything they did for me. My mother has been a constant source of inspiration in my life. Her stability and composure in difficult stages in our lives has been a great lesson for me. My father was a great influence in the formative years of my life. He would have been the happiest man had he been alive today. I fondly remember him today and dedicate this thesis to him.

I owe my thanks and gratitude to all my family members and relatives, specially Pulu Da, Mani Da, Dulu Baidew, Putuli Baidew, Bhanti Baidew, Auto Baidew, BAni, Mausumi and Umesh Moha to name a few, for their support throughout the journey. At this juncture of my life, I could not help mentioning Pinku and his family for supporting our family in all possible ways, when we were rendered homeless during my M.Sc days.

Finally, I am deeply indebted to my beloved wife Panchi for her unconditional love and support throughout this journey. She took complete care of our cutest children Nibir and Harshit single-handedly to allow me to focus on my research. Without her support, I could not have completed this thesis. The role played by my parents-in-law deserves special mention for giving me the peace of mind by their support in bringing our my children.

# Abstract

The primary objective of the first half of this thesis titled "A Study of Torsion of Elliptic Curves and Fundamental Units over Number Fields" is to study the torsion subgroup of elliptic curves over certain quadratic number fields. In the second half of the thesis, we derive certain congruence relations for the fundamental unit of totally imaginary biquadratic number fields of odd class number by refining existing congruences for the fundamental unit of its maximal real subfield.

The first part of the work is devoted to finding possible torsion structures over given quadratic fields. In 1922, Louis Mordell proved that the group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated and in 1928, André Weil generalized this result for abelian varieties over algebraic number fields. In 1977, Barry Mazur opened up a vast area of research by listing all possible torsion subgroups of all possible elliptic curves over the rational field. He showed that only 15 possible groups can occur as the torsion subgroup of elliptic curves over $\mathbb{Q}$. After extensive collaborations among various mathematicians, Kenku, Momose and Kamienny to name a few, a complete list of 26 groups was finally published for the torsion subgroup of elliptic curves over all possible quadratic number fields.

In 2011, Najman computed the torsion subgroups of all elliptic curves over the imaginary quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ separately. In 2012, Kamienny and Najman outlined an approach that can be used to study the possible torsion structures over a quadratic field. We follow their method in determining the possible torsion structures over the remaining imaginary quadratic fields of class number 1 i.e over the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$. We also compute the possible torsion structures over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, which have the smallest discriminants among all real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \mod 4$ and $d \equiv 1 \mod 4$ respectively.

In the latter half of our work, we prove certain congruence relations for the fundamental unit of totally imaginary biquadratic fields of odd class number. In 2014, Zhang and Yue obtained certain congruence relations for the fundamental unit of real

quadratic fields of odd class number by using 2-adic analysis. In 2016, Chakraborty and Saikia obtained the same congruences by elementary methods. We refine these congruences by using ramification of primes in quadratic fields. We then use these congruences to establish certain congruence relations for the fundamental unit of totally imaginary biquadratic fields of odd class number.

# Contents

# List of Symbols

| | |
|---|---|
| $\overline{K}$ | A fixed algebraic closure of a given field $K$ |
| $\mathbb{Z}$ | The ring of integers |
| $\mathbb{Q}$ | The field of rational numbers |
| $\mathbb{C}$ | The field of complex numbers |
| $\mathbb{F}_{p^n}$ | The finite field with $p^n$ elements |
| $\mathbb{H}$ | The complex upper half plane |
| $\mathbb{H}^*$ | The extended complex upper half plane |
| $E(K)$ | Group of $K$-rational points of an elliptic curve over a number field $K$ |
| $E(K)_{tors}$ | Torsion subgroup of $E(K)$ |
| $\mathcal{C}_N$ | The finite cyclic group of order $N$ |
| $\mathbb{A}^2(\overline{K})$ | Affine plane over a field $K$ |
| $\mathbb{P}^2(\overline{K})$ | Projective plane over a field $K$ |
| $E[N]$ | The subgroup of $E(\overline{K})$ of points having order dividing $N$ |
| $E(K)[N]$ | The subgroup of $E[N]$ of points having co-ordinates in $K$ |
| $\mathcal{O}$ | The point at infinity for an elliptic curve over a field |
| $\mathcal{O}_K$ | The ring of integers of a number field $K$ |
| $\mathcal{O}_K^\times$ | The group of units of $\mathcal{O}_K$ |
| $E^d$ | Quadratic twist of an elliptic curve $E$ by $d$ |
| $\mathrm{Gal}(L/K)$ | Galois group of $L$ over $K$ |
| $J(C)$ | Jacobian of an algebraic curve $C$ |
| $K(C)$ | Field of rational functions of an algebraic curve $C$ |
| $SL(2,\mathbb{Z})$ | The modular group of $2\times 2$ matrices with integer entries with determinant 1 |
| $\Gamma_1(M,N)$ | Congruence subgroup of $SL(2,\mathbb{Z})$ level $N$ |
| $Y_1(M,N)$ | Modular curve of level $N$ |
| $d(K)$ | Discriminant of a number field $K$ |
| $h(K)$ | Class number of a number field $K$ |

# Chapter 1

# Introduction

The primary objective of our work in this thesis is to study the groups that can occur as the torsion subgroup of the group of $K$-rational points on an elliptic curve over certain quadratic number fields. By an elliptic curve $E$ over a number field $K$, we mean the projective closure of a smooth plane curve of the form $y^2 = f(x)$, where $f$ is a separable polynomial over $K$ of degree 3. Around 1900, Henri Poincaré showed that the set $E(K)$ of $K$-rational points on a given elliptic curve $E$ over a given field $K$, together with a specified base point $\mathcal{O}$, can be given the structure of an abelian group in the projective setting using a geometric chord-tangent law. He further conjectured that the group $E(\mathbb{Q})$ is finitely generated and it was proved in the affirmative in 1922 by Louis Mordell. In 1928, André Weil generalized this result for abelian varieties over algebraic number fields (finite extensions of $\mathbb{Q}$).

In a seminal work in 1977, Barry Mazur [22] listed all possible torsion subgroups of all possible elliptic curves over the rational field $\mathbb{Q}$. He showed that only 15 groups can occur as the torsion subgroup of an elliptic curve if we vary the elliptic curve over $\mathbb{Q}$. He found these groups explicitly as $\mathcal{C}_n, \quad 1 \leq n \leq 12, n \neq 11$ and $\mathcal{C}_2 \times \mathcal{C}_{2n}, \ 1 \leq n \leq 4$, where $\mathcal{C}_n$ denotes the finite cyclic group of order $n$. In 1986, Reichert [30] constructed explicit elliptic curve $E$ for each of these 15 groups $G$ such that $E(\mathbb{Q})_{tors} = G$. It is now known that each of these 15 groups can be realised as $E(\mathbb{Q})_{tors}$ for infinitely many

non-isomorphic elliptic curves over $\mathbb{Q}$.

The quadratic number fields are the only case where a direct analogue of Mazur's theorem is available till date. It took a collective effort of many researchers before it was finally shown in 1992 in a series of papers by Kenku, Momose [19] and Kamienny [17] that 11 additional groups can occur as the torsion subgroup of elliptic curves over all possible quadratic number fields. These are the groups $\mathcal{C}_n, \quad n = 11, \quad 13 \leq n \leq 18, n \neq 17, \ \mathcal{C}_2 \times \mathcal{C}_{2n}, \ n = 5, 6, \ \mathcal{C}_3 \times \mathcal{C}_{3n}, \ 1 \leq n \leq 2$ and $\mathcal{C}_4 \times \mathcal{C}_4$. It was also shown that the groups $\mathcal{C}_3 \times \mathcal{C}_3$ and $\mathcal{C}_3 \times \mathcal{C}_6$ can occur over the quadratic field $\mathbb{Q}(\sqrt{-3})$ only, while the group $\mathcal{C}_4 \times \mathcal{C}_4$ can occur over the quadratic field $\mathbb{Q}(\sqrt{-1})$ only.

There is no direct analogue of Mazur's theorem over number fields of degree higher than two yet. Over cubic fields, the largest prime that can divide the order of the torsion subgroup of an elliptic curve defined over a cubic number field is 13. This was proved by Pierre Parent in 2003 ( [27], [28]). In 2004 Jeon, Kim and Schweizer [16] determined all the torsion subgroups that arise for an infinite number of non-isomorphic elliptic curves over cubic number fields by classifying trigonal modular curves (those modular curves which can be realized as a 3-sheeted covering of $\mathbb{P}_1$ ). However, it is not yet completely known which groups may appear as torsion for only finitely many non-isomorphic elliptic curves. In 2004, Jeon, Kim, and Lee gave explicit parametrization for each case [14]. In 2016, F. Najman [26] found that the group $\mathcal{C}_{21}$ occurs only for one elliptic curve, namely the elliptic curve $162B1$ over $\mathbb{Q}(\zeta_9)^+$ (as per Cremona's table). Similar results are now available for quartic, quintic and sextic fields ( [8], [15]).

The above results regarding torsion list the possible torsion subgroups of elliptic curves if the elliptic curves are allowed to vary over all number fields of a given degree. However, it does not reveal any information which torsion subgroups will occur if the elliptic curves are allowed to vary only over a fixed number field except for the fact that the list of subgroups in the later case will be a subset of the corresponding list when the number field is also allowed to vary as in the preceding paragraph. In 2011, Filip

Najman ( [23], [24]) considered this problem when the number field is a given quadratic field. He computed the torsion subgroups of all elliptic curves over the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ separately. In 2012, Najman and Kamienny [18] described methods that can be applied to compute the torsion subgroup for any given quadratic field. We follow their method in determining the possible torsion structures over the remaining imaginary quadratic fields of class number 1 i.e. over the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$ [33]. We also compute the possible torsion structures over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, which have the smallest discriminants among all real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \bmod 4$ and $d \equiv 1 \bmod 4$ respectively [32]. We use a freely available version of MAGMA for our computations.

In the latter half of our work, we prove certain congruence relations of the fundamental unit of totally imaginary biquadratic fields of odd class number. Such a biquadratic field must have the form $\mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ or $\mathbb{Q}(\sqrt{-2}, \sqrt{-p})$, where $p \equiv q \equiv (3 \bmod 4)$ are distinct primes [7]. The ring of integers of a number field $K$ is the integral closure of the rational integers in $K$ and is denoted by $\mathcal{O}_K$. A fractional ideal of $K$ is a non-zero $\mathcal{O}_K$- module $I \subset K$ such that $dI \subset \mathcal{O}_K$ for some $0 \neq d \in \mathcal{O}_K$. The ideal class group of $K$ is the quotient group of all fractional ideals of $\mathcal{O}_K$ by the subgroup of all principal fractional ideals. The order of the ideal class group of a number field is known to be finite and is known as the class number of the number field. Loosely speaking, class number of a number field gives a measure how much it deviates from being a unique factorization domain. It is well known that $\mathcal{O}_K$ is a unique factorization domain precisely when class number of $K$ is 1. The relevant definitions are made more precise in the next chapter.

By Dirichlet's unit theorem, we know that the group of units of $\mathcal{O}_K$ has rank 1 for a totally imaginary biquadratic field $K := \mathbb{Q}(\sqrt{-d_1}, \sqrt{-d_2})$. The group of units of the maximal real quadratic subfield $k := \mathbb{Q}(\sqrt{d_1 d_2})$ is also of rank 1. So there exist units $\xi_K, \xi_k > 1$ such that all other units are of the form $\zeta \xi_K^m$, $\eta \xi_k^n$, where $m, n \in \mathbb{Z}$ and $\zeta, \eta$

are some roots of unity in $K$ and $k$ respectively. $\xi_K$ and $\xi_k$ are called fundamental units of the number fields $K$ and $k$ respectively. We study the relation between $\xi_k$ and $\xi_K$ in certain cases and use them to obtain congruence relations for the fundamental unit $\xi_K$ in those cases. In 2014, Zhang and Yue [41] obtained certain congruence relations for the fundamental unit of real quadratic fields of odd class number by using 2-adic analysis. In 2016, Chakraborty and Saikia [5] obtained these same congruences by elementary methods. We have refined these congruences by using ramification of primes in quadratic fields. We then use these congruences to prove certain congruence relations for the fundamental unit of totally imaginary biquadratic fields of odd class number [31].

In chapter 2, we develop the necessary tools for our subsequent work. In chapter 3, we discuss our results about the torsion subgroups of elliptic curves over imaginary quadratic fields of class number 1 and also over real quadratic fields of the smallest discriminant. The results contained in this chapter have been accepted for publication ( [32], [33]). In chapter 4, we present our improved results about the congruent relations satisfied by the fundamental unit of real quadratic fields of odd class number. In chapter 5, we use the results in chapter 4 to prove certain congruence relations satisfied by the fundamental unit of totally imaginary biquadratic number fields of odd class number. The results in this chapter have been communicated ( [31]).

# Chapter 2

# Background

In this chapter we briefly discuss the basic theory and some well-known results that we need later.

## 2.1 Elliptic curves

The following definitions and results can be found in any standard text on elliptic curves e.g. ( [21], [34], [38]).

**Projective plane**: Let $K$ be any field and $\overline{K}$ denotes a fixed algebraic closure of $K$. The affine plane over $K$, denoted by $\mathbb{A}^2$, is the set

$$\mathbb{A}^2 = \mathbb{A}^2(\overline{K}) := \{(x, y) : x, y \in \overline{K}\}.$$

The set of $K-$rational points of $\mathbb{A}^2$ i.e. the set of points with components in $K$ is denoted by $\mathbb{A}^2(K)$. The projective Plane over $K$, denoted by $\mathbb{P}^2 = \mathbb{P}^2(\overline{K})$, is the set of all equivalence classes $[x, y, z]$ of $(x, y, z) \in \mathbb{A}^3 - \{(0, 0, 0)\}$ arising from the equivalence relation

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$$

for some $0 \neq \lambda \in K$. The set of $K$-rational points in $\mathbb{P}^2$ is the set

$$\mathbb{P}^2(K) = \{[x, y, z] \in \mathbb{P}^2 : x, y, z \in K\}$$

The plane $\mathbb{A}^2(K)$ has a standard embedding in $\mathbb{P}^2(K)$ via the map

$$(x, y) \mapsto [x, y, 1].$$

The set that is missed by the image is the set where $z = 0$. These points with $z = 0$ are called the points at infinity. The set of points $[x, y, z]$ with $z = 0$ is called the line at infinity.

The main advantage of working over projective plane is that intersection theory works much better in projective plane. Bezout's theorem ensures that two projective curves $C_1$ and $C_2$ of degree $m$ and $n$ respectively over the complex field $\mathbb{C}$ intersects in exactly $mn$ points, counting multiplicity, provided $C_1, C_2$ have no common irreducible component.

**Projective closure of plane curves**: An algebraic curve in the affine plane $\mathbb{A}^2$ is the set of solutions to a polynomial equation in two variables of the form $f(x, y) = 0$. The homogenization of a polynomial $f(x, y)$ of degree $d$ is the homogeneous polynomial

$$F(X, Y, Z) := Z^d f(X/Z, Y/Z).$$

One can recover $f$ via $f(x, y) = F(X, Y, 1)$.

If $f(x, y) = 0$ is a plane curve C in $\mathbb{A}^2(K)$, then its projective closure is defined to be the curve $\tilde{C}$ in $\mathbb{P}^2(K)$ defined by the homogenized equation $F(X, Y, Z) = 0$. The curve $\tilde{C}$ equals $C$ together with some points at infinity.

**Elliptic curve over a field**: An elliptic curve $E$ over a field $K$ is defined as the projective closure of a smooth plane curve defined by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K. \tag{2.1.1}$$

If ch $K \neq 2, 3$, we can reduce the equation to the short Weierstrass form

$$y^2 = x^3 + Ax + B, \quad A, B \in K.$$

When $K = \mathbb{Q}$, the equation can be further reduced to the form

$$E: \ Y^2 = X^3 + AX + B: \quad A, B \ \in \mathbb{Z}.$$

The discriminant of the elliptic curve in short Weierstrass form is defined to be the quantity

$$D := (\alpha_0 - \alpha_1)^2(\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_0)^2 = 4A^3 + 27B^2,$$

where $\alpha_0, \alpha_1, \alpha_2$ are the roots of the polynomial $X^3 + AX + B$. The smoothness of the elliptic curve is equivalent to requirement that $D \neq 0$, which is further equivalent to the equation $x^3 + Ax + B = 0$ having distinct roots

**Group structure in elliptic curves**: Let $K$ be any number field and $\overline{K}$ denotes a fixed algebraic closure of $K$. Let $E$ be any elliptic curve over $K$ given by the short Weierstrass form. The points at infinity corresponds to $Z = 0$ in the corresponding homogenized polynomial and this leads to $X = 0$. Hence an elliptic curve has a unique point at infinity $[0, 1, 0]$ which we denote by $\mathcal{O}$. The set

$$E(\overline{K}) := \{(x, y) \in \overline{K}^2 : y^2 = x^3 + Ax + B, \quad A, B \in K\} \cup \{\mathcal{O}\}$$

forms an abelian group group under a geometric chord tangent law with $\mathcal{O}$ as the identity element. The additive group law can be computed explicitly as

$$(x_1, y_1) + (x_2, y_2) := (x_3, -y_3),$$

where $x_3 := \lambda^2 - A - x_1 - x_2$, $y_3 := \lambda x_3 + \nu$, $\lambda := \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu := y_1 - \lambda x_1$. Since this formula makes sense over any field, we see that for any field $K$, the set

$$E(K) := \{(x, y) \in K^2 : y^2 = x^3 + Ax + B, \quad A, B \in K\} \cup \{\mathcal{O}\}$$

forms a subgroup of $E(\overline{K})$. It is known that, $E(K)$ is a finitely generated group for any number field $K$.

**Torsion points on elliptic curves**: Let $E$ be an elliptic curve defined over a field $K$. For $N \in \mathbb{N}$, the set

$$E[N] := \{P \in E(\overline{K}) : NP = \mathcal{O}\}$$

forms a subgroup of $E(\overline{K})$. If ch $K = 0$ or ch $K = p \nmid N$, then we can see that

$$E[N] = \mathcal{C}_N \times \mathcal{C}_N,$$

where $\mathcal{C}_N$ denotes the finite cyclic group of order $N$. We also define,

$$E(K)[N] := \{P \in E(K) : NP = \mathcal{O}\}$$

Clearly $E(K)[N]$ is a subgroup of $E[N]$. In particular, we have,

$$E(\mathbb{Q})[N] \leq E[N] = \mathcal{C}_N \times \mathcal{C}_N.$$

**Quadratic twist of elliptic curves**: If $E$ is an elliptic curve over a field $K$ with short Weierstrass equation

$$E: \quad y^2 = x^3 + Ax + B$$

Then its $d$-quadratic twist is defined by the equation

$$E^d: \quad y^2 = x^3 + d^2Ax + d^3B.$$

Note this curve is isomorphic over $K$ to the curve with equation

$$dy^2 = x^3 + Ax + B.$$

Note further that, the map defined by

$$T : E^d \to E, \quad (x, y) \to (x, y\sqrt{d})$$

defines an isomorphism over $K(\sqrt{d})$. Hence if $d$ is a square in $K$, then $E$ and $E^d$ are isomorphic over all extensions of $K$ and if $d$ is not a square in $K$, then we have $E(K(\sqrt{d})) \cong E^d(K(\sqrt{d}))$.

**Theorem 2.1.1.** *(González-Jimenéz, Tornero, [12]) Let $K$ be a quadratic number field, $L = K(\sqrt{d})$ a quadratic extension of $K$ and let $\sigma$ denote the generator of $Gal(L/K)$. Then there exist homomorphisms*

$$f : E(K) \times E^d(K) \to E(L), \quad g : E(L) \to E(K) \times E^d(K)$$

*such that the kernels and co-kernels of $f$ and $g$ are annihilated by* [2]. *In particular, if $N$ is odd, we have*

$$E(K(\sqrt{d}))[N] \cong E(K)[N] \times E^d(K)[N].$$

The following theorem [21] plays a crucial role in studying the 2-part of the torsion of an elliptic curve:

**Theorem 2.1.2.** *Let $E$ be an elliptic curve over a field $K$ with ch $K \neq 2, 3$. Suppose $E$ is given by*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

*with $\alpha, \beta, \gamma \in K$. For $P = (x_0, y_0)$ in $E(K)$, there exists $Q \in E(K)$ such that $2Q = P$ iff $x_0 - \alpha, x_0 - \beta, x_0 - \gamma$ are squares in $K$.*

**Division polynomials**: Let $E$ be an elliptic curve over a field $K$ defined by the short Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

We define [38] the division polynomials $\psi_n \in \mathbb{Z}[x, y, A, B]$ by

$$\begin{aligned}
\psi_0 &= 0,\ \psi_1 = 1,\ \psi_2 = 2y;\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2;\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3);\\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \quad n \geq 2;\\
\psi_{2n} &= (2y)^{-1}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \quad n \geq 3.
\end{aligned}$$

It can be checked that $\psi_n$ is a polynomial in $\mathbb{Z}[x, y^2, A, B]$ when $n$ is odd, and $\psi_n$ is a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$ when $n$ is even. We next define the polynomials

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1};\\
\omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).
\end{aligned}$$

One can check that $\phi_n \in \mathbb{Z}[x, y^2, A, B]$ for all $n$. If $n$ is odd, then $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$. If $n$ is even, then $\omega_n \in \mathbb{Z}[x, y^2, A, B]$. Replacing $y^2$ with $x^3 + Ax + B$, we see that $\phi_n$ and $\psi_n^2$ can be considered as polynomials in $x$ only. Division polynomials are related to torsion points on an elliptic curve by the following theorem:

**Theorem 2.1.3.** *Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$ and let $N$ be a positive integer. Then*

$$NP = \Big(\frac{\phi_N(x)}{\psi_N^2(x)}, \frac{\omega_N(x,y)}{\psi_N^3(x,y)}\Big).$$

Note that

$$NP = \mathcal{O} \iff \psi_N(x(P)) = 0.$$

**Rank of an elliptic curve**: Let $E$ be an elliptic curve over a number field $K$. Then by Mordell-Weil's theorem, $E(K)$ is a finitely generated abelian group. As a result, there exist a non-negative integer $r$ such that

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r.$$

The non-negative integer $r$ is called the rank of the elliptic curve over $K$. In MAGMA, one can compute the rank of any elliptic curve over the rational field. The rank of any rational elliptic curve $E$ over any quadratic field $K = \mathbb{Q}(\sqrt{d})$ can be computed using the relation

$$\text{rank } (E(\mathbb{Q}(\sqrt{d}))) = \text{ rank}(E(\mathbb{Q})) + \text{ rank } (E^d(\mathbb{Q})),$$

where $E^d$ denote the quadratic twist of $E$ ( Ex 10.16, [34])

**Reduction of an elliptic curve modulo a prime** $p$: Let $E$ be an elliptic curve given by the short Weierstrass equation

$$E: \quad y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}.$$

We can reduce the coefficients of $E$ modulo a prime $p(\neq 2)$ to get an elliptic curve

$$\overline{E}: \quad y^2 = x^3 + \overline{A}x + \overline{B}, \qquad \overline{A}, \overline{B} \in \mathbb{F}_p.$$

where we require that the discriminant $\overline{D} := 4\overline{A}^3 + 27\overline{B}^2 \neq 0$ in $\mathbb{F}_p$. Keeping this in mind, we say that $E$ has good reduction at $p$ if $p \nmid D := 4A^3 + 27B^2$ and we say that $E$ has bad reduction at $p$ if $p \mid D$. When $p = 2$, we need to work with the more general elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $P = (x, y) \in E(\mathbb{Q})$ be a rational point on an elliptic curve. Let $x = \frac{a}{b} \in \mathbb{Q}$. If $p \nmid b$, then $\bar{b}$ has an inverse in $\mathbb{F}_p$, so we set $\overline{x} := \bar{a}\bar{b}^{-1} \in \mathbb{F}_p$. We define $\overline{y}$ in a similar way. If $p$ divides the denominator of $x$ or $y$, then we can check that $p$ divides the denominators of both $x$ and $y$. In this case, we define $\overline{P} = \overline{\mathcal{O}}$, the point at infinity on $\overline{E}$. We have thus defined a reduction Modulo $p$ map

$$E(\mathbb{Q}) \longmapsto \overline{E}(\mathbb{F}_p), \qquad P \longmapsto \overline{P}.$$

**Theorem 2.1.4.** *If the elliptic curve*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}$$

*has good reduction at $p$, then the reduction modulo $p$ map*

$$E(\mathbb{Q}) \longmapsto \overline{E}(\mathbb{F}_p), \qquad P \longmapsto \overline{P}$$

*is a group homomorphism. Further, if $p$ is odd or else $p = 2$ and $a_1 = 0$, then the restriction of the reduction homomorphism to $E(\mathbb{Q})_{tors}$ is injective.*

## 2.2 Hyperelliptic curves

A hyperelliptic curve $C$ of genus $g$ ($\geq 1$) over a field $K$ is defined by an equation of the form:

$$C : \qquad y^2 + h(x)y = f(x),$$

where $h(x) \in K[x]$ is a polynomial of degree at most $g$ and $f(x) \in K[x]$ is a monic polynomial of degree $2g + 1$. To avoid any singular points, we require that there are no solutions $(x, y) \in \bar{K}^2$ which simultaneously satisfy $y^2 + h(x)y = f(x)$ and the partial derivatives $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$. Note that an elliptic curve is a hyperelliptic curve of genus 1.

Let $C$ be a hyperelliptic curve over $K$ defined by the above equation. We note that,

1. If $h(x) = 0$, then ch $K \neq 2$.

2. If ch $K \neq 2$, then the change of variables $x \to x, y \to (y - h(x)/2)$ transforms $C$ to the form $y^2 = f(x)$ where deg $f = 2g + 1$.

3. Let $C$ be an equation of the form $y^2 = f(x)$. Then $C$ is a hyperelliptic curve if and only if $f(x)$ has no repeated roots in $\bar{K}$.

**Jacobian of an algebraic curve**: Let $C$ be a non-singular algebraic curve. A divisor $D$ is a formal sum of points in $C$ of the form $D := \sum_{P \in C} m_P P$, $m_P \in \mathbb{Z}$ where only a finite number of the $m_P's$ are non-zero. The degree of $D$, denoted by $deg(D)$, is the integer $\sum_{P \in C} m_P$. The set of all divisors, denoted by $\mathcal{D}$, forms an additive group under the addition rule:

$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P.$$

The set of all divisors of degree 0, denoted by $\mathcal{D}^0$, is a subgroup of $\mathcal{D}$.

Let $K(C)$ denote the field of rational functions on $C$ and $f \in K(C)^*$. The divisor of $f$ is defined by div $(f) := \sum_{P \in C} (ord_P f) P$. Note that if $f = g/h$, then div$(f)$ = div$(g)$ - div$(h)$. Since $f$ has a finite number of zeros and poles and since $\sum_{P \in C} (ord_P f) = 0$, we see that the divisor of a rational function is indeed a finite formal sum and has degree 0. A divisor $D \in \mathcal{D}^0$ is called a principal divisor if $D =$ div $(f)$ for some rational function $f \in K(C)^*$. The set of all principal divisors, denoted by $\mathcal{P}$, is a subgroup of $\mathcal{D}^0$. The quotient group $J = \mathcal{D}^0/\mathcal{P}$ is called the Jacobian of the curve $C$ and is denoted by $J(C)(K)$.

The following results [37] plays a useful role in our study of torsion subgroups:

1. When $K$ is a number field, $J(C)(K)$ is a finitely generated abelian group for any non-singular algebraic curve $C$ over $K$.

2. Let $C$ be a hyperelliptic curve over $\mathbb{Q}$ with Jacobian $J$, and let $p$ be a prime of good reduction for $C$. Denote the Jacobian of $\bar{C}$ by $\bar{J}$. Then there is a reduction map

$J(\mathbb{Q}) \to J(\mathbb{F}_p)$ that is actually a group homomorphism. Further, its restriction to $J(\mathbb{Q})_{tors}$ is injective.

3. If we fix a base point $P_0 \in C(\mathbb{Q})$ and denote the induced embedding of $C$ into $J$ by $i : P \to [P - P_0]$, then there is also the embedding $\bar{i} : \bar{C} \to \bar{J}$ that sends $P \to [P - \bar{P_0}]$.

## 2.3 Modular curves and cusps

The following definitions and results are taken from [9].

**Modular group and its congruence subgroups**: The modular group is the group of $2 \times 2$ matrices with integer entries and determinant 1,

$$SL(2,\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

For positive integers $M$ and $N$ with $M|N$, consider the sets

$$\Gamma(M,N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod(N), \quad M|b \right\},$$

$$\Gamma_1(M,N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} mod(N), \quad M|b \right\}.$$

It can be easily checked that $\Gamma(M,N), \Gamma_1(M,N)$ are subgroups of the modular group such that $\Gamma(M,N) \subseteq \Gamma_1(M,N)$. The subgroup $\Gamma(M,N)$ is known as a principal congruence subgroup. When $M = 1$, we denote the subgroup $\Gamma(1,N)$ simply by $\Gamma(N)$. In a similar way, we denote the subgroup $\Gamma_1(1,N)$ simply by $\Gamma_1(N)$. Note that $\Gamma(1) = \Gamma_1(1) = SL(2,\mathbb{Z})$.

A subgroup $\Gamma$ of the modular group is said to be a congruence subgroup of level $N$ if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$. Since $\Gamma_1(M,N) \subseteq \Gamma_1(N) \subseteq \Gamma(N)$ for any $M, N \in \mathbb{N}, M \mid N$, we see that $\Gamma_1(M,N)$ is a congruence subgroup of level $N$ for any $M \mid N$.

**Action of congruence subgroups on** $\mathbb{H}$: Any congruence subgroup $\Gamma$ acts on the upper half plane $\mathbb{H}$ by fractional linear transformations :

$$(\gamma, \tau) \to \gamma(\tau) := \frac{a\tau + b}{c\tau + d}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \tau \in \mathbb{H}.$$

When $\Gamma := \Gamma_1(M, N)$, the set of orbits of this action is denoted by $Y_1(M, N)$ and is called a modular curve of level $N$. We can put appropriate local co-ordinate charts on $Y_1(M, N)$ to obtain a Riemann surface which is unbounded along the positive imaginary axis. Transferring the fundamental domain to the Riemann sphere via stereographic projection gives a triangle with one vertex missing. It turns out that $Y_1(M, N)$ parametrizes isomorphism classes of complex elliptic curves $(E, P_M, P_N)$ with torsion points $P_M$ and $P_N$ of order $M$ and $N$ respectively which generate a subgroup isomorphic to $\mathcal{C}_M \times \mathcal{C}_N$.

**Cusp of modular curves**: The action of a congruence subgroup $\Gamma$ on the upper half plane can be continued to the extended upper half plane $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ by making $\Gamma$ act on the set $\mathbb{Q} \cup \{\infty\}$ by the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix} = \frac{aM + bN}{cM + dN},$$

where this means to take $\infty$ to $\frac{a}{c}$ and $-\frac{d}{c}$ to $\infty$ if $c \neq 0$ and to take $\infty$ to $\infty$ if $c = 0$. The resulting additional orbits are known as the cusps. When $\Gamma = SL(2, \mathbb{Z})$, there is only one cusp, namely the orbit of $\infty$. Indeed, given any rational number $s = \frac{a}{c}$, with $a, c \in \mathbb{Z}$ and $\gcd(a, c) = 1$, we can choose $b, d \in \mathbb{Z}$ such that $ad - bc = 1$ thereby giving $\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\infty) = \frac{a}{c} = s$. For a proper congruence subgroup $\Gamma$, the number of cusps is still finite and is bounded by $[S.L(2, \mathbb{Z}) : \Gamma] \leq [SL(2, \mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} (1 - \frac{1}{p^2})$.

The modular curve obtained adjoining the cusps to the modular curve $Y_1(M, N)$ is denoted by $X_1(M, N)$ and can be identified with a triangle in the Riemann sphere. When $M = 1$, we denote this curve by $X_1(N)$. Since a modular curve has the structure of a compact Riemann surface, it can be interpreted as a non-singular irreducible projective algebraic curve $\mathcal{C}$. Equivalently, the field of rational functions on $\mathcal{C}$ is isomorphic

to the field of meromorphic functions on the modular curve. Hence, the homogeneous polynomials defining $\mathcal{C}$ are often referred to as defining equations of the corresponding modular curve. It turns out that the modular curve $X_1(M,N)$ is always defined over $\mathbb{Q}(\zeta_M)$, where $\zeta_M$ is the $M^{th}$ primitive root of unity.

**Connection between modular curve and elliptic curve**: The uniformization theorem on elliptic curves guarantees that every lattice $\Lambda_\tau, \tau \in \mathbb{H}$ in $\mathbb{R}^2$ gives rise to a complex elliptic curve $\mathbb{C}/\Lambda_\tau$ and conversely every complex elliptic curve arises in this way. The modular curve $Y_1(M,N)$ parametrizes isomorphism classes of complex elliptic curves $(E, P_M, P_N)$ with torsion points $P_M$ and $P_N$ of order $M$ and $N$ respectively which generate a subgroup isomorphic to $\mathcal{C}_M \times \mathcal{C}_N$. Indeed, the map $S_1(M,N) \to Y_1(M,N),\ [\mathbb{C}/\Lambda_\tau, \frac{1}{M}+\Lambda_\tau, \frac{1}{N}+\Lambda_\tau] \to \Gamma_1(M,N)\tau$ gives a one to one correspondence between $S_1(M,N)$, the set of all isomorphism classes of elliptic curves with torsion points of order $M$ and $N$ and $Y_1(M,N)$. As a result, every point on $X_1(M,N)$ which is not a cusp, defines a unique elliptic curve with torsion subgroup isomorphic to $\mathcal{C}_M \times \mathcal{C}_N$.

Nice models for the modular curves $X_1(N)$ and $X_1(2,N)$ that we require can be found in ( [3], [29]). For example, the defining equation for the modular curve $X_1(11)$ is given by

$$X_1(11): \qquad y^2 - y \;=\; x^3 - x, \tag{2.3.1}$$

where the cusps are given by

$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0.$$

Except for the cusps, each solution of (2.3.1) corresponds to a point on $Y_1(11)$, and hence to an isomorphism class of elliptic curves with a torsion point of order 11. Note that the equation (2.3.1) represents an elliptic curve. Similarly the defining equations for the modular curves $X_1(14)$, $X_1(15)$, $X_1(2,10)$ and $X_1(2,12)$ indicate that they are all elliptic curves while the defining equations for the modular curves $X_1(13), X_1(16)$ and $X_1(18)$ indicate that these are hyperelliptic curves.

## 2.4 Some results from algebraic number theory

The following definitions and results are fairly standard and can be found in any introductory texts on algebraic number theory ( [1], [36]).

**The ring of integers in a number field**: A complex number is said to be an algebraic integer if it satisfies some monic polynomial over $\mathbb{Z}$. The set of all algebraic integers in $K$ is denoted by $\mathcal{O}_K$. It is well known that $\mathcal{O}_K$ a Dedekind domain.

Let $K$ be a quadratic number field. Then there exist a unique square-free integer $d$ such that

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

The quadratic field $K = \mathbb{Q}(\sqrt{d})$ is said to be real if $K \subset \mathbb{R}$ and imaginary otherwise. Clearly $K$ is real if $d > 0$ and imaginary if $d < 0$. It is well known that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{if } d \not\equiv 1(\mod 4), \\ \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2}) & \text{if } d \equiv 1(\mod 4). \end{cases}$$

**Structure of the group of units in a number field**: The group of units of a number field $K$ is denoted by $\mathcal{O}_K^\times$. The structure of $\mathcal{O}_K^\times$ is described by the following celebrated theorem of Dirichlet:

**Theorem 2.4.1.** *(Dirichlet's Unit Theorem) The group of units in a number field $K$ is finitely generated of rank $r + s - 1$, where $r$ denotes the number of real embeddings of $K$ and $2s$ denotes the number of non-real complex embeddings.*

When $K = \mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field, the group of units has rank $0 + 1 - 1 = 0$ and hence $\mathcal{O}_K^\times$ is a finite group. When $K$ is a real quadratic field, the group of units has rank $2 + 0 - 1 = 1$. In this case, there always exists a unique unit $\xi_d > 1$ in $\mathcal{O}_K$ such that all units in $K$ are given by $\pm\xi_d^n$ for $n = 0, \pm 1, \pm 2, \ldots$. This unit is called the fundamental unit of $K$.

**Fractional ideals**: Let $D$ be an integral domain and let $K$ be its quotient field. A non-empty subset $\mathcal{F}$ of $K$ satisfying the following three properties:

- $\alpha, \beta \in \mathcal{F} \Rightarrow \alpha + \beta \in \mathcal{F}$.
- $\alpha \in \mathcal{F}, r \in K \Rightarrow r\alpha \in \mathcal{F}$.
- there exists $0 \neq \gamma \in D$ such that $\gamma\mathcal{F} \subseteq D$.

is called a fractional ideal of $D$. The third condition ensures that the elements of a fractional ideal have $\gamma$ as a 'common denominator'. For example,

$$A = \left\{ \frac{n}{25} : n \in \mathbb{Z} \right\}$$

is a fractional ideal of $\mathbb{Z}$ as $A$ is an ideal of $\mathbb{Q}$ such that $25A = \mathbb{Z}$. On the other hand,

$$B = \left\{ \frac{n}{5^m} : n \in \mathbb{Z}, m \in \mathbb{N} \cup \{0\} \right\}$$

is a not a fractional ideal of $\mathbb{Z}$.

**Discriminant of a number field**: Let $w_1, ..., w_n$ be $n$ elements of a number field $K$ of degree $n$. Let $\sigma_k, 1 \leq i \leq n$ denote the $n$ distinct monomorphisms $\sigma_i : K \to \mathbb{C}$. For $i, j = 1, ..., n$ let $w_i^{(j)} := \sigma_j(w_i)$ denote the conjugates of $w_i$ relative to $K$. Then the discriminant of $\{w_1, ..., w_n\}$ is defined by

$$D(w_1, ..., w_n) := \det((w_i^{(j)})).$$

Let $K$ be an algebraic number field of degree $n$. If $\{w_1, ..., w_n\}$ is a set of elements of $\mathcal{O}_K$ such that every element $\alpha \in \mathcal{O}_K$ can be expressed uniquely in the form

$$\alpha = x_1 w_1 + ..... + x_n w_n, \quad x_i \in \mathbb{Z},$$

then $\{w_1, ..., w_n\}$ is called an integral basis of $K$. If $\{w_1, ..., w_n\}$ is any integral basis of $K$, then $D(w_1, ..., w_n)$ is an invariant of the number field $K$ and is called the discriminant of $K$ and is denoted by $d(K)$. When $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, then the discriminant $d(K)$ of $K$ is given by

$$d(K) = \begin{cases} 4d & \text{if } d \not\equiv 1(\text{ mod } 4), \\ d & \text{if } d \equiv 1(\text{ mod } 4). \end{cases}$$

**Class number of a number field**: Let $K$ be an algebraic number field. Let $\mathcal{O}_K$ be the ring of integers of $K$. Then the set of all non-zero fractional ideals of $\mathcal{O}_K$ forms an abelian group $\mathcal{I}(K)$ with respect to multiplication of ideals. Let $\mathcal{P}(K)$ denote the subgroup of principal ideals of $\mathcal{I}(K)$. Then the factor group $\mathcal{I}(K)/\mathcal{P}(K)$ is called the ideal class group of $K$ and is denoted by $\mathcal{H}(K)$. The order of the ideal class group $\mathcal{H}(K)$, which is known to be finite, is called the class number of $K$ and is denoted by $h(K)$. The following results regarding class number are well known:

**Theorem 2.4.2.** *Let $K$ be an algebraic number field. Then*

$$h(K) = 1 \Leftrightarrow \mathcal{O}_K \text{ is a PID } \Leftrightarrow \mathcal{O}_K \text{ is a UFD .}$$

**Theorem 2.4.3.** *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field of odd class number. Then $d$ must be of the form $p$, $2p$ or $pq$ where $p$ and $q$ are primes congruent to 3 modulo 4 [7].*

**Ramification in number fields**: Let $K$ be an algebraic number field. As the ring of integers $\mathcal{O}_K$ is a Dedekind domain, any non-zero ideal can be uniquely factorized into a product of prime ideals. For any rational prime $p$, we have

$$p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} ..... P_k^{e_k},$$

where $P_1, ..., P_k$ are prime ideals of $\mathcal{O}_K$ and $e_i \in \mathbb{N}$. If $e_i > 1$ for some $i \in \{1, 2, ..., k\}$, then $p$ is said to be a ramified prime in $K$. If $e_i = 1$ for all $i = 1, 2, ..., k$, then $p$ is said to be unramified in $K$. The natural number $e_i$ is known as the ramification index of the prime ideal $P_i$.

When $K$ be a quadratic number field, then for any rational prime $p$, there are only three possibilities:

- $p\mathcal{O}_K = P_1 P_2, \quad P_1 \neq P_2, \quad N(P_1) = N(P_2) = p.$
- $p\mathcal{O}_K = P^2, \quad N(P) = p.$
- $p\mathcal{O}_K = P, \quad N(P) = p^2.$

where $P_1, P_2, P$ denote prime ideals of $\mathcal{O}_K$. In the first case, we say that $p$ splits in $K$. In the second case, we say that $p$ ramifies in $K$, while in the last case, we say that $p$ is

inert (or remains prime) in $K$.

**Theorem 2.4.4.** *Let $K$ be an algebraic number field. Then the rational prime $p$ ramifies in $K$ if and only if $p|d(K)$, where $d(K)$ denote the discriminant of $K$.*

**Theorem 2.4.5.** *Let $K$ be a quadratic field. Let $p$ be a rational prime. Then*

- *$p$ splits in $K \iff (\frac{d(K)}{p}) = 1$.*
- *$p$ ramifies in $K \iff (\frac{d(K)}{p}) = 0$.*
- *$p$ is inert in $K \iff (\frac{d(K)}{p}) = -1$.*

*where $d(K)$ is the discriminant of $K$ and $(\frac{d(K)}{p})$ is the Legendre symbol for $p > 2$ and the Kronecker symbol for $p = 2$.*

Note that for a square free integer $d$ with $d \equiv 0, 1(\ mod\ 4)$, the Kronecker symbol is defined by

$$\left(\frac{d}{2}\right) := \begin{cases} 0 & \text{if } d \equiv 0(\ mod\ 4), \\ 1 & \text{if } d \equiv 1(\ mod\ 4), \\ -1 & \text{if } d \equiv 5(\ mod\ 4). \end{cases}$$

# Chapter 3

# Torsion of Elliptic Curves over Quadratic Fields

## 3.1 Introduction

In this chapter, we present our results about torsion of imaginary quadratic fields of class number 1. We also list the torsion subgroups of elliptic curves over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, which have the smallest discriminant among real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1(\bmod 4)$ and $d \equiv 1(\bmod 4)$ respectively.

Henri Poincaré showed that the set $E(K)$ of $K$-rational points on a given elliptic curve $E$ over a given field $K$, together with a specified base point $\mathcal{O}$, forms an abelian group in the projective setting under a geometric chord-tangent law. He further conjectured that the group $E(\mathbb{Q})$ is finitely generated and it was proved in the affirmative in 1922 by Louis Mordell. Later, André Weil generalized this result for abelian varieties over algebraic number fields. Barry Mazur proved the following deep theorem which lists all the possibilities for the torsion subgroup of $E(\mathbb{Q})$.

**Theorem 3.1.1.** *(B. Mazur, [22]) Let $E$ be any elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ must be one of the following 15 groups:*

$$\begin{aligned} &\mathcal{C}_N && 1 \leq N \leq 12, \quad N \neq 11, \\ &\mathcal{C}_N \times \mathcal{C}_{2N} && 1 \leq N \leq 4. \end{aligned}$$

Subsequently, several mathematicians worked on the possible torsion groups that can appear over quadratic extensions of $\mathbb{Q}$, culminating in the following theorem.

**Theorem 3.1.2.** *( Kamienny [17], Kenku-Momose [19] ) Let $E$ be an elliptic curve over a quadratic extension $K$ of $\mathbb{Q}$. Then as $K$ varies, $E(K)_{tors}$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned} &\mathcal{C}_N && 1 \leq N \leq 18, \quad N \neq 17, \\ &\mathcal{C}_2 \times \mathcal{C}_{2N} && 1 \leq N \leq 6, \\ &\mathcal{C}_3 \times \mathcal{C}_{3N} && 1 \leq N \leq 2, \\ &\mathcal{C}_4 \times \mathcal{C}_4. \end{aligned}$$

In 2011, Najman ( [24]) fixed a quadratic extension $K$ of $\mathbb{Q}$ and then looked at the possible torsion structures over $K$. He found all the possible torsion subgroups for the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.

**Theorem 3.1.3.** *(Najman, [24]) Let $E$ be an elliptic curve defined over $\mathbb{Q}(\sqrt{-1})$. Then $E(\mathbb{Q}(\sqrt{-1}))_{tors}$ is either one of the groups from Mazur's theorem or $\mathcal{C}_4 \times \mathcal{C}_4$.*

**Theorem 3.1.4.** *(Najman, [24]) Let $E$ be an elliptic curve defined over $\mathbb{Q}(\sqrt{-3})$. Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is either one of the groups from Mazur's theorem or $\mathcal{C}_3 \times \mathcal{C}_3$ or $\mathcal{C}_3 \times \mathcal{C}_6$.*

In 2012, Kamienny and Najman [18] outlined an approach that can be used to study the possible torsion structure over a quadratic field. In this work, we follow that approach to determine the possible torsion structures over the remaining imaginary quadratic fields of class number 1 and also over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$.

## 3.2 Statement of our main results

When we consider the possibilities for the torsion subgroup of an elliptic curve over an imaginary quadratic field of class number 1, we may not realize all the groups listed in Theorem 3.1.2. This work determines those exceptional groups which can not be realized

as torsion group of elliptic curves over imaginary quadratic fields of class number 1. The main result of our work on torsion of elliptic curves over quadratic fields can be summarized in the following theorems :

**Theorem 3.2.1.** *Let $E$ be an elliptic curve over an imaginary quadratic number field $K$ of class number* 1. *Then as $K$ varies, $E(K)_{tors}$ is isomorphic to one of the groups appearing in Theorem 3.1.2 excluding the groups $\mathcal{C}_{13}, \mathbb{C}_{16}$ and $\mathcal{C}_{18}$ ( [33]).*

**Theorem 3.2.2.** *The torsion subgroups of any elliptic curve over the real quadratic field $\mathbb{Q}(\sqrt{2})$ are the torsion groups appearing in Mazur's theorem together with $\mathcal{C}_{11}$( [32]).*

**Theorem 3.2.3.** *The torsion subgroups of any elliptic curve over the real quadratic field $\mathbb{Q}(\sqrt{5})$ are the torsion groups appearing in Mazur's theorem together with $\mathcal{C}_{15}$( [32]).*

## 3.3 Key steps in our proof

The basic ingredients in our work are the modular curves $Y_1(M, N)$ and $X_1(M, N)$ introduced in the last chapter. We adopt the following steps in determining the torsion subgroup over a quadratic field $K = \mathbb{Q}(\sqrt{d})$ ( [18]).

- If $X_1(M, N)$ is an elliptic curve $E$, then we compute its rank over $K$. In MAGMA, we can compute the rank of any elliptic curve $\mathbb{Q}$ but not over $K$. However, the rank of a rational elliptic curve $E$ over a quadratic field $K = \mathbb{Q}(\sqrt{d})$ can be computed using the relation

$$\text{rank } (E(\mathbb{Q}(\sqrt{d}))) = \text{ rank}(E(\mathbb{Q})) + \text{ rank } (E^{(d)}(\mathbb{Q})),$$

  where $E^{(d)}$ denote the quadratic twist of $E$ (Ex 10.16, [34]).

  If the rank of $E$ over $K$ is positive, then there are infinitely many distinct points on $Y_1(M, N)$ and hence there will be infinitely many non-isomorphic elliptic curves with torsion $\mathcal{C}_M \times \mathcal{C}_N$ over $K$.

If the rank of $E$ over $K$ is zero, we proceed to compute the torsion subgroup of $E(K)$. As in the case of computation of rank, in MAGMA we can compute the torsion subgroup of any elliptic curve $E$ over $\mathbb{Q}$. Having computed the torsion subgroups of the elliptic curves $E$ and its $d$-quadratic twist $E^{(d)}$ over $\mathbb{Q}$, the torsion subgroup of $E$ over $K = \mathbb{Q}(\sqrt{d})$ can be computed using the relation

$$E(K)[N] = E(\mathbb{Q})[N] \times E^{(d)}(\mathbb{Q})[N],$$

when $N$ is odd ( [6]). To compute the even torsion over $K$, we use the division polynomials. Note that if $P = (x, y)$, then the group law of elliptic curve defined by short Weierstrass form ensures that $-P = (x, -y)$. Hence the 2-torsion points are precisely the points obtained by putting $y = 0$ in the short Weierstrass form of the elliptic curve.

Having found the torsion subgroup over $K$, one has to check whether all the torsion points are cusps. If not, then there will be finitely many elliptic curves with torsion subgroup $\mathcal{C}_M \times \mathcal{C}_N$. On the other hand, if all the torsion points are cusps, then $\mathcal{C}_M \times \mathcal{C}_N$ can not appear as a torsion group for any elliptic curve over $K$.

- If $X_1(M, N)$ is hyperelliptic curve, namely $X_1(13)$, $X_1(16)$ or $X_1(18)$ then there are only finitely many $K$-rational points by a celebrated result of Faltings. In order to find all these points, we study the Jacobian of $X_1(M, N)$. Note that the set of $K$-rational points on a hyperelliptic curve does not have any natural group structure like those on an elliptic curve. In MAGMA, like in the case of elliptic curves, we can compute the rank of the Jacobian over $\mathbb{Q}$ only. The rank of the Jacobian over any quadratic field can be found by using the relation (lemma 3 in [23])

$$\text{rank } (J(\mathbb{Q}(\sqrt{d}))) = \text{ rank}(J(\mathbb{Q})) + \text{ rank } (J^{(d)}(\mathbb{Q})),$$

where $J^{(d)}$ denote the quadratic twist of $J$ by $d$.

If the rank of the Jacobian is zero, we find the torsion of the Jacobian and check whether any of the torsion points arise from a $K$-rational point that is not a cusp. If no such point is found, then $\mathcal{C}_M \times \mathcal{C}_N$ can not appear as a torsion group for any elliptic curve over $K$.

If the rank is positive, we can apply Chabauty's method ( if the rank is one ) or other similar methods. However, this case does not arise in our subsequent discussion.

- Having found a $K$-rational point on $Y_1(M, N)$, we can construct ( [29]) elliptic curves with torsion $\mathcal{C}_M \times \mathcal{C}_N$ over $K$.

## 3.4 Torsion over imaginary quadratic fields of class number 1

We first state certain results that are already known and that simplifies our work.

- The groups $\mathcal{C}_3 \times \mathcal{C}_3$ and $\mathcal{C}_3 \times \mathcal{C}_6$ can occur as torsion of elliptic curves over the quadratic field $\mathbb{Q}(\sqrt{-3})$ only ( [19]).
- The group $\mathcal{C}_4 \times \mathcal{C}_4$ can occur as torsion of elliptic curves over the quadratic field $\mathbb{Q}(\sqrt{-1})$ only ( [19]).
- Let $E$ be an elliptic curve over an imaginary quadratic field $K$. Then $E(K)_{tors}$ can not be $\mathcal{C}_{13}$ or $\mathcal{C}_{18}$ ( [4]).

Note that the torsion groups appearing in Mazur's theorem will appear over any number field. So we are left to examine the additional 11 torsion structures mentioned in Theorem 3.1.2 i.e. the groups $\mathcal{C}_{11}, \mathcal{C}_{13}, \mathcal{C}_{14}, \mathcal{C}_{15}, \mathcal{C}_{16}, \mathcal{C}_{18}, \mathcal{C}_2 \times \mathcal{C}_{10}, \mathcal{C}_2 \times \mathcal{C}_{12}, \mathcal{C}_3 \times \mathcal{C}_3, \mathcal{C}_3 \times \mathcal{C}_6$ and $\mathcal{C}_4 \times \mathcal{C}_4$. Using the above results, our study is further reduced to the torsion groups $\mathcal{C}_{11}, \mathcal{C}_{13}, \mathcal{C}_{14}, \mathcal{C}_{15}, \mathcal{C}_2 \times \mathcal{C}_{10}$ and $\mathcal{C}_2 \times \mathcal{C}_{12}$.

We use the version of MAGMA freely available at *www.magma.maths.usyd.edu/calc* for our computations. We prove the main theorem about the torsion over imaginary quadratic fields of class number 1 in a series of lemmas.

**Lemma 3.4.1.** *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathcal{C}_{11}$ *appears as torsion of elliptic curves are* $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-19})$ *and* $\mathbb{Q}(\sqrt{-43})$.

Proof: By [29], elliptic curves with torsion $\mathcal{C}_{11}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation

$$X_1(11): \quad y^2 - y = x^3 - x^2,$$

where the cusps are those points whose $x$-coordinates satisfy the equation

$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0.$$

We see that $X_1(11)$ is an elliptic curve. By a change of variable, the equation for $X_1(11)$ can be reduced to the short Weierstrass form

$$y^2 = x^3 - 432x + 8208.$$

- Consider first the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2})$. In this case, we compute that the rank of $X_1(11)(\mathbb{Q})$ is 0 while the rank of the quadratic twist $X_1(11)^{(-2)}(\mathbb{Q})$ is 1. Therefore,

  $$\text{rank } (X_1(11)(\mathbb{Q}(\sqrt{-2})) = 0 + 1 = 1.$$

  Hence $\mathcal{C}_{11}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}(\sqrt{-2})$. Using the non-torsion point $(2+\sqrt{-2}, -1-2\sqrt{-2})$, we obtain the curve

  $$y^2 + (15 - 8\sqrt{-2})xy + 4(33 + 39\sqrt{-2})y = x^3 + 54(2 + \sqrt{-2})x^2,$$

  which has $(0,0)$ as a point of order 11. In a similar way, we find that the rank of $X_1(11)$ over each of the fields $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-19})$ and $\mathbb{Q}(\sqrt{-43})$ is 1 and hence $\mathcal{C}_{11}$

appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these imaginary quadratic fields of class number 1.

- Next consider the field $K = \mathbb{Q}(\sqrt{-11})$. In this case the rank of $X_1(11)(\mathbb{Q})$ and $X_1(11)^{(-11)}(\mathbb{Q})$ are both 0. Therefore,

$$\text{rank } (X_1(11)(\mathbb{Q}(\sqrt{-11})) = 0 + 0 = 0.$$

We then compute

$$(X_1(11)(\mathbb{Q}))_{tors} \cong \mathcal{C}_5, \qquad (X_1(11)^{(-11)}(\mathbb{Q}))_{tors} \cong \{\mathcal{O}\}.$$

The $N$-torsion of $X_1(11)(\mathbb{Q}(\sqrt{-11}))$ for odd $N$ is determined by the above computation. To compute the 2-torsion, we note that points of order 2 corresponds to $y = 0$ in the short Weierstrass equation $y^2 = f(x)$. In this case, as noted above, $f(x) = x^3 - 432x + 8208$. We find that $f(x)$ is irreducible over $\mathbb{Q}$ and hence over all quadratic extensions of $\mathbb{Q}$. This ensures that $X_1(11)$ does not have 2-torsion over $K = \mathbb{Q}(\sqrt{-11})$. As a result,

$$X_1(11)(\mathbb{Q}(\sqrt{-11})) \cong \mathcal{C}_5 \cong \{\mathcal{O}, (0,0), (0,1), (1,0), (1,1)\}.$$

We see that all these torsion points correspond to $x = 0$ or 1 and hence are cusps of $X_1(11)$. Therefore, $\mathcal{C}_{11}$ can not occur as torsion over the quadratic field $\mathbb{Q}(\sqrt{-11})$. Exactly the same arguments show that $\mathcal{C}_{11}$ can not occur as torsion over the quadratic fields $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$.

**Lemma 3.4.2.** *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathcal{C}_{14}$ *appears as torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$.

Proof: By [29], elliptic curves with torsion $\mathcal{C}_{14}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation

$$X_1(14): \qquad y^2 + xy + y = x^3 - x,$$

where the cusps satisfy

$$x(x-1)(x+1)(x^3-9x^2-x+1)(x^3-2x^2-x+1)=0.$$

We see that $X_1(14)$ is an elliptic curve, which can be reduced to the short Weierstrass form

$$y^2=x^3-675x+13662.$$

- Consider first the imaginary quadratic field $K=\mathbb{Q}(\sqrt{d})$, where $d=-11$, $-43$, $-67$ or $-163$. In each of these cases, we compute that the rank of $X_1(14)(\mathbb{Q})$ is 0 while the rank of $X_1(14)^{(d)}(\mathbb{Q})$ is 1. Therefore,

  $$\text{rank } (X_1(14)(\mathbb{Q}(\sqrt{d}))=0+1=1.$$

  Hence $\mathcal{C}_{14}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$ for $d=-11$, $-43$, $-67$ or $-163$.

- We compute that the rank of $X_1(14)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d=-2$, $-7$ or $-19$. Also, we compute that in each of these cases,

  $$(X_1(14)(\mathbb{Q}))_{tors}\cong\mathcal{C}_6,\qquad (X_1(11)^{(d)}(\mathbb{Q}))_{tors}\cong\mathcal{C}_2$$

  We next note that complete 2-torsion is contained in $X_1(14)(\mathbb{Q}(\sqrt{d}))$ if and only if the 2-division polynomial splits over it. From the short Weierstrass form above, we note that $x^3-675x+13662$ splits only over $\mathbb{Q}(\sqrt{-7})$. This shows that

  $$(X_1(14)(\mathbb{Q}(\sqrt{-7})))_{tors}\cong\mathcal{C}_2\times\mathcal{C}_6,$$

  $$(X_1(14)(\mathbb{Q}(\sqrt{d})))_{tors}\cong\mathcal{C}_6 \text{ for } d=-2,\ -19.$$

  All the points in $\mathcal{C}_6$ correspond to $x=0$ or 1 and hence are cusps. As seen in [18], non-cuspidal torsion points in $X_1(14)(\mathbb{Q}(\sqrt{-7})$ induce the curve

  $$y^2+\frac{63+\sqrt{-7}}{56}xy+\frac{11+\sqrt{-7}}{112}y \;=\; x^3+\frac{11+\sqrt{-7}}{112}x^2,$$

  where $(0,0)$ is a point of order 14. Thus $\mathcal{C}_{14}$ appears as torsion over $\mathbb{Q}(\sqrt{-7})$ for finitely many elliptic curves defined over the field whereas $\mathcal{C}_{14}$ does not appear as torsion over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-19})$.

**Lemma 3.4.3.** *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathcal{C}_{15}$ *appears as torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$

Proof: By [29], elliptic curves with torsion $\mathcal{C}_{15}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation

$$X_1(15): \quad y^2 + xy + y = x^3 + x^2,$$

where the cusps satisfy

$$x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^3 - 6x^2 + 2x + 1) = 0.$$

We see that $X_1(15)$ is an elliptic curve, which can be reduced to the short Weierstrass form

$$y^2 = x^3 - 27x + 8694.$$

- Consider first the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, where $d = -7$, $-11$, $-43$, $-67$ or $-163$. In each of these case, we compute that the rank of $X_1(15)(\mathbb{Q})$ is 0 while the rank of $X_1(15)^{(d)}(\mathbb{Q})$ is 1. Therefore,

  $$\text{rank } (X_1(15)(\mathbb{Q}(\sqrt{d})) = 0 + 1 = 1.$$

  Hence $\mathcal{C}_{15}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$ where $d = -7$, $-11$, $-43$, $-67$ or $-163$.

- We compute that the rank of $X_1(15)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -2$ and $-19$. Also, we compute that in each of these cases that

  $$(X_1(15)(\mathbb{Q}))_{tors} \cong \mathcal{C}_4, \qquad (X_1(11)^{(d)}(\mathbb{Q}))_{tors} \cong \mathcal{C}_2.$$

  From the short Weierstrass form above, we note that $x^3 - 27x + 8694$ split only over $\mathbb{Q}(\sqrt{-15})$. Hence in each case, we obtain

  $$(X_1(15)(\mathbb{Q}(\sqrt{d})))_{tors} \cong \mathcal{C}_4.$$

  Clearly, all these points in $\mathcal{C}_4$ corresponds to $x = 0$ or 1 and hence are cusps. Hence $\mathcal{C}_{15}$ can not appear as torsion over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-19})$.

**Lemma 3.4.4.** *The only imaginary quadratic field of class number* 1 *over which the group* $\mathcal{C}_2 \times \mathcal{C}_{10}$ *appears as torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-11})$ *and* $\mathbb{Q}(\sqrt{-19})$.

Proof: By [29], elliptic curves with torsion $\mathcal{C}_2 \times \mathcal{C}_{10}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation

$$X_1(2,10) : y^2 = x^3 + x^2 - x,$$

where the cusps satisfy

$$x(x^2-1)(x^2+x-1)(x^2-4x-1) = 0.$$

We see that $X_1(2,10)$ is an elliptic curve.

- We compute that the rank of $X_1(2,10)(\mathbb{Q})$ is 0 while the rank of $X_1(15)^{(d)}(\mathbb{Q})$ is 1 for $d = -2, -11$ and $-19$. So, for these values of $d$ the rank of $X_1(2,10)(\mathbb{Q}(\sqrt{d})$ is 1, and hence $\mathcal{C}_2 \times \mathcal{C}_{10}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$.

- We compute that the rank of $X_1(2,10)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -7, -43, -67$ and $-163$. Also, we compute that in each of these cases

  $$(X_1(2,10)(\mathbb{Q}))_{tors} \cong \mathcal{C}_6, \qquad (X_1(2,10)^{(d)}(\mathbb{Q}))_{tors} \cong \mathcal{C}_2$$

  We observe that the polynomial $x^3 + x^2 - x$ splits only over $\mathbb{Q}(\sqrt{5})$. Hence, in each case, we obtain

  $$(X_1(2,10)(\mathbb{Q}(\sqrt{d})))_{tors} \cong \mathcal{C}_6$$

  We find that these points in $\mathcal{C}_6$ corresponds to $x = 0, -1$ or 1 and hence are cusps. Hence $\mathcal{C}_2 \times \mathcal{C}_{10}$ can not appear as torsion over any of these fields.

**Lemma 3.4.5.** *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathcal{C}_2 \times \mathcal{C}_{12}$ *appears as torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$.

Proof: By [29], elliptic curves with torsion $\mathcal{C}_2 \times \mathcal{C}_{12}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation

$$X_1(2,12): \quad y^2 = x^3 - x^2 + x,$$

where the cusps satisfy

$$x(x-1)(2x-1)(2x^2-x+1)(3x^2-3x-1)(6x^2-6x-1) = 0.$$

We see that $X_1(2,12)$ is an elliptic curve.

- We compute that the rank of $X_1(2,12)(\mathbb{Q})$ is 0 while the rank of $X_1(2,12)^{(d)}(\mathbb{Q})$ is 1 for $d = -19$, $-43$, $-67$ or $-163$. Therefore the rank of $X_1(2,12)(\mathbb{Q}(\sqrt{d})$ is 1, and hence $\mathcal{C}_2 \times \mathcal{C}_{12}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$ for $d = -19$, $-43$, $-67$ or $-163$.

- We compute that the rank of $X_1(2,12)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -2$, $-7$ and $-11$. Also, we compute that in each of these cases,

  $$(X_1(2,12)(\mathbb{Q}))_{tors} \cong \mathcal{C}_4, \qquad (X_1(11)^{(d)}(\mathbb{Q}))_{tors} \cong \mathcal{C}_2.$$

  We observe that the polynomial $x^3 - x^2 + x$ split only over $\mathbb{Q}(\sqrt{-3})$. Hence for $d = -2, -7, -11$, we obtain

  $$(X_1(2,12)(\mathbb{Q}(\sqrt{d})))_{tors} \cong \mathcal{C}_4.$$

  These points in $\mathcal{C}_4$ corresponds to $x = 0$ or 1 and hence are cusps of $X_1(2,12)$. Hence $\mathcal{C}_2 \times \mathcal{C}_{12}$ can not appear as torsion over any of these fields.

**Lemma 3.4.6.** *The group $\mathcal{C}_{16}$ can not appear as torsion subgroup of elliptic curves over any imaginary quadratic field of class number* 1.

Proof: By [29], elliptic curves with torsion $\mathcal{C}_{16}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation,

$$X_1(16): y^2 = x(x^2+1)(x^2+2x-1),$$

where the cusps satisfy

$$x(x-1)(x+1)(x^2-2x-1)(x^2+2x-1)=0.$$

We see that $X_1(16)$ is a hyperelliptic curve. As the points of a hyperelliptic curve have no group structure, we make use of the Jacobian of $X_1(16)$. Let $J$ be the Jacobian of $X_1(16)$. For $d \in \{-2,-7,-11,-19,-43,-67,-163\}$, let $X_1(16)^{(d)}$ denote the quadratic twist of $X_1(16)$ by $d$. Let $J^{(d)}$ be the Jacobian of $X_1(16)^{(d)}$. We compute that rank $(J(\mathbb{Q}))=0$ and rank $(J^{(d)}(\mathbb{Q}))=0$. Thus we obtain, as in lemma 3 of ( [23]),

$$\text{rank } (J(Q(\sqrt{d}))) = \text{ rank } (J(Q) + \text{ rank } (J^{(d)}(Q)) = 0+0=0$$

for each $d \in \{-2,-7,-11,-19,-43,-67,-163\}$. We next compute that

$$(J_1(\mathbb{Q}))_{tors} = \mathcal{C}_2 \times \mathcal{C}_{10}.$$

The discriminant of the $X_1(16)$ is $-2^{19}$, so 2 is the only rational prime with bad reduction. Since 3 splits in $Q(\sqrt{-2})$, so the prime-to-3 part of $(J(Q(\sqrt{-2})))_{tors}$ injects into $J(\mathbb{F}_3)$ and since the rational prime 5 remains inert in $Q(\sqrt{-2})$, so the prime-to-5-part of $(J(Q(\sqrt{-2})))_{tors}$ injects into $J(\mathbb{F}_{5^2})$. Since $|J(\mathbb{F}_3)|=20$ and $|J(\mathbb{F}_{5^2})|=40$, we see that

$$|(J(Q(\sqrt{-2})))_{tors}| \leq 20.$$

Hence it follows that

$$(J_1(\mathbb{Q}(\sqrt{-2})))_{tors} = (J_1(\mathbb{Q}))_{tors} = \mathcal{C}_2 \times \mathcal{C}_{10}.$$

Similar arguments with different primes of good reduction leads to

$$(J_1(\mathbb{Q}(\sqrt{d})))_{tors} = (J_1(\mathbb{Q}))_{tors} = \mathcal{C}_2 \times \mathcal{C}_{10}$$

for each $d \in \{-7,-11,-19,-43,-67,-163\}$. In MAGMA, we check that all these torsion points are induced by the cusps of $X_1(16)$. As a result, $\mathcal{C}_{16}$ can not appear as torsion of elliptic curves over any of these fields.

The Theorem 2.1 now follows from Lemmas 5.1 to 5.6 together with Theorems 1.3 and 1.4. The results in this section have been accepted for publication in [33].

## 3.5 Torsion over real quadratic fields of smallest discriminant

In this case, we need to examine the groups $\mathcal{C}_{13}$ and $\mathcal{C}_{18}$ too in addition to the groups in the previous section. Since our method in this section are similar, we omit some details in this section.

**The torsion $\mathcal{C}_{11}$**: First, consider $K = \mathbb{Q}(\sqrt{2})$. In this case, we compute in MAGMA that rank of $X_1(11)(\mathbb{Q}(\sqrt{2}))$ is 1. Therefore, $\mathcal{C}_{11}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}(\sqrt{2})$. Using the non-torsion point $(\frac{1}{2}, \frac{1}{4}(2+\sqrt{2})$, we obtain explicitly the curve

$$y^2 + \frac{1}{8}(3-\sqrt{2})xy + \frac{1}{128}\sqrt{2}y = x^3 + \frac{1}{64}\sqrt{2}x^2$$

where $(0,0)$ is a point of order 11.

Next consider $K = \mathbb{Q}(\sqrt{5})$. In this case the rank of $X_1(11)(\mathbb{Q}(\sqrt{5}))$ is 0 and the torsion group is $\mathbb{Z}_5$. Following ( [18]), we note that

$$X_1(11)(\mathbb{Q}(\sqrt{5})) = \{\mathcal{O}, (0,0), (0,1), (1,0), (1,1)\}$$

We see that all the torsion points corresponds to $x = 0$ or $x = 1$, and hence they are cusps. Therefore, $\mathcal{C}_{11}$ cannot occur as a torsion over the quadratic field $\mathbb{Q}(\sqrt{5})$.

**The torsion $\mathcal{C}_{13}$**: Elliptic curves with torsion $\mathcal{C}_{13}$ over a quadratic field $K$ are induced by solutions over $K$ of the equation ( [29]),

$$X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

where the cusps satisfy

$$x(x-1)(x^3 - 4x^2 + x + 1) = 0.$$

We see that $X_1(13)$ is a hyperelliptic curve. We find via 2-descent, that

$$\text{rank } (J_1(13)(\mathbb{Q}(\sqrt{d}))) = 0 \text{ for } d = 2, 5.$$

Further, we compute that

$$(J_1(13)(\mathbb{Q}(\sqrt{d})))_{tors} \cong \mathcal{C}_{21}$$

for these two values of $d$. All these points on $\mathcal{C}_{21}$ are generated by the cusps of $X_1(13)$. Hence $\mathcal{C}_{13}$ cannot occur as a torsion over these quadratic fields.

**The torsion $\mathcal{C}_{14}$**: The rank of $X_1(14)(K)$ is 0 for $K = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$. Also, $X_1(14)(K_{tors} \cong \mathcal{C}_6$ in both the cases. Since the points in $\mathcal{C}_6$ corresponds to $x = 0, 1$ or $-1$, all the torsion points are cusps. As a result, $\mathcal{C}_{14}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$.

**The torsion $\mathcal{C}_{15}$**: The rank of $X_1(15)$ over $\mathbb{Q}(\sqrt{2})$ is 0 and the torsion subgroup is $\mathcal{C}_4$. All the torsion point correspond to cusps, and hence $\mathcal{C}_{15}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$.

Next, the rank of $X_1(15)$ over $\mathbb{Q}(\sqrt{5})$ is 0 and the torsion subgroup is $\mathcal{C}_8$. From a non-cuspidal point on it, one can obtain an elliptic curve ( [18])

$$y^2 = x^3 + (281880\sqrt{5} - 630315)xy + 328392630 - 146861640\sqrt{5},$$

with a point $(264\sqrt{5} - 585, 5076\sqrt{5} - 11340)$ of order 15.

**The torsion $\mathcal{C}_{16}$**: Proceeding as in the case of $X_1(13)$, we compute that for $d = 2, 5$ rank $(J_1(16)(\mathbb{Q}(\sqrt{d}))) = 0$ and

$$(J_1(16)(\mathbb{Q}(\sqrt{2})))_{tors} = \mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_{10},$$
$$(J_1(16)(\mathbb{Q}(\sqrt{5})))_{tors} = \mathcal{C}_2 \times \mathcal{C}_{10}.$$

Since all these torsion points are induced by the cusps of $X_1(16)$, so $\mathcal{C}_{16}$ can not appear as torsion over these two fields.

**The torsion $\mathcal{C}_{18}$**: Elliptic curves with torsion $\mathcal{C}_{18}$ over a quadratic field $K$ are induced

by solutions over $K$ of the equation ( [29]),

$$X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

where the cusps satisfy

$$x(x+1)(x^2+x+1)(x^2-3x-1) = 0.$$

We see that $X_1(18)$ is a hyperelliptic curve. Since the prime 3 remains prime in $\mathbb{Q}(\sqrt{2})$, so by Proposition 2.4$(i)$ in [19], we see that $\mathcal{C}_{18}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$. On the other hand, as 5 ramifies in $\mathbb{Q}(\sqrt{5})$, so by Proposition 2.4$(iii)$ in [19], we see that $\mathcal{C}_{18}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{5})$.

**The torsion $\mathcal{C}_2 \times \mathcal{C}_{10}$**: The rank of $X_1(2,10)$ over $\mathbb{Q}(\sqrt{2})$ is 0 and the torsion subgroup is $\mathcal{C}_6$. We easily verify that all the torsion points correspond to cusps and hence $\mathcal{C}_2 \times \mathcal{C}_{10}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$.

The rank of the curve over the quadratic fields $\mathbb{Q}(\sqrt{5})$ is 0 and the torsion subgroup is $\mathcal{C}_2 \times \mathcal{C}_6$. All the torsion points correspond to cusps and hence $\mathcal{C}_2 \times \mathcal{C}_{10}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{5})$.

**The torsion $\mathcal{C}_2 \times \mathcal{C}_{12}$**: The rank of $X_1(2,12)$ over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are 0 and the torsion subgroup is $\mathcal{C}_4$. All the torsion points correspond to cusps, and hence $\mathcal{C}_2 \times \mathcal{C}_{12}$ can not appear as torsion over these quadratic fields.

Combining the results in this section, we obtain Theorem 2.2 and Theorem 2.3. The results in this section have been accepted for publication in [32].

# Chapter 4

# Fundamental Unit of Real Quadratic Fields of Odd Class Number

## 4.1 Introduction

In this chapter, we prove certain arithmetic properties of the fundamental unit of a real quadratic field of odd class number. It is well known by Dirichlet's theorem that the group of units in the ring of integers of a real quadratic field is of rank one, and the smallest unit $> 1$ is referred to as the fundamental unit. We consider a real quadratic field $k = \mathbb{Q}(\sqrt{d})$ of odd class number. It is well-known [7] that $d$ has to be of the form $p$, $2p$ or $pq$ where $p$ and $q$ are primes congruent to 3 modulo 4. The fundamental unit of a real quadratic field has been extensively studied, but there are still several interesting questions that remain unanswered. There is a famous conjecture by Ankeny, Artin and Chowla in ( [2]) concerning the fundamental unit $\frac{t_p+u_p\sqrt{p}}{2}$ of $\mathbb{Q}(\sqrt{p})$ where $p$ is a prime congruent to 1 modulo 4. A similar conjecture was made by Mordell concerning the fundamental unit of of $\mathbb{Q}(\sqrt{p})$ where $p$ is a prime congruent to 3 modulo 4. Let $\xi_d = x + y\sqrt{d}$ be the fundamental unit of $k$. The following results concerning $x$ and $y$ were first proved in [41].

**Theorem 4.1.1.** *Let $\xi_d = x + y\sqrt{d} > 1$ be the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$ of odd class number. Then*

1. *If* $d = p$ *with* $p \equiv 3 \mod 4$, *then* $x \equiv 0 \mod 2$. *More precisely, if* $p \equiv 3 \mod 8$, *then* $x \equiv 2 \mod 4$ *and if* $p \equiv 7 \mod 8$ *then* $x \equiv 0 \mod 4$.

2. *If* $d = 2p$ *with* $p \equiv 3 \mod 4$, *then* $y \equiv 0 \mod 2$ *and* $x + y \equiv 3 \mod 4$.

3. *If* $d = pq$ *with* $p \equiv q \equiv 3 \mod 4$, *then* $x \equiv 3 \mod 4$ *and* $y \equiv 0 \mod 4$.

Note that when $d = pq \equiv 5 \mod 8$, $\xi_d^3$ is contained in $\mathbb{Z}[\sqrt{d}]$ though $\xi_d$ may not belong to $\mathbb{Z}[\sqrt{d}]$. Hence in the third part of the above theorem, the congruences are satisfied by $x$ and $y$ where $x + y\sqrt{d} = \xi_d^3$ when $pq \equiv 5 \mod 8$.

In 2016, Chakraborty and Saikia ( [5]) obtained the above congruences by considering ramification of primes in quadratic fields. In this chapter, we prove certain stronger congruence relations and arithmetic properties for $x$ and $y$ as stated below.

**Theorem 4.1.2.** *Let* $p$ *be a prime congruent to* 7 *modulo* 8, *and* $\xi_p = x + y\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ *be the fundamental unit of* $k = \mathbb{Q}(\sqrt{p})$. *Then*

$(i)$ $x \equiv 0 \mod 8$.

$(ii)$ $x + 1$ *is the square of an odd integer.*

$(iii)$ $x - 1$ *is divisible by* $p$ *and* $\frac{x-1}{p}$ *is the square of an odd integer.*

**Theorem 4.1.3.** *Let* $p$ *be a prime congruent to* 3 *modulo* 8, *and* $\xi_p = x + y\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ *be the fundamental unit of* $k = \mathbb{Q}(\sqrt{p})$. *Then*

$(i)$ $x \equiv 2 \mod 8$.

$(ii)$ $x - 1$ *is the square of an odd integer.*

$(iii)$ $x + 1$ *is divisible by* $p$ *and* $\frac{x+1}{p}$ *is the square of an odd integer.*

**Theorem 4.1.4.** *Let* $p$ *be a prime congruent to* 7 *modulo* 8, *and* $\xi_{2p} = x + y\sqrt{2p} \in \mathbb{Z}[\sqrt{2p}]$ *be the fundamental unit of* $k = \mathbb{Q}(\sqrt{2p})$. *Then*

$(i)$ $y \equiv 0 \mod 4$.

$(ii)$ $x + 1$ *is the square of a multiple of* 4.

$(iii)$ $x - 1$ *is divisible by* $2p$ *and* $\frac{x-1}{2p}$ *is the square of an odd integer.*

**Theorem 4.1.5.** *Let* $p$ *be a prime congruent to* 3 *modulo* 8, *and* $\xi_p = x + y\sqrt{2p} \in \mathbb{Z}[\sqrt{2p}]$ *be the fundamental unit of* $k = \mathbb{Q}(\sqrt{2p})$. *Then*

$(i)$ $y \equiv 2 \mod 4$.

*(ii)* $x-1$ *is the square of an integer of the form* $4k+2$.

*(iii)* $x+1$ *is divisible by* $2p$ *and* $\frac{x+1}{2p}$ *is the square of an odd integer.*

**Theorem 4.1.6.** *Let* $p$ *and* $q$ *be two distinct primes congruent to* 3 *modulo* 4, *and* $x+y\sqrt{pq} \in \mathbb{Z}[\sqrt{pq}]$ *be the fundamental unit* $\xi_{pq}$ *of* $k=\mathbb{Q}(\sqrt{pq})$ *(or its cube when* $pq \equiv 5$ *mod* 8*). Without loss of generality, suppose* $\left(\frac{p}{q}\right)=1$, *i.e.,* $p$ *is a quadratic residue mod* $q$. *Then*

*(i)* $x \equiv 7$ *mod* 8, *and* $y \equiv 0$ *mod* 4.

*(ii)* $x-1$ *is divisible by* $2q$ *and* $\frac{x-1}{2q}$ *is the square of an odd integer.*

*(iii)* $x+1$ *is divisible by* $2p$ *and* $\frac{x+1}{2p}$ *is the square of an even integer.*

The case $\left(\frac{p}{q}\right)=-1$ follows by interchanging the roles of $p$ and $q$, as by quadratic reciprocity, $\left(\frac{p}{q}\right)=-1 \Leftrightarrow \left(\frac{q}{p}\right)=1$ when $p \equiv 3 \equiv q \bmod 4$.

The proofs crucially use the fact that the ramified primes in the quadratic extension must be principal as the class number is odd. In the next section we prove a few preliminary lemmas that we need for proving the theorems stated above.

## 4.2 Preliminary lemmas

Consider the fundamental unit $\xi_d$ of the field $k=\mathbb{Q}(\sqrt{d})$ of odd class number. Let $\mathcal{O}_k$ denote the ring of integers of $k$. When $d=p$ or $d=2p$ with $p \equiv 3 \bmod 4$, we have $\mathcal{O}_k=\mathbb{Z}[\sqrt{d}]$. When $d=pq$ with $p \equiv 3 \equiv q \bmod 4$, we know that $\mathcal{O}_k=\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{\alpha+\beta\sqrt{d} \mid 2\alpha,\ 2\beta \in \mathbb{Z},\ 2\alpha \equiv 2\beta \bmod 2\}$.

We use the following lemma (Lemma 3.1 in [5]).

**Lemma 4.2.1.** *If* $l \neq p$ *is a rational prime that ramifies in* $k/\mathbb{Q}$, *then* $lx=a^2+db^2$ *and* $ly=2ab$ *for some relatively prime integers* $a$ *and* $b$.

As the lemma is crucial for our arguments, and the proof is short, we provide it here. Let $\mathfrak{l}$ be the prime above $l$ in $k$. Then, $l\mathcal{O}_k=\mathfrak{l}^2$. Therefore, the class of $\mathfrak{l}$ has order dividing 2. As the class number of $k$ is odd, $\mathfrak{l}$ has to be a principal ideal. Therefore, there exist integers $a,b$ such that $l\xi_p^j=(a+b\sqrt{d})^2$ when $d=p$ or $d=2p$. Note that

$j$ has to be odd, hence we can take $j = 1$ by absorbing the even powers on the right hand side. As $\xi_d$ is a unit, $a$ and $b$ have to be co-prime. When $d = pq \equiv 1 \bmod 8$ with $p \equiv 3 \equiv q \bmod 4$, $\xi_d$ still belongs to $\mathbb{Z}[\sqrt{d}]$ even though the ring of integers of $\mathbb{Q}(\sqrt{d})$ is larger than $\mathbb{Z}[\sqrt{d}]$ and we still have $l\xi_p = (a + b\sqrt{d})^2$ with $a, b \in \mathbb{Z}$. When $d = pq \equiv 5 \bmod 8$ with $p \equiv 3 \equiv q \bmod 4$, $\xi_d$ may not belong to $\mathbb{Z}[\sqrt{d}]$ but $\xi_d^3$ does. Therefore, we can conclude from $l\mathcal{O}_k = \mathfrak{l}^2$ that $l\xi_d^3 = (a + b\sqrt{d})^2$ for some relatively prime integers $a$ and $b$.

Next we observe that the norm of $\xi_d$ has to be $+1$, i.e.,

$$N_{k/\mathbb{Q}}(\xi_d) = x^2 - dy^2 = 1. \tag{4.2.1}$$

The above observation follows from the fact that $d$ is divisible by a prime $p \equiv 3 \bmod 4$, and $-1$ can not be a quadratic residue for such a prime $p$. The above observation leads to the following additional information about $a$ and $b$ in Lemma 4.2.1. We first consider $d = p$ or $2p$ where $p$ is a prime congruent to 3 mod 4. The rational prime 2 ramifies in $k/\mathbb{Q}$, and we have $x = \frac{a^2+db^2}{2}$ and $y = ab$ for a pair of co-prime integers $a$ and $b$.

**Lemma 4.2.2.** *(i) When $p \equiv 7$ mod 8 and $d = p$ or $2p$, we have $a^2 - db^2 = 2$.*
*(ii) When $p \equiv 3$ mod 8 and $d = p$ or $2p$, we have $a^2 - db^2 = -2$.*

Proof: Using Lemma 4.2.1 in equation (4.2.1), we have $(\frac{a^2+db^2}{2})^2 - da^2b^2 = 1$, which implies $a^2 - db^2 = \pm 2$. When $p \equiv 7 \bmod 8$, $-2$ is not a quadratic residue of $p$ and hence $a^2 - db^2 \neq -2$. When $p \equiv 3 \bmod 8$, 2 is not a quadratic residue of $p$ and hence $a^2 - db^2 \neq 2$.

Now we consider the case $d = pq$ where $p \equiv q \equiv 3 \bmod 4$. As the prime $p$ ramifies in $\mathbb{Q}(\sqrt{pq})$, we have $x = \frac{a^2+pqb^2}{p}$ and $y = \frac{2ab}{p}$ by Lemma 4.2.1. We can extract the following additional information about $a$ and $b$.

**Lemma 4.2.3.** *(i) When $\left(\frac{p}{q}\right) = 1$, we have $a^2 - pqb^2 = p$.*
*(ii) When $\left(\frac{p}{q}\right) = -1$, we have $a^2 - pqb^2 = -p$.*

Proof: By (5.2.2), we have $(\frac{a^2+pqb^2}{p})^2 - pq(\frac{2ab}{p})^2 = 1$, which implies $a^2 - pqb^2 = \pm p$. When $\left(\frac{p}{q}\right) = 1$, we have $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right) = -1$, hence $a^2 - db^2 \neq -p$. When $\left(\frac{p}{q}\right) = -1$, we have $\left(\frac{p}{q}\right) = -1$, hence $a^2 - db^2 \neq p$.

## 4.3 Proof of the theorems

We now prove our results using the lemmas of the previous section.

Proof of Theorem 4.1.2: Consider the fundamental unit $\xi_p = x + y\sqrt{p}$ where $p \equiv 7 \bmod 8$. By Lemmas 4.2.1 and 4.2.2, we have

$$2x = a^2 + pb^2, \;\; 2 = a^2 - pb^2 \;\; \Rightarrow \;\; x + 1 = a^2, \;\; x - 1 = pb^2. \tag{4.3.1}$$

By above, $a$ and $b$ must have same parity. As they are co-prime, both $a$ and $b$ are odd. In particular, $x = a^2 - 1 \equiv 0 \bmod 8$. Further, $x + 1$ and $\frac{x-1}{p}$ are squares of odd integers and the Theorem 4.1.2 follows.

Proof of Theorem 4.1.3: Consider the fundamental unit $\xi_p = x + y\sqrt{p}$ where $p \equiv 3 \bmod 8$. By Lemmas 4.2.1 and 4.2.2, we have

$$2x = a^2 + pb^2, \;\; -2 = a^2 - pb^2 \;\; \Rightarrow \;\; x - 1 = a^2, \;\; x + 1 = pb^2. \tag{4.3.2}$$

As above, $a$ and $b$ must both be odd. In particular, $x = a^2 + 1 \equiv 2 \bmod 8$. Further, $x - 1$ and $\frac{x+1}{p}$ are squares of odd integers and the Theorem 4.1.3 follows.

Proof of Theorem 4.1.4: Consider the fundamental unit $\xi_{2p} = x + y\sqrt{2p}$ where $p \equiv 7 \bmod 4$. By Lemmas 4.2.1 and 4.2.2, we have

$$2x = a^2 + 2pb^2, \;\; y = ab, \;\; 2 = a^2 - 2pb^2 \;\; \Rightarrow \;\; x + 1 = a^2, \;\; x - 1 = 2pb^2. \tag{4.3.3}$$

By above, $a$ must be even and hence $b$ must be odd. In particular, $x \equiv 3 \bmod 4$ and $y \equiv 0 \bmod 2$. Further, $\frac{x-1}{2p}$ is a square of an odd integer, and $x + 1$ is a square of an even number $a$. Considering $2x = a^2 + 2pb^2$ modulo 8 and observing that $p \equiv 7 \bmod 8$, $b^2 \equiv 1 \bmod 8$, we obtain $a^2 \equiv 2(x - 1pb^2) \equiv 0 \bmod 8$. Therefore, $a \equiv 0 \bmod 4$. Thus $y \equiv 0 \bmod 4$ and the theorem follows.

Proof of Theorem 4.1.5: Consider the fundamental unit $\xi_{2p} = x + y\sqrt{2p}$ where $p \equiv 3$ mod 8. By Lemmas 4.2.1 and 4.2.2, we have

$$2x = a^2 + 2pb^2, \;\; y = ab, \;\; -2 = a^2 - 2pb^2 \;\; \Rightarrow \;\; x - 1 = a^2, \;\; x + 1 = 2pb^2. \tag{4.3.4}$$

As above, $a$ must be even and hence $b$ must be odd. Hence $y \equiv 0$ mod 2, and $x \equiv 1$ mod 4. Further, $\frac{x+1}{2p}$ is the square of an odd integer, and $x - 1$ is the square of an even integer $a$. Considering $2x = a^2 + 2pb^2$ modulo 8 and observing that $p \equiv 3$ mod 8, $b^2 \equiv 1$ mod 8, we obtain $a^2 \equiv 2x - 2p \equiv 4$ mod 8. Therefore $a \equiv 2$ mod 4, and $y \equiv 2$ mod 4. The Theorem 4.1.5 follows.

Proof of Theorem 4.1.6: Consider the fundamental unit $\xi_{pq} = x + y\sqrt{pq}$ where $p$ and $q$ are primes congruent to 3 mod 4. By Lemmas 4.2.1 and 4.2.3, we have

$$\begin{aligned} & px = a^2 + pqb^2, \;\; py = 2ab, \;\; p = a^2 - pqb^2 \\ \Rightarrow \;\; & p(x+1) = 2a^2, \;\; x - 1 = 2qb^2. \end{aligned} \tag{4.3.5}$$

Considering $p = a^2 - pqb^2$ mod 4, we find that $a$ is even and $b$ is odd. In particular, $y \equiv 0$ mod 4. As $x - 1 = 2qb^2 \equiv 6$ mod 8, we have $x \equiv 7$ mod 8. Clearly, $x - 1$ is divisible by $2q$ and $\frac{x-1}{2q}$ is the square of an odd integer. Moreover, $x + 1$ is divisible by $2p$ and $\frac{x+1}{2p}$ is the square of an even integer. The Theorem 4.1.6 follows.

## 4.4 Examples

We now provide a few examples that illustrate our results. The computations have been carried out in SAGE ( [35]).

Examples for Theorem 4.1.2:

Table 4.1: $d = p$, where $p \equiv 7 \bmod 8$ is a prime

| $d = p$ | $\xi_p = x + y\sqrt{p}$ | $x \bmod 8$ | $x + 1$ | $x - 1$ |
|---|---|---|---|---|
| 7 | $8 + 3\sqrt{7}$ | 0 | $3^2$ | $7.1^2$ |
| 23 | $24 + 5\sqrt{7}$ | 0 | $5^2$ | $23.1^2$ |
| 31 | $1520 + 273\sqrt{7}$ | 0 | $69^2$ | $31.7^2$ |
| 47 | $48 + 7\sqrt{47}$ | 0 | $7^2$ | $47.1^2$ |
| 71 | $3480 + 413\sqrt{71}$ | 0 | $59^2$ | $71.7^2$ |
| 79 | $80 + 9\sqrt{79}$ | 0 | $9^2$ | $79.1^2$ |

Examples for Theorem 4.1.3:

Table 4.2: $d = p$, where $p \equiv 3 \bmod 8$ is a prime

| $d = p$ | $\xi_p = x + y\sqrt{p}$ | $x \bmod 8$ | $x - 1$ | $x + 1$ |
|---|---|---|---|---|
| 3 | $2 + \sqrt{3}$ | 2 | $1^2$ | $3.1^2$ |
| 11 | $10 + 3\sqrt{11}$ | 2 | $3^2$ | $11.1^2$ |
| 19 | $170 + 39\sqrt{7}$ | 2 | $13^2$ | $19.3^2$ |
| 43 | $3482 + 531\sqrt{43}$ | 2 | $59^2$ | $43.9^2$ |
| 59 | $530 + 69\sqrt{59}$ | 2 | $23^2$ | $59.3^2$ |
| 67 | $48842 + 5967\sqrt{67}$ | 2 | $221^2$ | $67.27^2$ |
| 83 | $82 + 9\sqrt{83}$ | 2 | $9^2$ | $83.1^2$ |

Examples for Theorem 4.1.4:

Table 4.3: $d = 2p$, where $p \equiv 7 \bmod 8$ is a prime

| $d = 2p$ | $\xi_p = x + y\sqrt{2p}$ | $y \bmod 4$ | $x + 1$ | $x - 1$ |
|---|---|---|---|---|
| 2.7 | $15 + 4\sqrt{14}$ | 0 | $(4.1)^2$ | $2.7.1^2$ |
| 2.23 | $24335 + 3588\sqrt{7}$ | 0 | $(4.39)^2$ | $2.23.23^2$ |
| 2.31 | $63 + 8\sqrt{62}$ | 0 | $(4.2)^2$ | $2.31.1^2$ |
| 2.47 | $2143295 + 221064\sqrt{94}$ | 0 | $(4.366)^2$ | $2.47.151^2$ |
| 2.71 | $143 + 12\sqrt{142}$ | 0 | $(4.3)^2$ | $2.71.1^2$ |
| 2.79 | $7743 + 616\sqrt{158}$ | 0 | $(4.22)^2$ | $2.79.7^2$ |

Examples for Theorem 4.1.5:

Table 4.4: $d = 2p$, where $p \equiv 3 \bmod 8$ is a prime

| $d = 2p$ | $\xi_p = x + y\sqrt{2p}$ | $y \bmod 4$ | $x - 1$ | $x + 1$ |
|---|---|---|---|---|
| 2.3 | $5 + 2\sqrt{6}$ | 2 | $2^2$ | $2.3.1^2$ |
| 2.11 | $197 + 42\sqrt{22}$ | 2 | $14^2$ | $2.11.3^2$ |
| 2.19 | $37 + 6\sqrt{38}$ | 2 | $6^2$ | $2.19.1^2$ |
| 2.43 | $10405 + 1122\sqrt{86}$ | 2 | $102^2$ | $2.43.11^2$ |
| 2.59 | $306917 + 28254\sqrt{118}$ | 2 | $554^2$ | $2.59.51^2$ |
| 2.67 | $145925 + 12606\sqrt{134}$ | 2 | $382^2$ | $2.67.33^2$ |

Examples for Theorem 4.1.6:

Table 4.5: $d = pq$, where $p \equiv 3 \equiv q \bmod 4$ are primes and $(\frac{p}{q}) = 1$

| $pq \equiv 1 \bmod 8$ | $\xi_p = x + y\sqrt{pq}$ | $x \bmod 8$ | $y \bmod 4$ | $x-1$ | $x+1$ |
|---|---|---|---|---|---|
| 3.11 | $23 + 4\sqrt{33}$ | 7 | 0 | $2.11.1^2$ | $2.3.2^2$ |
| 11.19 | $46551 + 3220\sqrt{209}$ | 7 | 0 | $2.19.35^2$ | $2.11.46^2$ |
| 31.23 | $5286367 + 197976\sqrt{713}$ | 7 | 0 | $2.23.339^2$ | $2.31.292^2$ |
| $pq \equiv 5 \bmod 8$ | $\xi_p^3 = x + y\sqrt{pq}$ | $x \bmod 8$ | $y \bmod 4$ | $x-1$ | $x+1$ |
| 7.3 | $55 + 12\sqrt{21}$ | 7 | 0 | $2.3.3^2$ | $2.7.2^2$ |
| 11.7 | $351 + 40\sqrt{77}$ | 7 | 0 | $2.7.5^2$ | $2.11.4^2$ |
| 23.11 | $3222617399 + 202604220\sqrt{253}$ | 7 | 0 | $2.11.12103^2$ | $2.23.8370^2$ |

# Chapter 5

# Fundamental Unit of Totally Imaginary Biquadratic Fields of Odd Class Number

## 5.1 Introduction

In this chapter, we examine the fundamental unit in a totally imaginary biquadratic field $K$ of odd class number. In the last chapter, we derived certain congruence relations for the fundamental unit of real quadratic fields of odd class number. By considering the maximal real subfield $k$ of $K$, we determine congruence properties for the fundamental unit of $K$ by using the congruence properties of the fundamental unit of $k$ (developed in the last chapter).

Let $K = \mathbb{Q}(\sqrt{-d_1}, \sqrt{-d_2})$ be a totally imaginary biquadratic field. It is well known by Dirichlet's theorem that the units in the ring of integers of $K$ form an abelian group $\mathcal{O}_K^\times$ of rank one. Let $W_K$ denote the group consisting of the roots of unity in $K$. By Dirichlet's unit theorem, we can write

$$\mathcal{O}_K^\times = W_K \times \xi^{\mathbb{Z}},$$

where $\xi$ is a generator of the infinite cyclic subgroup of $\mathcal{O}_K^\times$. Clearly, $\zeta\xi^{\pm 1}$ can also be taken as a generator for any $\zeta \in W_K$. For simplicity, we assume that $W_K = \{\pm 1\}$.

Then we have four choices for the generator of the infinite subgroup $\mathcal{O}_K^\times$, namely $\pm\xi^{\pm 1}$. We refer to a generator of absolute value $> 1$ as fundamental unit of $K$ and denote it by $\xi_K$ henceforth. The maximal real subfield of $K$ is given by $k = \mathbb{Q}(\sqrt{d_1 d_2})$. The group $\mathcal{O}_k^\times$ of units in $k$ is of rank 1 as well, and the smallest unit $\xi_k > 1$ is referred to as the fundamental unit of $k$. The relation between the fundamental unit and the class number of a real quadratic field has also been closely examined, for example, in [40] and [41]. Congruence properties of the fundamental units of certain classes of totally real biquadratic fields have been proved in [20].

In this chapter, we examine the fundamental unit of totally imaginary biquadratic field $K$ of odd class number. If $K$ is a totally imaginary biquadratic field of odd class number with $W_K = \{\pm 1\}$, then either $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ or $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ where $p$, $q$ are primes congruent to 3 modulo 4 (theorem 20.3 in [7]). As shown in [39], the ring of integers of $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ is given by

$$\mathcal{O}_K = \left\{ \frac{x_1 + x_2\sqrt{-p} + x_3\sqrt{-q} + x_4\sqrt{pq}}{4} \;\middle|\; x_i \in \mathbb{Z} \right\} \tag{5.1.1}$$

where $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \bmod 2$, and $x_1 - x_2 + x_3 - x_4 \equiv 0 \bmod 4$,

and the ring of integers of $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ is given by

$$\mathcal{O}_K = \left\{ \frac{x_1 + x_2\sqrt{-2} + x_3\sqrt{-q} + x_4\sqrt{2q}}{2} \;\middle|\; x_i \in \mathbb{Z} \right\} \tag{5.1.2}$$

where $x_1 \equiv x_3 \bmod 2$, and $x_2 \equiv x_4 \bmod 2$.

We study the fundamental unit $\xi_K$ of $K$ by relating it to the fundamental unit $\xi_k$ of its maximal real subfield $k$. In the last chapter, we determined certain congruence properties for $\xi_k$ considering ramification of primes in $k$. In this chapter we extend these congruences to the fundamental unit of $K$.

We first consider $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$. By quadratic reciprocity, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. Without loss of generality we assume that $\left(\frac{p}{q}\right) = 1$. It is easy to see that

$$\xi_k = \begin{cases} x + y\sqrt{pq}, & x, y \in \mathbb{Z} & \text{when } pq \equiv 1 \bmod 8 \\ \dfrac{x + y\sqrt{pq}}{2}, & x, y \in \mathbb{Z}, \quad x \equiv y \bmod 2 & \text{when } pq \equiv 5 \bmod 8. \end{cases}$$

Accordingly, we examine $\xi_K$ as well as $\xi_k$ by distinguishing the cases $pq \equiv 1$ modulo 8 and $pq \equiv 5$ modulo 8. Our results can be stated as follows.

**Theorem 5.1.1.** *Let $p,\ q > 3$ be two primes congruent to 3 modulo 4 such that $pq \equiv 1$ modulo 8. Then the fundamental unit of $\mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ is of the form $\alpha\sqrt{-p} + \beta\sqrt{-q}$, where $\alpha$ is an even integer and $\beta$ is an odd integer. Further, $\alpha$ is divisible by 4 if and only if $p \equiv 7$ modulo 8.*

**Theorem 5.1.2.** *Let $p,\ q > 3$ be two primes congruent to 3 modulo 4 such that $pq \equiv 5$ modulo 8. Then the fundamental unit of $\mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ is of the form $\dfrac{\alpha\sqrt{-p} + \beta\sqrt{-q}}{2}$, where $\alpha$ and $\beta$ are integers of same parity. Further, if $\alpha$ and $\beta$ are even then $\alpha \equiv 0$ mod 4 and $\beta \equiv 2$ mod 4.*

We have the following result for the remaining case when a totally imaginary biquadratic number field $K$ has odd class number with $W_K = \{\pm 1\}$.

**Theorem 5.1.3.** *Let $q > 3$ be a congruent to 3 modulo 4. Then the fundamental unit of $\mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ is of the form $\alpha\sqrt{-2} + \beta\sqrt{-q}$, where $\beta$ is always odd and $\alpha$ is odd if and only if $q \equiv 3$ mod 8.*

We prove these theorems by considering their analogues (Theorems 5.2.5, 5.2.6 and 5.2.7 below) for the fundamental unit $\xi_k$ in the maximal real subfield obtained in the last chapter and then extending them to $\xi_K$. Before that, we establish a relation between $\xi_K$ and $\xi_k$ which we exploit later.

## 5.2 Relation between $\xi_K$ and $\xi_k$

In this section, we establish a relationship between the fundamental units $\xi_k$ and $\xi_K$, when $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ and $p,\ q > 3$ are distinct primes congruent to 3 modulo 4. In the next section, we shall use this relation and the congruence properties of $\xi_k$ obtained in the previous chapter, to obtain congruence relations for $\xi_K$.

When $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ and $p,\ q > 3$ are distinct primes congruent to 3 modulo 4, we know that (see (2.5) on page 197 in [10])

$$\left[\mathcal{O}_K^\times : W_K \mathcal{O}_k^\times\right] = 2. \tag{5.2.1}$$

Now we prove a lemma concerning the form of the fundamental unit $K$.

**Lemma 5.2.1.** *Let $\xi_K$ be the fundamental unit of $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$ where $p,\ q > 3$ are distinct primes congruent to 3 modulo 4. Then*

$$\xi_K = \frac{x_2\sqrt{-p} + x_3\sqrt{-q}}{4}, \qquad \text{where } x_2, x_3 \in \mathbb{Z}, \qquad \text{and } x_2 \equiv x_3 \bmod 4.$$

Proof: By (5.1.1), we can write $\xi_K = \dfrac{x_1 + x_2\sqrt{-p} + x_3\sqrt{-q} + x_4\sqrt{pq}}{4}$, where $x_i$ are integers of same parity and $x_1 - x_2 + x_3 - x_4 \equiv 0 \bmod 4$. By considering the norm of $\xi_K$ to its subfield $\mathbb{Q}(\sqrt{-p})$, and noting that $\pm 1$ are the only units in the quadratic imaginary subfield, we obtain

$$\begin{aligned} N_{K/\mathbb{Q}(\sqrt{-p})}(\xi_K) = \frac{(x_1 + x_2\sqrt{-p})^2 - (x_3\sqrt{-q} + x_4\sqrt{pq})^2}{4^2} = (\pm 1) \\ \implies x_1x_2 - qx_3x_4 = 0. \end{aligned} \tag{5.2.2}$$

Similarly, considering the norm of $\xi_K$ to the imaginary quadratic subfield $\mathbb{Q}(\sqrt{-q})$, we obtain

$$\begin{aligned} (x_1 + x_3\sqrt{-q})^2 - (x_1\sqrt{-p} + x_4\sqrt{pq})^2 = (\pm 1).4^2 \\ \implies x_1x_3 - px_2x_4 = 0. \end{aligned} \tag{5.2.3}$$

By (5.2.2) and (5.2.3), we obtain $(qx_3^2 - px_2^2)x_4 = 0$. But $qx_3^2 = px_2^2$ would imply that the exponent of $p$ in the factorization of $x_3^2$ is odd, which is impossible unless $x_3 = 0$. If $x_3 = 0$, then $x_2 = 0$ as well. In that case, $\xi_K \in \mathcal{O}_K^\times \cap k^\times = \mathcal{O}_k^\times$, which would contradict (5.2.1). Therefore, $x_4 = 0$. Now, if $x_1 \neq 0$ then $x_2$ and $x_3$ must vanish by (5.2.2) and (5.2.3) and $\xi_K \in \mathbb{Q}$, which is not possible. Therefore, we must have $x_4 = 0 = x_1$ and consequently, $x_2 \equiv x_3 \bmod 4$ by (5.1.1).

We have a similar lemma for the fundamental unit in $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$.

**Lemma 5.2.2.** *Let $\xi_K$ be the fundamental unit of $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ where $q > 3$ is a prime congruent to 3 modulo 4. Then $\xi_K = \alpha\sqrt{-2} + \beta\sqrt{-q}$ where $\alpha$ and $\beta$ are integers.*

Proof: By (5.1.1), we can write $\xi_K = \dfrac{x_1 + x_2\sqrt{-p} + x_3\sqrt{-q} + x_4\sqrt{pq}}{2}$, where $x_i$ are integers of with $x_1 \equiv x_3 \bmod 2$ and $x_2 \equiv x_4 \bmod 2$ by 5.1.2. By considering the norm of $\xi_K$ to its subfield $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-q})$ as in the previous lemma, we obtain $x_4 = 0 = x_1$. By (5.1.2), $x_2 \equiv x_4 = 0 \bmod 2$ and $x_3 \equiv x_1 = 0 \bmod 2$, and the lemma follows.

**Lemma 5.2.3.** *Let $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$, where $p,\ q > 3$ are distinct primes congruent to 3 modulo 4. Then $\xi_K^2 = -\xi_k^{-1}$.*

Proof: By (5.2.1), $\xi_K^2 = \pm\xi_k^j$ for some integer $j$. If possible, let the exponent $j$ is even. Then either $\xi_K = \xi_k^{\frac{j}{2}} \in k$, which is not possible by (5.2.1) or $\sqrt{-1} = \xi_K/\xi_k^{\frac{j}{2}} \in K$, which is not possible by our choice of $K$. If $j$ is a positive odd integer, then both the rational and irrational part of $(\pm 1)\xi_k^j$ would be of same sign, which is not the case for $\xi_K^2 = \left(\dfrac{x_2\sqrt{-p} + x_3\sqrt{-q}}{4}\right)^2$. Therefore, $j = -(2l+1)$ for some non-negative integer $l$. By considering the sign of the rational and the irrational part, we must have

$$\xi_K^2 = -\xi_k^{-(2l+1)}. \tag{5.2.4}$$

On the other hand, we must have $\xi_k = \pm\xi_K^t$ for some integer $t$ as $\xi_k \in \mathcal{O}_K^\times$. By considering the irrational part of the left hand side in (5.2.4), we must have $t$ as even. By considering the sign of the rational and the irrational part in (5.2.4), we must have

$$\xi_k = -\xi_K^{-(2s)}, \tag{5.2.5}$$

where $s$ is a positive integer. By combining (5.2.4) and (5.2.5), we have

$$\xi_K^2 = -\xi_k^{-(2l+1)} = -(-\xi_K)^{2s(2l+1)}. \tag{5.2.6}$$

Therefore, $2 = 2s(2l+1)$ and we must have $l = 0$, i.e., $\xi_K^2 = -\xi_k^{-1}$.

The Lemma 5.2.3 holds for $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ as well by exactly similar arguments. All we need is to ensure that the index formula of (5.2.1) holds in this case too. We include a proof for the index in the proposition below as it is not explicitly covered by the result (2.5) in [10], but the arguments are fairly standard.

**Proposition 5.2.4.** *Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ where $q$ is a prime congruent to 3 modulo 4, and $k = \mathbb{Q}(\sqrt{2q})$. Then*

$$\left[\mathcal{O}_K^\times : W_K \mathcal{O}_k^\times\right] = 2. \tag{5.2.7}$$

proof: Since $q \equiv 3 \bmod 4$, the fundamental unit $\xi_k$ of $k$ has norm $+1$. Let the Galois group of $k/\mathbb{Q}$ be generated by $\sigma$. By Hilbert 90, there exists $\rho \in k^\times$ such that $\rho^{1-\sigma} = \xi_k$. By multiplying $\rho$ with a suitable rational integer, we can assume that $\rho \in \mathcal{O}_k$. As $\rho = \xi_k \rho^\sigma$, the ideal $(\rho) = \rho\mathcal{O}_k$ is Galois-invariant. By considering the ideal factorization of $(\rho)$ and grouping the primes ideal factors into inert, unmarried and ramified primes, we can write $(\rho) = r\mathfrak{a}$, where $r$ is a positive rational number and $\mathfrak{a}$ is a square-free ideal divisible only by the ramified primes of $k$. By replacing $\rho$ with $r^{-1}\rho$, we can assume $(\rho) = \mathfrak{a}$, where $\mathfrak{a} = \mathfrak{a}^\sigma$. We now show that for each of the possibilities for $(\rho) = \mathfrak{a}$, $\xi_k$ is $\pm w^2$ for some unit $w$ in $\mathcal{O}_K$.

When $(\rho) = \mathcal{O}_k$, $\xi_k = \dfrac{\rho}{\rho^\sigma} = \dfrac{\rho^2}{\rho\rho^\sigma} = \rho^2$.

When $(\rho) = \sqrt{2q}\mathcal{O}_k$, $w = \dfrac{\rho}{\sqrt{2q}} \in \mathcal{O}_k^\times$ and $\xi_k = \dfrac{\rho}{\rho^\sigma} = \dfrac{w\sqrt{2q}}{w^\sigma(\sqrt{2q})^\sigma} = -\dfrac{w^2}{ww^\sigma} = -w^2$.

When $(\rho)^2 = 2\mathcal{O}_k$, $w = \dfrac{\rho}{\sqrt{-2}} \in \mathcal{O}_K^\times$ and $\xi_k = \dfrac{\rho}{\rho^\sigma} = \dfrac{w\sqrt{-2}}{w^\sigma(\sqrt{-2})^\sigma} = \pm\dfrac{w^2}{ww^\sigma} = \pm w^2$.

When $(\rho)^2 = q\mathcal{O}_k$, $w = \dfrac{\rho}{\sqrt{-q}} \in \mathcal{O}_K^\times$, and

$\xi_k = \dfrac{\rho}{\rho^\sigma} = \dfrac{w\sqrt{-q}}{w^\sigma(\sqrt{-q})^\sigma} = \pm\dfrac{w^2}{ww^\sigma} = \pm w^2$.

**Congruence properties of $\xi_k$**: In order to exploit the relation between the fundamental units of $K$ and $k$, we recall some of the properties of the fundamental unit of $k$ obtained in the last chapter in this section.

**Theorem 5.2.5.** *Suppose $pq$ is congruent to 1 modulo 8. Let $\xi_k = x + y\sqrt{pq} \in \mathbb{Z}[\sqrt{pq}]$ be the fundamental unit of $\mathbb{Q}(\sqrt{pq})$. Then $x \equiv 7$ modulo 8 and $y \equiv 0$ modulo 4. More precisely,*

*(i) $x \equiv 7$ modulo 16 and $y \equiv 4$ modulo 8 when $p \equiv 3$ modulo 8.*

*(i) $x \equiv 15$ modulo 16 and $y \equiv 0$ modulo 8 when $p \equiv 7$ modulo 8.*

**Theorem 5.2.6.** *Let $p$ and $q$ be distinct primes congruent to 3 modulo 4 such that $pq \equiv 5$ modulo 8. Without loss of generality, let $(\frac{p}{q}) = 1$. Then the fundamental unit of*

*$k = \mathbb{Q}(\sqrt{pq})$ is given by $\xi_k = \dfrac{x + y\sqrt{pq}}{2}$, where either*
*(i) $x \equiv 1$ modulo 4 and $y$ is odd, or*
*(ii) $x \equiv 14$ modulo 16 and $y \equiv 0$ modulo 8.*

**Theorem 5.2.7.** *Let $q$ be a prime congruent to 3 modulo 4 and $\xi_k = x + y\sqrt{2q}$ be the fundamental unit of $k = \mathbb{Q}(\sqrt{2q})$.*
*(i) When $q \equiv 3$ mod 8, $x \equiv 5$ modulo 16 and $y \equiv 2$ mod 4*
*(ii) When $q \equiv 7$ mod 8, $x \equiv 15$ modulo 16 and $y \equiv 0$ modulo 4.*

## 5.3 Congruence properties of $\xi_K$

We now prove Theorems 5.1.1, 5.1.2 and 5.1.3 by using the corresponding results for $\xi_k$ mentioned in the previous section and Lemma 5.2.3. First we consider the case $pq \equiv 1$ modulo 8, where $p$ and $q$ are primes congruent to 3 modulo 4 and $p$ is a quadratic residue modulo $p$. By Lemma 5.2.3, we know that $\xi_K^2 = -\xi_k^{-1}$. Combining with (5.2.1), we obtain

$$\begin{aligned}
&\left(\frac{x_2\sqrt{-p} + x_3\sqrt{-q}}{4}\right)^2 = x + y\sqrt{pq} \\
\implies & px_2^2 + qx_3^2 = 16x, \quad 2x_2x_3 = 16y \\
\implies & 3x_2^2 + 3x_3^2 \equiv 0 \bmod 4 \\
\implies & x_2 = 2\alpha_2, \quad x_3 = 2\alpha_3, \qquad \alpha_2, \alpha_3 \in \mathbb{Z} \\
\implies & 3\alpha_2^2 + 3\alpha_3^2 = 4x \equiv 0 \bmod 4 \\
\implies & \alpha_2 = 2\alpha \quad \alpha_3 = 2\beta, \qquad \alpha, \beta \in \mathbb{Z} \\
\implies & \xi_K = \alpha\sqrt{-p} + \beta\sqrt{-q}, \quad x = p\alpha^2 + q\beta^2, \quad y = 2\alpha\beta.
\end{aligned}$$

By Theorem 5.2.5,

$$p\alpha^2 + q\beta^2 = x \equiv 7 \bmod 8, \qquad 2\alpha\beta = y \equiv 0 \bmod 4. \tag{5.3.1}$$

Therefore, $\alpha$ and $\beta$ have different parity. By considering the norm of $\xi_K$ to $\mathbb{Q}$, we further have

$$(p\alpha^2 - q\beta^2)^2 = \pm 1 \implies p\alpha^2 - q\beta^2 = 1. \tag{5.3.2}$$

In the last equality above, we have to take the + sign as $(\frac{p}{q}) = 1$ and $(\frac{-1}{q}) = -1$. By considering (5.3.2) modulo 4, we can conclude that $\alpha$ has to be even, and $\beta$ is odd. It proves the first part of the Theorem 5.1.1.

When $p \equiv 3 \bmod 8$, $q \equiv 3 \bmod 8$ as well since $pq \equiv 1$ modulo 8. By (5.3.2), $3\alpha^2 - 3\beta^2 \equiv 1$ modulo 8, which implies $\alpha \equiv 2$ modulo 4. When $p \equiv 7$ modulo 8, $q \equiv 7$ mod 8 as well, and considering (5.3.2) modulo 8, we have $\alpha \equiv 0$ modulo 4. It concludes the proof of Theorem 5.1.1.

In the case $pq \equiv 5$ modulo 8 too, we proceed similarly noting that $\xi_k = \frac{x+y\sqrt{pq}}{2}$. Letting $\xi_K = \dfrac{x_2\sqrt{-p} + x_3\sqrt{-q}}{4}$ in $\xi_K^2 = -\xi_k^{-1}$, we obtain

$$\begin{aligned}
& px_2^2 + qx_3^2 = 8x, \quad 2x_2x_3 = 8y \\
\implies & 3x_2^2 + 3x_3^2 \equiv 0 \bmod 4 \\
\implies & x_2 = 2\alpha, \quad x_3 = 2\beta, \qquad \alpha, \beta \in \mathbb{Z} \\
\implies & \xi_K = \frac{\alpha\sqrt{-p} + \beta\sqrt{-q}}{2}, \quad p\alpha^2 + q\beta^2 = 2x, \quad \alpha\beta = y.
\end{aligned}$$

In the case when $y$ is odd in Theorem 5.2.6, we have $\alpha$ and $\beta$ odd as well. In the case when $y \equiv 0$ modulo 8, and $x \equiv 14 \bmod 16$ in Theorem 5.2.6, we have $\alpha\beta \equiv 0 \bmod 8$. By considering the norm of $\xi_K$ to $\mathbb{Q}$, we obtain $p\alpha^2 - q\beta^2 = 4$. Therefore, both $\alpha$ and $\beta$ are even. If $\beta \equiv 0$ modulo 4, then $\alpha \equiv 2 \bmod 4$ and $p\alpha^2 + q\beta^2 = 2x \equiv 2.14$ modulo 16 implies $p \equiv 1$ modulo 4, which is a contradiction. Therefore, $\alpha \equiv 0 \bmod 4$ and $\beta \equiv 2$ mod 4.

Finally we consider the fundamental unit $\xi_K = \alpha\sqrt{-2} + \beta\sqrt{-q}$ of $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$ where $\alpha, \beta \in \mathbb{Z}$ by Lemma 5.2.2. When $q \equiv 3$ modulo 8, Lemma 5.2.3 and Theorem 5.2.7 implies

$$2\alpha^2 + q\beta^2 = x \equiv 5 \bmod 16, \qquad 2\alpha\beta = y \equiv 2 \bmod 4. \tag{5.3.3}$$

Therefore, $\alpha$ and $\beta$ are odd.

When $q \equiv 7$ modulo 8, Lemma 5.2.3 and Theorem 5.2.7 implies

$$2\alpha^2 + q\beta^2 = x \equiv 15 \bmod 16, \qquad 2\alpha\beta = y \equiv 0 \bmod 4. \tag{5.3.4}$$

Therefore, $\alpha$ is even, and $\beta$ is odd.

## 5.4 Examples

In this section, we provide some examples of fundamental units of totally biquadratic fields and of their maximal real subfields to illustrate our results. The computations have been carried out in SAGE ( [35]).

Table 5.1: $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$, $p, q \equiv 3 \bmod 4$, $pq \equiv 1 \bmod 8$, $(\frac{p}{q}) = 1$, $\xi_k = x + y\sqrt{pq}$, $\xi_K = \alpha\sqrt{-p} + \beta\sqrt{-q}$.

| $p \equiv 3\ (8)$ | $q \equiv 3\ (8)$ | $x \equiv 7\ (16)$ | $y \equiv 4\ (8)$ | $\alpha \equiv 2\ (4)$ | $\beta \equiv 1\ (2)$ |
|---|---|---|---|---|---|
| 11 | 19 | 46551 | 3220 | 46 | 35 |
| 11 | 43 | 87 | 4 | 2 | 1 |
| 67 | 11 | 252975383 | 9318468 | 1374 | 3391 |
| 59 | 43 | 8274617367 | 164281132 | 8374 | 9809 |
| $p \equiv 7\ (8)$ | $q \equiv 7\ (8)$ | $x \equiv 15\ (16)$ | $y \equiv 0\ (8)$ | $\alpha \equiv 0\ (4)$ | $\beta \equiv 1\ (2)$ |
| 23 | 7 | 11575 | 928 | 16 | 29 |
| 31 | 23 | 367 | 976 | 292 | 339 |
| 71 | 7 | 1201887 | 53912 | 92 | 293 |
| 7 | 47 | 2376415 | 131016 | 412 | 159 |

Table 5.2: $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-q})$, $q \equiv 3 \bmod 4$, $\xi_k = x + y\sqrt{2q}$, $\xi_K = \alpha\sqrt{-2} + \beta\sqrt{-q}$.

| $q \equiv 3\ (8)$ | $x \equiv 5\ (16)$ | $y \equiv 2\ (4)$ | $\alpha \equiv 1\ (2)$ | $\beta \equiv 1\ (2)$ |
|---|---|---|---|---|
| 11 | 197 | 42 | 7 | 3 |
| 19 | 37 | 6 | 3 | 1 |
| 43 | 10405 | 1122 | 51 | 11 |
| 59 | 306917 | 28254 | 277 | 51 |
| $q \equiv 7\ (8)$ | $x \equiv 15\ (16)$ | $y \equiv 0\ (4)$ | $\alpha \equiv 0\ (2)$ | $\beta \equiv 1\ (2)$ |
| 7 | 15 | 4 | 2 | 1 |
| 23 | 24335 | 3588 | 78 | 23 |
| 31 | 63 | 8 | 4 | 1 |
| 47 | 2143295 | 221064 | 1732 | 151 |

# Chapter 6

# Scope for Future Work

In the first part of our work, we examined the torsion structures of elliptic curves over certain quadratic fields. In a similar vein, we would like to examine the possible torsion structures of elliptic curves over certain suitable classes of cubic and quartic fields.

In 2014, González-Jimenéz and Tornero [12] studied the relationship between $E(\mathbb{Q})_{tors}$ and $E(K)_{tors}$, when $K$ varies over all quadratic extensions of $\mathbb{Q}$ and $E$ varies over all elliptic curves over $\mathbb{Q}$. For each of the torsions $G$ appearing in the Mazur's theorem, they listed the possibilities for $E(K)_{tors}$ when $E(\mathbb{Q})_{tors} = G$. In 2016, González-Jimenéz and Tornero [13] extended their work and computed, for every such $G$, all possible situations where $G \neq H$, where $H$ is any one of the choices for $E(K)_{tors}$. In 2016, Najman et al. [11] studied the relation between the torsion subgroups $E(\mathbb{Q})_{tors}$ and the torsion group $E(K)_{tors}$, where $K$ is any cubic number field. We would like to explore similar questions for quartic fields.

In 2012, F. Najman [25] studied the possible torsions of elliptic curves that appear over the cubic field with smallest absolute value of the discriminant and having Galois group $S_3$ and did the same for Galois group $\mathbb{Z}_3$, under the assumption that the list given in [16] is complete. We are trying to classify the possible torsions of elliptic curves that can appear over pure cubic field $\mathbb{Q}(\sqrt[3]{2})$, which has the smallest discriminant $(-108)$ in absolute value among all pure cubic fields. We are also considering the torsion over the cubic field obtained by adjoining a root of $x^3 + x^2 - 3x - 1$, which have the smallest

discriminant (148) among all non-cyclic totally real cubic fields.

We are also trying for further refinements of our results on fundamental units of real quadratic fields and imaginary biquadratic fields of odd class number.

# Bibliography


[1] S. Alaca and K. S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, 2004.

[2] N. C. Ankeny, E. Artin, and S. Chowla. The class-number of real quadratic number fields. *Annals of Mathematics*, pages 479–493, 1952.

[3] H. Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. *Mathematics of computation*, 79(272):2371–2386, 2010.

[4] J. Bosman, P. Bruin, A. Dujella, and F. Najman. Ranks of elliptic curves with prescribed torsion over number fields. *International mathematics research notices*, 2014(11):2885–2923, 2014.

[5] D. Chakraborty and A. Saikia. Congruence relations for the fundamental unit of a pure cubic field and its class number. *Journal of Number Theory*, 166:76–84, 2016.

[6] M. Chou. Torsion of rational elliptic curves over quartic galois number fields. *Journal of Number Theory*, 160:603–628, 2016.

[7] P. Conner and J. Hurrelbrink. Class number parity, world sci. *Publishing, Singapore*, 1988.

[8] M. Derickx and A. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proceedings of the American Mathematical Society*, 145(10):4233–4245, 2017.

[9] F. Diamond and J. M. Shurman. *A First Course in Modular Forms*, volume 228. Springer, 2005.

[10] A. Fröhlich and M. Taylor. Algebraic number theory cambridge university press, 1991.

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

[12] E. González-Jiménez and J. M. Tornero. Torsion of rational elliptic curves over quadratic fields. *Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas*, 108(2):923–934, 2014.

[13] E. González-Jiménez and J. M. Tornero. Torsion of rational elliptic curves over quadratic fields *II*. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 110(1):121–143, 2016.

[14] D. Jeon, C. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Mathematics of Computation*, 80(273):579–591, 2011.

[15] D. Jeon, C. H. Kim, and E. Park. On the torsion of elliptic curves over quartic number fields. *Journal of the London Mathematical Society*, 74(1):1–12, 2006.

[16] D. Jeon, C. H. Kim, and A. Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arithmetica*, 113:291–301, 2004.

[17] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones mathematicae*, 109(1):221–229, 1992.

[18] S. Kamienny and F. Najman. Torsion groups of elliptic curves over quadratic fields. *Acta Arithmetica*, 3(152):291–305, 2012.

[19] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988.

[20] S. Kim. On congruence relations between the fundamental units of biquadratic fields. *Journal of Number Theory*, 121(1):7–29, 2006.

[21] A. W. Knapp. *Elliptic Curves.(MN-40)*, volume 40. Princeton University Press, 2018.

[22] B. Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[23] F. Najman. Complete classification of torsion of elliptic curves over quadratic cyclotomic field. *Journal of Number Theory*, 130(10):1964–1968, 2010.

[24] F. Najman. Torsion of elliptic curves over quadratic cyclotomic fields. *Mathematical Journal of Okayama University*, 53(1):75–82, 2011.

[25] F. Najman. Torsion of elliptic curves over cubic fields. *Journal of number theory*, 132(1):26–36, 2012.

[26] F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(N)$. *Mathematical research letters*, 23(1):245, 2016.

[27] P. Parent. Torsion des courbes elliptiques sur les corps cubiques. *Ann. Inst. Fourier (Grenoble)*, 50(3):723–749, 2000.

[28] P. Parent. No 17-torsion on elliptic curves over cubic number fields. *J. Théor. Nombres Bordeaux*, 15(3):831–838, 2003.

[29] F. P. Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques. *Acta Arithmetica*, 144:17–52, 2010.

[30] M. Reichert. Explicit determination of nontrivial torsion structure of elliptic curves over quadratic number fields. *Math. of Comp.*, 61:445–462, 1993.

[31] A. Saikia, N. K. Sarma, and D. Chakraborty. On the congruence relations for the fundamental unit of totally imaginary biquadratic fields of odd class number. *Communicated*, 2018.

[32] N. K. Sarma. Torsion of elliptic curves over real quadratic fields of smallest discriminant. *Indian journal of Pure and Applied Mathematics, to appear*, 2018.

[33] N. K. Sarma and A. Saikia. Torsion of elliptic curves over imaginary quadratic fields of class number 1. *Rocky Mountain Journal of Mathematics, to appear*, 2018.

[34] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer Science & Business Media, 2009.

[35] W. Stein. Sage mathematics software. *http://www. sagemath. org/*, 2007.

[36] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. AK Peters/CRC Press, 2001.

[37] M. Stoll. Arithmetic of hyperelliptic curves. *Summer Semester*, 2014.

[38] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, 2003.

[39] K. S. Williams. Integers of biquadratic fields. *Canad. Math. Bull*, 13(4):519–526, 1970.

[40] H. Yokoi. The fundamental unit and bounds for class numbers of real quadratic fields. *Nagoya Mathematical Journal*, 124:181–197, 1991.

[41] Z. Zhang and Q. Yue. Fundamental units of real quadratic fields of odd class number. *Journal of Number Theory*, 137:122–129, 2014.