IMAGINARY QUADRATIC FIELDS, ELLIPTIC CURVES AND PELL SURFACES

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

MANASA K J

DEPARTMENT OF MATHEMATICAL AND
COMPUTATIONAL SCIENCES
NATIONAL INSTITUTE OF TECHNOLOGY
KARNATAKA SURATHKAL, MANGALORE - 575 025

JULY, 2016

Dedicated to all my Teachers.

DECLARATION

By the Ph.D. Research Scholar

I hereby declare that the Research Thesis entitled **Imaginary Quadratic Fields, Elliptic Curves and Pell surfaces** which is being submitted to the ***National Institute of Technology Karnataka, Surathkal*** in partial fulfillment of the requirements for the award of the Degree of ***Doctor of Philosophy*** in ***Mathematical and Computational Sciences*** is a ***bonafide report of the research work carried out by me***. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

Manasa K J

(Register No.: MA12F01)

Department of Mathematical and Computational Sciences

Place: NITK, Surathkal.

Date: 27 /07/2016

CERTIFICATE

This is to *certify* that the Research Thesis entitled **IMAGINARY QUADRATIC FIELDS, ELLIPTIC CURVES AND PELL SURFACES** submitted by **Ms. MANASA K J**, (Register Number: 121182MA12F01) as the record of the research work carried out by her, is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of **Doctor of Philosophy**.

Dr. B. R. Shankar

Research Guide

Chairman - DRPC

(Signature with Date and Seal)

ACKNOWLEDGEMENT

It is indeed a great pleasure to have this opportunity to express my thanks to my thesis supervisor Dr B R Shankar for his continuous support, his advice, his enthusiasm, his patience with me and constant encouragement during this work.

I thank all faculty members, staff and research scholars of the Department of Mathematical and Computational Sciences, for their sincere support throughout my work.

I am grateful to the former Head of the Department Prof. Murulidhar N N and the present Head of the Department Prof. Santhosh George for permitting me to attend various conferences and workshops, which inturn helped me to understand the current research trends. I sincerely thank my research progress assesment committe members Prof. K. P. Halemane and Prof. U. Sripathi for their valuable suggestions and excellent advice in accomplishing this work. I also express my heartfelt gratitude to Prof Sujatha Ramdorai, for her constant encouragement. Special thanks to Prof Raghupathi Rao, and Mrs. Chetana U. V for their advice and suggestions.

I also acknowledge, with gratitude, **National Institute of Technology Karnataka, Surathkal** for providing financial support throughout my research work.

Place: NITK, Surathkal Manasa K J

Date: 27/07/2016

Abstract

This thesis consists of two parts: first part (Chapters 1, 2 and 3) deals with the Cubic Pell's equation and Units of Pure Cubic Fields. We study an algorithm given by Barbeau to compute solutions of a cubic analogue of Pell's equation, $x^3 + my^3 + m^2z^3 - 3mxyz = 1$. For a pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$ with ring of algebraic integers as $\mathfrak{O}_K$, the above equation arises naturally in connection with the study of units in $\mathfrak{O}_K$. Comparisons with other methods like the Jacobi-Perron algorithm are also done. Extensive computations using Python have been carried out and the tables are compared to those obtained by Wada.

In the second part (Chater 4 & 5) we have related elliptic curves, imaginary quadratic fields, and Pell surfaces. Let E_m be the elliptic curve $y^2 = x^3 - m$, where $m > 0$ is a squarefree positive integer and $-m \equiv 2, 3 \pmod 4$. Let $Cl(K)[3]$ denote the 3-torsion subgroup of the ideal class group of the quadratic field $K = \mathbb{Q}(\sqrt{-m})$. Let $S_3 : y^2 + mz^2 = x^3$ be the Pell surface. We show that the collection of primitive integral points on S_3 coming from the elliptic curve E_m do not form a group with respect to the binary operation given by Hambleton and Lemmermeyer. We also show that there is a group homomorphism κ from rational points of E_m to $Cl(K)[3]$ using 3-descent on E_m, whose kernel contains $3E_m(\mathbb{Q})$. We also show that our homomorphism κ, the homomorphism ψ of Hambleton and Lemmermeyer and the homomorphism ϕ of Soleng are related.

Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

The theory of Diophantine equations deals with the study of integer or rational solutions to polynomial equations $f(x_1, x_2, ..., x_s) = 0$ with integer coefficients. The word *Diophantine* refers to the Greek algebraist Diophantus of Alexandria. Diophantus lived sometime between 150 AD and 350 AD and wrote a collection of books on number theory known as the Arithmetica. These books consist entirely of equations and particular solutions. The study of Diophantine equations has a long history. They were studied intensely by ancient Greek, Indian and Chinese mathematicians. Well known are the methods to solve the linear Diophantine equation, systems of linear Diophantine equations (Chinese Remainder Theorem) and the Pythagorean equation $x^2 + y^2 = z^2$. The study of Diophantine equations has attracted the attention of many gifted mathematicians. In 1637 Fermat scribbled on the margin of his copy of *Arithmetica* a problem which is now known as Fermat's last theorem: the equation $x^n + y^n = z^n$ has no nontrivial integer solutions when n is an integer ≥ 3. This problem remained unsolved for more than 300 years and was finally solved by Andrew Wiles in 1995. One of the major issues of Diophantine equation is to decide whether it is solvable at all. In 1900, David Hilbert posed a question "Devise a process according to which it can be determined in a finite number of operations whether a given Diophantine equation is solvable" as the 10th of his celebrated list of 23 problems. In 1970, Martin Davis, Julia Robinson and Yuri Matiyasevich settled the problem negatively.

In this thesis we mainly study two Diophantine equations: namely, Cubic Pell's equation and Pell Surfaces in connection with pure cubic fields and quadratic fields respectively.

On the other hand, the problem of finding integer and rational solutions to Diophantine equations takes tools from algebraic number theory that describe the rings and fields wherein those solutions lie. In Chapter 2 some definitions and background to algebraic number fields are given with special focus on quadratic fields. Kummer(1810-1893), Kronecker(1823-1891) and Dedekind(1831-1916) may be considered as inventors of modern number theory. The whole subject of agebraic number theory came into being through the attempts of mathematicians to prove Fermat's last theorem.

Let m be a positive squarefree integer. The misnamed Pell equation is an expression of the form $x^2 - my^2 = 1$ where $x,\ y$ are constrained to be integers. This very simple equation seems to have been known to mathematicians for over 2000 years. Indeed it was known to Archimedes, as the cattle problem, attributed to him in antiquity. Even today research involving this equation continues to be very active. For about a thousand years, mathematicians had various ad hoc methods of solving such equations, and it slowly became clear that such equations always have positive integer solutions other than $(x,\ y) = (1,\ 0)$. Later it was shown that for any positive squarefree integer m, the equation has infinite number of solutions, which can be expressed in terms of the fundamental solution. It is this puzzle of finding the fundamental solution that is referred to as the problem of solving the Pell equation. Pell's equation is part of a central area of algebraic number theory that treats quadratic forms and the structure of the rings of integers in algebraic number fields.

So far there is no well studied theory for the higher-degree analogues of Pell's Equation. However a great deal of work was done on the cubic equation by P H Daus, G B Mathews, A Cayley and E S Selmer in the late nineteenth and early twentieth century. The continued fraction method seems to be very special to the quadratic case and it is very hard to generalize it to higher degree irrationals. Even at the specific level of quadratic Diophantine equations, there are unsolved problems, and the higher degree analogues of Pell's equation, particularly beyond the third do not appear to have been well studied. In Chapter 3 we study cubic Pell's equation in connection with units of pure cubic fields.

Another Diophantine equation which is studied widely is the equation of elliptic curves. This occured for the first time in the work of Diophantus. Elliptic curves lie in one of the most vibrant areas of mathematics, at the frontiers of research in number theory . An elliptic curve can be described by an equation of the form $y^2 = x^3 + Ax + B$ where $A,\ B$ are fixed integers. The theory of elliptic curves is rich and vast. In 1984 Lenstra found that elliptic curves could be used for factoring integers. Thereafter it is being used in cryptography, factorization and primality testing. Fermat's last theorem was also proved using elliptic curves. Thus elliptic curves have been a center of attraction for many mathematicians. In Chapter 4 we have given a brief introduction to elliptic curves.

A conic is a plane affine curve of degree 2. The conic $Q_0(y, z) = 1$ where $Q_0(y, z)$ is a principal binary quadratic form is called a *Pell conic.* It is well known that there is a close analogy between elliptic curves and number fields. Franz Lemmermeyer gave a close analogy between elliptic curves and Pell conics. He wrote a series of articles to give analogy of arithmetic of elliptic curves, such as 2-descent, Selmer and Tate-Shafarevich groups and even the conjecture of Birch and Swinnerton-Dyer to Pell conics. Later he and Sam Hambelton studied arithmetics of Pell surfaces: i.e, equations of the form $Q_0(y, z) = x^n$. In Chapter 5 we have shown a connection between quadratic fields, elliptic curves and Pell surfaces. Using this relation we have defined a homomorphism between rational points on the elliptic curves and 3- part of class group of imaginary quadratic fields.

In the last chapter, Chapter 6, we conclude the thesis with some problems that can be taken for further study and research.

Chapter 2

NUMBER FIELDS

2.1 INTRODUCTION

The fundamental theorem of arithmetic asserts that every natural number can be written in a unique way as a product of its prime factors. The theory of algebraic number fields has its origin in the generalization of the unique factorization theorem, quadratic reciprocity law and related questions. The period 1800 - 1870 is considered an Introductory period. In this period Gauss published "Disquisitiones Arithmeticae". In this book Gauss brings together results in number theory by mathematicians such as Fermat, Euler, Lagrange, Legendre and adds important new results of his own such as proofs of the quadratic and biquadratic reciprocity laws. It served as the starting point for the work of other mathematicians including Kummer, Dirichlet and Dedekind. Kummer worked on cyclotomic fields. He restricted his investigations to algebraic numbers connected with the nth roots of unity. On the other hand, Dirichlet considered the group of units of the ring generated over $\mathbb{Z}$ by an arbitrary integral algebraic number and determined the structure of this group. It was Dedekind who understood that the basic notion of the theory is the notion of algebraic number field which was absent in the investigations of his predecessors.

Next period $1871 - 1896$ is considered as basic period. In this period the basic notions and theorems were formulated and proved. This was done in three equivalent ways by Dedekind, Kronecker, and Zolotarev. After discovering that uniqueness of factorization into irreducibles holds in some rings of integers but not in all, Kummer and Dedekind took steps to develop more insightful theories. Kummer introduced a new concept called 'ideal numbers.' Dedekind looked at the same ideas from a different direction, introducing the notion of 'ideals', an approach which is now generally accepted. Dedekind showed that although unique factorization may fail for numbers, an elegant theory of unique factorization can be developed for ideals. This was a major turning point in the development of algebra.

Many mathematicians like Jacobi, Eisenstein, Kummer and Hilbert were trying to generalize quadratic reciprocity laws to higher powers. In 1920 Takagi gave the finishing touches by creating class field theory. This period 1897-1930, where development of class field theory began, is considered as heroic period in the development of algebraic number theory. An extension is an abelian extension if it is a Galois extension and the Galois group is abelian. Class field theory describes the abelian extensions of a number field in terms of the arithmetic of the field. This theory was first formulated by D.Hilbert and H. Weber. The Hilbert class field of an algebraic number field K was defined by Hilbert. It is the largest abelian extension H of K, unramified at all primes of K (including the infinite primes); and also $G(H/K) \cong Cl(K)$ where $Cl(K)$ is the class group of K. Hilbert conjectured that every ideal in K becomes principal in the Hilbert class field (Principal Ideal Theorem). On the basis of Artin's reciprocity law in 1930 Furtwangler proved Hilbert's Principal ideal conjecture.

In fact a large part of classical number theory can be expressed in the language of algebraic numbers. This point of view had an enormous influence on the development of number theory. As a result, today algebraic number theory is an important branch of mathematics with applications not only to number theory but also to group theory, algebraic geometry, topology, and analysis.

Most of the material in this chapter are taken from standard books on algebraic number theory, especially from [Alaca and Williams, 2004], [Murty and Esmonde, 2005], and [Stewart and Tall, 2002].

2.2 PRELIMINARY CONCEPTS

DEFINITION 2.2.1. *A number α in $\mathbb{C}$ is called an **algebraic number** if there exists a polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_0$ such that, $a_0, ..., a_n$, not all zero are in $\mathbb{Q}$ and $f(\alpha) = 0$.*

DEFINITION 2.2.2. *A number α in $\mathbb{C}$ is called an **algebraic integer** if there exists a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ such that, $a_0, ..., a_{n-1}$, are in $\mathbb{Z}$ and $f(\alpha) = 0$.*

The complex numbers that are not algebraic are called **trascendental numbers**, examples being e and π.

DEFINITION 2.2.3. *Let α be an algebraic number. The polynomial $p(x)$ over $\mathbb{Q}$ is said to be the minimal polynomial of α if $p(\alpha) = 0,\ p(x)$ is monic and has least degree.*

THEOREM 2.2.1. *Let α be an algebraic number. Then the minimal polynomial $p(x) \in \mathbb{Q}[x]$ of α, is unique and irreducible. Moreover, if $f(x) \in \mathbb{Q}[x]$ is such that $f(\alpha) = 0$ then $p(x)$ divides $f(x)$.*

The degree of the minimal polynomial $p(x)$ is called the **degree** of α. The roots of $p(x)$ are all distinct and are called conjugate roots or conjugates of α. Thus if deg $p(x) = n$ then α has $n - 1$ conjugates.

DEFINITION 2.2.4. *A subfield K of $\mathbb{C}$ is called an algebraic number field if its dimension as a vector space over $\mathbb{Q}$ is finite.*

The dimension of K over $\mathbb{Q}$ is called the degree of K, and is denoted by $[K : \mathbb{Q}]$. In general any algebraic number field K is $\mathbb{Q}(\theta)$ for some algebraic number θ. The number field K is called a quadratic field if degree of extension is 2 and cubic field if degree of extension is 3. The set of all algebraic integers in the algebraic number field K forms a ring called the **ring of integers** and denoted as $\mathfrak{O}_K$. This is a finitely generated $\mathbb{Z}$- module with rank same as $[K : \mathbb{Q}]$. For any $\alpha \in K$, there exists $m \in \mathbb{Z}$ such that $m\alpha \in \mathfrak{O}_K$. Hence a $\mathbb{Z}$ - basis of $\mathfrak{O}_K$ is also a $\mathbb{Q}$ - basis of K and is called **integral basis** of K.

THEOREM 2.2.2. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field of degree n. Then there exist n distinct embeddings $\sigma_i : K \longrightarrow \mathbb{C}$ $(i = 1, 2, ..., n)$, suct that $\sigma_i(\alpha) = \alpha_i$ and these are precisely the roots of the minimal polynomial $p(x)$ of α over $\mathbb{Q}$.*

The following definition is well known:

DEFINITION 2.2.5. *Let K be an algebraic number field of degree n with $\{\omega_1, \omega_2, ..., \omega_n\}$ as integral basis. Let $\{\sigma_i,\ i = 1, 2, ..., n\}$ be n distinct embeddings of K. The discrimininant Δ_K of the field K is the square of the determinant of the matrix $[\sigma_i(\omega_j)]$.*

$$i.e.,\ \ \Delta_K := \{det[\sigma_i(\omega_j)]\}^2.$$

Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let $\theta \in K$ be such that $K = \mathbb{Q}(\theta)$. Let $\theta_1 = \theta, \theta_2, ..., \theta_n$ be the conjugates of θ over $\mathbb{Q}$. For $\alpha \in K$ there exist unique rational number $c_0, c_1, ..., c_{n-1}$ such that

$$\alpha = c_0 + c_1\theta + ... + c_{n-1}\theta^{n-1}.$$

For $k = 1, 2, ..., n$ set $\alpha_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k)$.

DEFINITION 2.2.6. *The collection of algebraic numbers $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ as above are called the $K-$conjugates of α.*

Let $\alpha \in K$, with $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ as K-conjugates of α. Then the trace and norm of α is denoted respectively as $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ and is defined as

$$Tr(\alpha) = \alpha_1 + \alpha_2 + ... + \alpha_n,$$

$$N(\alpha) = \alpha_1\alpha_2...\alpha_n.$$

THEOREM 2.2.3. *Let K be an algebraic number field of degree n. Let $\alpha, \beta \in K$. Then*

$$Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$$

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

If $\alpha \in \mathfrak{O}_K$ then the norm and trace of α are rational integers.
An element $\alpha \in \mathfrak{O}_K$ is called a **unit** if there exists a $\beta \in \mathfrak{O}_K$ such that, $\alpha\beta = 1$.

THEOREM 2.2.4. *$\alpha \in \mathfrak{O}_K$ is a unit if and only if $N(\alpha) = \pm 1$.*

The set of all units in $\mathfrak{O}_K$ denoted by $U(K)$ forms a multiplicative subgroup of K^* where K^* is the multiplicative group of non zero elements of K.

EXAMPLE 1. *(i) For $K = \mathbb{Q}$, $\mathfrak{O}_K = \mathbb{Z}$, then $U(K) = \{\pm 1\}$.*

(ii) For $K = \mathbb{Q}(i)$, $\mathfrak{O}_K = \mathbb{Z}[i]$, then $U(K) = \{\pm 1, \pm i\}$.

Structure of the unit group $U(K)$ is given by Dirichlet as follows:

THEOREM 2.2.5. *(Dirichlet's Units Theorem)*
Let $U(K)$ be the unit group of K. Let $[K : \mathbb{Q}] = n$, and $n = r_1 + 2r_2$ where r_1 and $2r_2$ are respectively, the number of real and nonreal embeddings of K in $\mathbb{C}$. Then

there exist fundamental units $\epsilon_1, \epsilon_2, ..., \epsilon_r$, where $r = r_1 + \ r_2 - 1$, such that every unit $\epsilon \in U(K)$ can be written uniquely in the form

$$\epsilon = \zeta \epsilon_1^{n_1} ... \epsilon_r^{n_r}$$

where $n_1, ..., n_r \in \mathbb{Z}$ and ζ is a root of unity in $\mathfrak{O}_K$. More precisely, if W_K is the subgroup of $U(K)$ consisting of roots of unity, then W_K is finite and cyclic and $U(K) \simeq W_K \times \mathbb{Z}^r$.

A nonzero, nonunit element $\alpha \in K$ is called an **irreducible** if $\alpha = \beta\gamma$ then either β or γ is an unit in K. An element y is called an **associate** of x if $x = uy$ for some unit u. We list some properties of units, associates and irreducibles.

PROPOSITION 2.2.6. *For an integral domain D,*

(i) x is a unit if and only if $x \mid 1$,

(ii) any two units are associates and any associate of a unit is a unit,

(iii) x, y are associates if and only if $x \mid y$ and $y \mid x$,

(iv) a non zero non unit element x is irreducible if and only if every divisor of x is an associate of x or a unit,

(v) an associate of an irreducible is irreducible

Proofs follow directly from definition.

DEFINITION 2.2.7. *An **ideal** is a nonempty subset $\mathfrak{a}$ of a commutative ring R having the following proprties:*

- *for $\alpha, \ \beta \in \mathfrak{a}$, then $\alpha - \beta \in \mathfrak{a}$*
- *for $r \in R$, and $\alpha \in \mathfrak{a}$, then $r\alpha \in \mathfrak{a}$.*

DEFINITION 2.2.8. *If $\{\alpha_1, ..., \alpha_n\}$ is a set of elements in $\mathfrak{O}_K$ then*

$$\Big\{ \sum_{i=1}^{n} r_i \alpha_i : r_i \in \mathfrak{O}_K \Big\}$$

is an ideal of $\mathfrak{O}_K$which is generated by $\{\alpha_1, ..., \alpha_n\}$ and is denoted as $\langle \alpha_1, ..., \alpha_n \rangle$.

An ideal $\mathfrak{a}$ in a commutative ring R is called a **principal ideal** if there exist some $\alpha \in R$ such that, $\mathfrak{a} = \langle \alpha \rangle = \{\lambda\alpha : \lambda \in \mathfrak{O}_K\}$. An integral domain D is a **principal ideal domain** (PID) if every ideal of D is a principal ideal.

DEFINITION 2.2.9. *The product of the ideals $\mathfrak{a}$ and $\mathfrak{b}$ is $\mathfrak{ab}$ and consists of all finite sums $\sum_{k=1}^{l} x_k y_k$, with $l \geq 1$, $x_k \in \mathfrak{a}$ and $y_k \in \mathfrak{b}$.*

DEFINITION 2.2.10. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a commutative ring, write $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} = \mathfrak{ac}$ for some ideal $\mathfrak{c}$.*

If $\mathfrak{a} \mid \mathfrak{b}$ then for some ideal $\mathfrak{c}$ we have $\mathfrak{b} = \mathfrak{ac} \subset \mathfrak{a}$, so $\mathfrak{a} \supset \mathfrak{b}$. Thus in a commutative ring divisibility implies containment.
The converse also holds in the ring of integers of a number field, i.e., $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a} \supset \mathfrak{b}$.

PROPOSITION 2.2.7. *In any commutative ring R, an ideal $\mathfrak{p}$ is prime if and only if for all ideals $\mathfrak{a}$ and $\mathfrak{b}$ in R,*

$$\mathfrak{p} \supset \mathfrak{ab} \Rightarrow \mathfrak{p} \supset \mathfrak{a} \text{ or } \mathfrak{p} \supset \mathfrak{b}.$$

PROPOSITION 2.2.8. *If $\mathfrak{a}$ is a nonzero ideal in $\mathfrak{O}_K$, then $\mathfrak{a}$ has finite index in $\mathfrak{O}_K$.*

DEFINITION 2.2.11. *The norm of nonzero ideal in $\mathfrak{O}_K$ is its index in $\mathfrak{O}_K$, and it is denoted as $N(\mathfrak{a})$.*

Relation between elements and ideal generated by them are as follows:

PROPOSITION 2.2.9. *If D is a domain and x, y are non-zero elements of D then*

(i) *$x \mid y$ if and only if $\langle x \rangle \supseteq \langle y \rangle$,*

(ii) *x and y are associates if and only if $\langle x \rangle = \langle y \rangle$,*

(iii) *x is a unit if and only if $\langle x \rangle = D$,*

(iv) *x is irreducible if and only if $\langle x \rangle$ is maximal among the proper principal ideals of D.*

DEFINITION 2.2.12. *A ring is called **Noetherian** if every ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset ....$ terminates, i.e., if there exists n such that $I_n = I_{n+k}$ for all $k \geq 0$.*

THEOREM 2.2.10. *For any commutative ring R, the following conditions are equivalent:*

(i) R is Noetherian

(ii) every nonempty set of ideals contains a maximal element.

(iii) every ideal of R is finitely generated.

THEOREM 2.2.11. *If a domain D is Noetherian, then factorization into irreducibles is possible in D.*

Any PID is a Noetherian ring. Also in any number field K, the ideals in $\mathfrak{O}_K$ are finitely generated $\mathbb{Z}$-modules. Therefore $\mathfrak{O}_K$ is a Noetherian ring. Hence factorization into irreducibles is possible in $\mathfrak{O}_K$ which may not be unique.

THEOREM 2.2.12. *The ring of integers $\mathfrak{O}_K$ of a number field K has the following properties:*

(i) It is an integral domain, with field of fractions K,

(ii) It is Noetherian,

(iii) If $\alpha \in K$ satisfies a monic polynomial equation with coefficients in $\mathfrak{O}_K$ then $\alpha \in \mathfrak{O}_K$

(iv) Every non-zero prime ideal of $\mathfrak{O}_K$ is maximal

A domain with the property (iii) of the above theorem is called **integrally closed domain.**

DEFINITION 2.2.13. *A* ***fractional ideal*** *in K is a nonzero $\mathfrak{O}_K$-module $\mathfrak{a} \subset K$ such that for some $\alpha \in \mathfrak{O}_K - \{0\}, \quad \alpha\mathfrak{a} \subset \mathfrak{O}_K$.*

Since $\alpha\mathfrak{a}$ is an $\mathfrak{O}_K$-module in $\mathfrak{O}_K$, hence is an ideal of $\mathfrak{O}_K$. Let $\alpha\mathfrak{a} = \mathfrak{b}$, then $\mathfrak{a} = \frac{1}{\alpha}\mathfrak{b}$.

THEOREM 2.2.13. *Any fractional ideal in K is a free $\mathbb{Z}$-module of rank* $[K : \mathbb{Q}]$.

In comparison with fractional ideals, nonzero ideals in $\mathfrak{O}_K$ are called **integral ideals.** A fractional ideal of the form $\beta\mathfrak{O}_K$ for $\beta \in K^\times$ is called **principal.** When $\mathfrak{O}_K$ is a PID, all fractional ideals in K are principal.

DEFINITION 2.2.14. *For a fractional ideal* $\mathfrak{a}$ *in* $\mathfrak{O}_K$ *define* $\mathfrak{a}^{-1}$ *by* $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{O}_K\}$.

Then $\mathfrak{a}^{-1}$ is a fractional ideal of $\mathfrak{O}_K$ with $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}_K$.

THEOREM 2.2.14. *The non-zero fractional ideals in* K *form an abelian group under multiplication which is freely generated by the nonzero prime ideals in* $\mathfrak{O}_K$.

THEOREM 2.2.15. *Every non-zero ideal of* $\mathfrak{O}_K$ *can be written as a product of prime ideals, uniquely up to the order of factors.*

Since $\mathfrak{O}_K$ has unique factorization of ideals it is possible to define the greatest common divisor $\mathfrak{g}$ and the least common multiple $\mathfrak{l}$ of two non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ as follows:

DEFINITION 2.2.15. *Define* $\mathfrak{d}$ *to be the greatest common divisor of* $\mathfrak{a}$,$\mathfrak{b}$ *if:*

(i) $\mathfrak{d}|\mathfrak{a}$ *and* $\mathfrak{d}|\mathfrak{b}$ *and*

(ii) $\mathfrak{e}|\mathfrak{a}$ *and* $\mathfrak{e}|\mathfrak{b} \Rightarrow \mathfrak{e}|\mathfrak{d}$.

Similarly, define $\mathfrak{m}$ *to be the least common multiple of* $\mathfrak{a}$,$\mathfrak{b}$ *if:*

(i) $\mathfrak{a}|\mathfrak{m}$ *and* $\mathfrak{b}|\mathfrak{m}$ *and*

(ii) $\mathfrak{a}|\mathfrak{n}$ *and* $\mathfrak{b}|\mathfrak{n} \Rightarrow \mathfrak{m}|\mathfrak{n}$.

LEMMA 2.2.16. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals of* $\mathfrak{O}_K$, *and* $\mathfrak{g}$, $\mathfrak{l}$ *are the greatest common divisor and least common multiple, respectively, of* $\mathfrak{a}$ *and* $\mathfrak{b}$, *then*

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{l} = \mathfrak{a} \cap \mathfrak{b}.$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathfrak{O}_K$ with $\mathfrak{a}+\mathfrak{b} = \langle 1 \rangle$, then $\mathfrak{a}$ and $\mathfrak{b}$ are said to be **relatively prime.**

THEOREM 2.2.17. *The ring* $\mathfrak{O}_K$ *is a unique factorization domain if and only if it is a principal ideal domain .*

DEFINITION 2.2.16. *An integral domain* D *is a* ***Dedekind domain*** *if it satisfies the following properties:*

- *D is integrally closed in its quotient field.*

- *every nonzero prime ideal of D is maximal .*
- *D is Noetherian*

The ring of algebraic integers in any number field is an example of a Dedekind domain. Also, a principal ideal domain is both a Dedekind domain and a unique factorisation domain. The converse is also true: a ring that is a UFD and a Dedekind domain is a PID. One of the important properties of a Dedekind domain is that every nonzero integral ideal can be expressed uniquely as a product of powers of prime ideals.

2.3 IDEAL CLASS GROUP

Let K be a Dedekind domain .The collection of all fractional ideals I_K forms an abelian group with respect to the ideal multiplication in K. The collection P_K of all principal fractional ideals of K is a subgroup of I_K.

DEFINITION 2.3.1. *The quotient group I_K/P_K is called the* ***ideal class group*** *$Cl(K)$ of K.*

Surprisingly we have following result:

THEOREM 2.3.1. *The group $Cl(K)$ is a finite group.*

The cardinality of $Cl(K)$ denoted by h_K is called the **class number** of K. This group measures the extent to which unique factorization fails. Most importantly, K has unique factorisation into irreducibles if and only if $h_K = 1$.
An element $\beta \in K$ is said to be **totally positive** if $N(\beta) > 0$. Let P_K^+ be the group of principal fractional ideals $\langle\beta\rangle = \beta\mathfrak{O}_K$ where $N(\beta) > 0$. The quotient group I_K/P_K^+ is called the **narrow class group** $Cl^+(K)$ of K.
For imaginary quadratic fields, the norm of any nonzero element is always positive, thus the class group and the narrow class group are identical. A collection of ideal classes of order dividing 2 in K forms a subgroup of $Cl(K)$ and is called the 2-part of the ideal class group and is denoted as $Cl(K)[2]$.

DEFINITION 2.3.2. *Let K be a number field with signature $\{r_1, r_2\}$, discriminant Δ_K and of degree $n = r_1 + 2r_2$. The value*

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}$$

is called Minkowski bound for K.

THEOREM 2.3.2. *(Minkowski theorem)*
Let K be an algebraic number field of degree n over $\mathbb{Q}$. Then each ideal class contains an integral ideal $\mathfrak{b}$ satisfying

$$N(\mathfrak{b}) \leq M_K.$$

The Minkowski bound is used for computing the ideal class group and to show that class group is finite.

2.4 QUADRATIC FIELDS

A quadratic field K is a number field of degree 2. Then $K = \mathbb{Q}(\sqrt{m})$ where $m \neq 1$ is a squarefree rational integer. Every element $\alpha \in K$ is of the form $x + y\sqrt{m}$ where $x,\ y \in \mathbb{Q}$. The field K is real if $m > 0$, otherwise it is an imaginary quadratic field. For any $\alpha = x + y\sqrt{m} \in K$, its conjugate is $\overline{\alpha} = x - y\sqrt{m}$. Thus $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2x$ and $N(\alpha) = \alpha\overline{\alpha} = x^2 - my^2$. Every $\alpha \in K$ is a root of the monic polynomial $p(x)$ of the form $p(x) = x^2 - \mathrm{Tr}(\alpha)x + N(\alpha)$. Thus an element $\alpha \in K$ is an algebraic integer of K precisely when its trace and norm are in $\mathbb{Z}$.
The ring of algebraic integers of the quadratic field K is :

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{if } m \not\equiv 1 \ (mod\ 4) \\ \mathbb{Z}\Big[\dfrac{1+\sqrt{m}}{2}\Big], & \text{if } m \equiv 1 \ (mod\ 4). \end{cases}$$

Let

$$\omega = \begin{cases} \sqrt{m}, & \text{if } m \not\equiv 1 \ (mod\ 4) \\ \dfrac{1+\sqrt{m}}{2}, & \text{if } m \equiv 1 \ (mod\ 4). \end{cases}$$

Thus the ring $\mathfrak{O}_K = \mathbb{Z}[\omega] = \{a + b\omega : a,\ b \in \mathbb{Z}\}$.

THEOREM 2.4.1. *For $m \in \mathbb{Z}$ and $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, $\ m \mid \alpha$ in $\mathbb{Z}[\omega]$ if and only if $m \mid a$ and $m \mid b$ in $\mathbb{Z}$.*

THEOREM 2.4.2. *If $\alpha \in \mathfrak{O}_K$ then $\overline{\alpha} \in \mathfrak{O}_K$.*

THEOREM 2.4.3. *(a) If $m \not\equiv 1(mod\ 4)$ then K has $\{1, \sqrt{m}\}$ as integral basis.*

(b) If $m \equiv 1(mod\ 4)$ then K has $\{1, \frac{1+\sqrt{m}}{2}\}$ as integral basis.

The discriminant of the field K is,

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

Since the discriminants of isomorphic fields are equal, it follows that for distinct squarefree m the fields $\mathbb{Q}(\sqrt{m})$ are not isomorphic.

THEOREM 2.4.4. *The discriminant uniquely determines a quadratic field.*

By Dirchlet's units theorem, the unit group of a quadratic field K is, $U(K) \cong \{\pm 1\} \times \langle \epsilon_K \rangle$ where ϵ_K is called the fundamental unit.

THEOREM 2.4.5. *The group of units U of the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$, for m squarefree positive, is as follows:*

(i) *For $m = 1$, $U = \{\pm 1, \pm i\}$*

(ii) *For $m = 3$, $U = \{\pm 1, \ \pm \omega, \ \pm \omega^2\}$ where $\omega = e^{2\pi i/3}$.*

(iii) *For all other m, $U = \{\pm 1\}$*

THEOREM 2.4.6. *The group of units of a real quadratic field $\mathbb{Q}(\sqrt{m})$ is an infinite cyclic group.*

THEOREM 2.4.7. *Every ideal in $\mathfrak{O}_K$ is finitely generated, with at most two generators.*

THEOREM 2.4.8. *Any ideal in $\mathfrak{O}_K$ which has a set of generators from $\mathbb{Z}$ is a principal ideal.*

DEFINITION 2.4.1. *For an ideal $\mathfrak{a}$, its conjugate ideal is $\overline{\mathfrak{a}} := \{\overline{\alpha} : \alpha \in \mathfrak{a}\}$.*

Clearly $\overline{\mathfrak{a}}$ is an ideal.

THEOREM 2.4.9. *If $\mathfrak{a} = (\alpha_1, ..., \alpha_m)$ then $\overline{\mathfrak{a}} = (\overline{\alpha_1}, ..., \overline{\alpha_m})$. In particular, if $\mathfrak{a} = \langle \alpha \rangle$ is principal then $\overline{\mathfrak{a}} = \langle \overline{\alpha} \rangle$ is also principal.*

For principal ideals divisibility of ideals is exactly divisibility of the generators as elements of $\mathfrak{O}_K$.

THEOREM 2.4.10. *For α and β in $\mathfrak{O}_K$, $\langle \alpha \rangle | \langle \beta \rangle$ if and only if $\alpha | \beta$.*

THEOREM 2.4.11. *For ideals $\mathfrak{a}$ and $\mathfrak{b}$, if $\mathfrak{a}|\mathfrak{b}$ then $\mathfrak{a} \supset \mathfrak{b}$. In particular, if $\mathfrak{a} \mid \mathfrak{b}$ and $\mathfrak{b} \mid \mathfrak{a}$ then $\mathfrak{a} = \mathfrak{b}$*

THEOREM 2.4.12. *If $\mathfrak{a} = \langle \alpha_1, ..., \alpha_m \rangle$ has m generators then $\mathfrak{a}\overline{\mathfrak{a}}$ is generated by the m integers $(N(\alpha_1), ..., N(\alpha_m))$ and $\frac{m(m-1)}{2}$ integers $Tr(\alpha_i \overline{\alpha_j})$ where $i < j$.*

Thus ideal $\mathfrak{a}\bar{\mathfrak{a}}$ has a set of generators from $\mathbb{Z}$. Thus by Theorem 2.4.8 $\mathfrak{a}\bar{\mathfrak{a}}$ is principal.

THEOREM 2.4.13. *For any ideal $\mathfrak{a}$ in $\mathfrak{O}_K$, the product $\mathfrak{a}\bar{\mathfrak{a}}$ is a principal ideal.*

Hence for any nonzero ideal $\mathfrak{a}$ in $\mathfrak{O}_K$, ideal $\mathfrak{a}\bar{\mathfrak{a}}$ is principal with a generator in $\mathbb{Z}$. Without loss of generality we may choose generator in $\mathbb{Z}^+$.

DEFINITION 2.4.2. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$. The ideal norm of $\mathfrak{a}$ denoted as $N\mathfrak{a}$ be the positive integer which generates $\mathfrak{a}\bar{\mathfrak{a}}$:*

$$\mathfrak{a}\bar{\mathfrak{a}} = \langle N\mathfrak{a}\rangle, \quad N\mathfrak{a} \in \mathbb{Z}^+.$$

THEOREM 2.4.14. *If ideal $\mathfrak{a}$ is principal say $\mathfrak{a} = \langle\alpha\rangle$ then $N\mathfrak{a} =\mid N(\alpha) \mid$.*

Thus for principal ideal, ideal norm is compatible with the element norm.

THEOREM 2.4.15. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals then $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}\ N\mathfrak{b}$.*

COROLLARY 2.4.15.1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals, if $\mathfrak{a} \mid \mathfrak{b}$ then $N\mathfrak{a} \mid N\mathfrak{b}$ in $\mathbb{Z}$.*

DEFINITION 2.4.3. *The sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ is*

$$\mathfrak{a} + \mathfrak{b} = \{x + y : x \in \mathfrak{a},\ y \in \mathfrak{b}\}.$$

Clearly $\mathfrak{a} + \mathfrak{b}$ is an ideal. This is the greatest common divisior of $\mathfrak{a}$ and $\mathfrak{b}$.

THEOREM 2.4.16. *Every nonzero prime ideal in $\mathfrak{O}_K$ divides a unique prime number.*

Let $\mathfrak{p}$ be a prime ideal and p be the unique rational prime such that $\mathfrak{p} \mid \langle p\rangle$ then p is called the rational prime lying below $\mathfrak{p}$, and ideal $\mathfrak{p}$ is said to be a prime ideal lying over p.

COROLLARY 2.4.16.1. *Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$ then $N\mathfrak{p}$ is either p or p^2 for some rational prime p.*

PROPOSITION 2.4.17. *For an odd rational prime p and a quadratic field of discriminant d, the following holds:*

- $p\mathfrak{O}_K = \mathfrak{p}^2, \quad \mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = 0$
- $p\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}', \mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = 1$
- $p\mathfrak{O}_K = \mathfrak{p}, \mathfrak{p}$ *prime if and only if* $\left(\frac{d}{p}\right) = -1$, *where* $\left(\frac{d}{p}\right)$ *is the Legendre symbol.*

Chapter 3

CUBIC PELL'S EQUATION AND UNITS IN A PURE CUBIC FIELD

3.1 QUADRATIC PELL'S EQUATION

A Diophantine equation of the form $x^2 - my^2 = 1$ where m is a squarefree natural number is known as quadratic Pell's equation. When m is a perfect square or negative, the equation has only trivial solutions. When m is squarefree and positive, the equation has nontrivial solutions. Observe that if (x, y) is a solution then $(\pm x, \pm y)$ are also solutions. Hence it is sufficient to find only positive solutions. Methods of solving the above equation in positive integers have been studied extensively; special cases were considered by Greeks. However, Indian mathematicians have given clear constructive methods of solution. The Indian method was described as the *Chakravala or Cyclic method*. Earliest accounts are due to Brahmagupta, Jayadeva and Bhaskaracharya. This equation should rightly be called as the *Brahmagupta-Bhaskara equation* and is now widely acknowledged as such. However, due to an error by Euler, this equation has been attributed to John Pell. The name has stuck and is commonly known as Pell's equation. This was first posed as a challenge problem to the British mathematicians by Pierre Fermat. His challenge was taken up in England by Brouncker and Wallis. Finally Brouncker succeeded in solving it. Brouncker's method was modified and extended by Euler, who realized that continued fractions could be used to solve it. The *smallest nontrivial solution* of Pell's equation is so *unpredictable* that its existence is not clear in general. However in 1768 Lagrange proved that if m is any non square positive integer, $x^2 - my^2 = 1$ has nontrivial solutions. Around 1840, using the "pigeonhole principle", Dirichlet gave a new proof of the above result, *purely existential*. He also proved the existence of a *fundamental* solution from which every other solution can be obtained. There is a close relation between solutions to Pell's equation and the group of units of quadratic fields.

3.2 RELATION BETWEEN QUADRATIC PELL'S EQUATION AND QUADRATIC FIELDS

Consider the quadratic field $F = \mathbb{Q}(\sqrt{m})$ where m is a square free positive integer. For any $\alpha = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, the norm of α is defined as $N(\alpha) = x^2 - my^2$. Let $\mathfrak{O}_F$ be the ring of integers of F. Then

$$\mathfrak{O}_F = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if} \quad m \equiv 2, 3 \ (mod\ 4) \\ \mathbb{Z}\Big[\dfrac{1+\sqrt{m}}{2}\Big] & \text{if} \quad m \equiv 1 \ (mod\ 4) \end{cases}$$

For $m \equiv 2, 3 \ (mod\ 4)$ an element $\alpha \in \mathfrak{O}_F$ is a unit iff $x^2 - my^2 = \pm 1$. Thus, Pell's equation can also be written as $N(x + y\sqrt{m}) = 1$. The collection of units in $\mathfrak{O}_F$ forms a group with respect to multiplication and is called the unit group, U_F, of F. The structure of the unit group is obtained through Dirichlet's units theorem. It determines the rank of the group U_F. It states that the group of units is finitely generated and has rank equal to $r = r_1 + r_2 - 1$ where r_1 is the number of real embeddings and r_2 is the number of conjugate pairs of complex embeddings. Hence for F, rank of the unit group is one i.e., there exist unit ε_m such that $U_F \simeq \{\pm 1\} \times \langle \varepsilon_m \rangle$. All the units in the ring $\mathfrak{O}_F$ can be obtained as powers of ε_m and ε_m is called the *fundamental unit.* The number of fundamental units of a ring of integers of a number field is 0 or infinite. Thus, study of integer solutions to Pell's equation gives an understanding of the group of units in $\mathfrak{O}_F$ for $m \equiv 2, 3 \ (mod\ 4)$. [Eventhough Dirichlet's theorem enables one to find the exact number of fundamental units of $\mathfrak{O}_F$, it is purely existential and not constructive. For quadratic fields there is a method of continued fractions using which the fundamental unit of $\mathfrak{O}_F$ can be found, and hence all solutions to Pell's equation.]

3.3 CONTINUED FRACTIONS

An expression of the form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cdots}}}$$

where $b_i \in \mathbb{N}$ for $i \geq 1$ and $b_0 \in \mathbb{Z}$ is called *infinite simple continued fraction*, which is denoted as $[b_0, b_1, b_2, ...]$. The b_i's are called as **partial quotients.** If a continued fraction terminates then it is called a **finite** simple continued fraction. Continued fraction of a real number α is finite iff α is a rational number. Otherwise it is infinite. The continued fraction algorithm for a real number α_0 is given by $\alpha_k = b_k + \frac{1}{\alpha_{k+1}}, k \geq 0$ where $b_k = \lfloor \alpha_k \rfloor, \alpha_{k+1} = \frac{1}{\alpha_k - b_k}$ (Euclid algorithm for 1 and α).

DEFINITION 3.3.1. *The mth* ***convergent*** *of the sequence $\{b_i\}$ is the truncated continued fraction $[b_0, b_1, b_2, ..., b_m]$ which is denoted as C_m.*

Consider sequences $\{p_m\}$ and $\{q_m\}$, $m = 0, 1, 2, ...$, defined as below:
$p_0 = b_0$, $p_1 = b_1 b_0 + 1$, $p_m = b_m p_{m-1} + p_{m-2} \quad m \geq 2$
$q_0 = 1$, $q_1 = b_1$, $q_m = b_m q_{m-1} + q_{m-2} \quad m \geq 2$.
Then, the mth convergent of the simple continued fraction $[b_0, b_1, b_2, ...]$ has the value $C_m = \frac{p_m}{q_m}$, $0 \leq m$ (proof is by induction).

DEFINITION 3.3.2. *An infinite continued fractions $[b_0, b_1, b_2, ...]$ is* ***periodic*** *if there exist $l \in \mathbb{N}, r \geq 0$ such that $b_k = b_{k+l}$ for all $k \geq r$. If $r = 0$, then the continued fraction is said to be* ***purely periodic****.*

Using continued fractions we can distinguish the set of quadratic irrationals from other real numbers. Suppose a real number α satisfies a polynomial, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ of degree n with integral coefficients $a_0, a_1, a_2, ..., a_n$ and does not satisfy any equation of lower degree. Then α is said to be an **algebraic number of degree** n. An algebraic number of degree two is called a **quadratic irrational**.

DEFINITION 3.3.3. *The quadratic irrational α is said to be* ***reduced*** *if $\alpha > 1$ and if its conjugate lies between -1 and 0.*

LEMMA 3.3.1. *(**Galois**) The continued fraction of α is purely periodic iff α is a reduced quadratic irrational.*

The above lemma can be used to prove the following,

THEOREM 3.3.2. ***(Euler-Lagrange)***
The continued fraction of α is periodic iff α is a quadratic irrational.

Thus, the continued fraction expansion characterizes quadratic irrationals.

Solutions to Pell's Equation

THEOREM 3.3.3. *If (p, q) is a positive solution of $x^2 - my^2 = 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of $\sqrt{m}$.*

This is proved using the following theorem;

THEOREM 3.3.4. *If l is the length of the period in the continued fraction expansion of $\sqrt{m}$, then $p_{kl-1}^2 - mq_{kl-1}^2 = (-1)^{kl}$ where k runs through all natural numbers and $\frac{p_k}{q_k}$ is a convergent of the continued fraction of $\sqrt{m}$.*

By generalizing the above theorem we get

THEOREM 3.3.5. *Let $\frac{p_k}{q_k}$ be the convergents of the continued fraction expansion of $\sqrt{m}$, and let l be the period length of the expansion,*

(i) If l is even, then all positive solutions of $x^2 - my^2 = 1$ are given by $x = p_{kl-1}, \quad y = q_{kl-1}, \quad$ k=1,2,3....

(ii) If l is odd, then all positive solutions of $x^2 - my^2 = 1$ are given by $x = p_{2kl-1}, \quad y = q_{2kl-1}, \quad$ k=1,2,3,...

Thus, the fundamental solution to Pell's equation can be obtained by using method of continued fractions. The continued fractions method was the undisputed method for solving a given Pell equation and only recently faster methods have been developed which is given in [Lenstra Jr, 2008].

Rational Approximation to Real Numbers

LEMMA 3.3.6. *Let $\frac{p_m}{q_m}$ be the mth convergent of the continued fraction representing the irrational number α. If a and b are integers, with $1 \leq b < q_{m+1}$, then $|q_m\alpha - p_m| \leq |b\alpha - a|$.*

Using the above lemma we have

THEOREM 3.3.7. *If $1 \leq b \leq q_m$, the rational number $\frac{a}{b}$ satisfies*

$$|\alpha - \frac{p_m}{q_m}| \leq |\alpha - \frac{a}{b}|$$

THEOREM 3.3.8. *Let α be an arbitrary irrational number. If the rational number $\frac{a}{b}$, where $b \geq 1$ and gcd(a,b) $= 1$, satisfies $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$ then $\frac{a}{b}$ is one of the convergents $\frac{p_m}{q_m}$ in the continued fraction representation of α.*

This shows that the convergents C_m of infinite continued fractions gives the best approximations to irrational numbers. Later, Hurwitz proved that for every irrational α there are infinitely many $p, q \in \mathbb{Z}$ such that $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$. Moreover, Thue, Siegel, and Roth proved that for algebraic irrationals, the exponent 2 is the best possible.

3.4 CUBIC PELL'S EQUATION

Pell's equation can be generalized in many ways. One such generalization is

$$x^3 + my^3 + m^2z^3 - 3mxyz = 1 \tag{3.1}$$

where m is cubefree integer, which is known as the cubic analogue of Pell's equation. Let m be a positive integer, not a perfect cube. The equation $x^3 - m = 0$ has three roots: $\omega, \rho\omega, \rho^2\omega$ where $\omega = \sqrt[3]{m}$, and ρ is the imaginary primitive cube root of unity. Then $K = \mathbb{Q}(\sqrt[3]{m}) = \{x + y\omega + z\omega^2 \mid x, y, z \in \mathbb{Q}\}$ is a **pure cubic field.** It is a non-Galois algebraic number field with one real embedding and two complex embeddings. Hence it has signature (1,1).

DEFINITION 3.4.1. *Let Kbe an algebraic number field.A basis for $\mathfrak{O}_K$ is called an* **integral basis for K.**

DEFINITION 3.4.2. *Let K be an algebraic number field of degree 3. If there exist an element $\theta \in \mathfrak{O}_K$ such that $\mathfrak{O}_K = \mathbb{Z}[\theta]$. The powers of such an element constitute an integral basis called a power integral basis, i.e., $\{1, \theta, \theta^2\}$ is a* **power integral basis.**

Let $1 \neq m \in \mathbb{N}$ be cube free and let $m = ab^2$ where ab is square free. If $m \not\equiv \pm 1 (\text{mod } 9)$ then K is said to be of the **first kind**, otherwise it is said to be of the **second kind.** Let $\mathfrak{O}_K$ denote the ring of algebraic integers of K. It is well known that K has a power integral basis if and only if m is square free and $m \not\equiv \pm 1 (\text{mod } 9)$.

In this case the norm of an element $\alpha = x + y\omega + z\omega^2 \in K$ is,

$$N\left(x + y\omega + z\omega^2\right) = \left(x + y\omega + z\omega^2\right)\left(x + y\omega\rho + z\rho^2\omega^2\right)\left(x + y\rho^2\omega + z\left(\rho^2\omega\right)^2\right)$$

On simplification we get a homogeneous polynomial of degree three in $x,\ y$ and z

$$N\left(x + y\omega + z\omega^2\right) = x^3 + my^3 + m^2z^3 - 3mxyz, \qquad x, y, z \in \mathbb{Q} \tag{3.2}$$

Also,

$$\begin{aligned} x^3 + my^3 + m^2z^3 - 3mxyz &= (x + y\omega + z\omega^2)[(x^2 - yzm) + (z^2m - xy)\omega + (y^2 - xz)\omega^2] \\ &= \frac{1}{2}(x + y\omega + z\omega^2)[(x - y\omega)^2 + (y - z\omega)^2(\omega)^2 + (z\omega^2 - x)^2]. \end{aligned} \tag{3.3}$$

An element $\alpha \in \mathfrak{O}_K$ is a unit if and only if $x^3 + my^3 + m^2z^3 - 3mxyz = \pm 1$. Thus units of K are nontrivial integer solutions to (3.1). An important property of the norm is that it is multiplicative: i.e.,

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Hence it follows that $N(\alpha^{-1}) = (N(\alpha))^{-1}$. Thus $N(\alpha^n) = [N(\alpha)]^n$ for every $n \in \mathbb{Z}$. Hence if $\alpha = x + y\omega + z\omega^2$ is a solution of (3.1) then $\alpha^n, n \in \mathbb{Z}$ is also a solution. As in the quadratic case, using the pigeon hole principle one can show that if m is a positive cube free integer then the corresponding cubic Pell's equation has **nontrivial integer solutions.** Indeed much more is true, one can show that there is a fundamental solution, say ε_m, from which all other solutions can be obtained. So, it is natural to expect an algorithm that computes all integer solutions to (3.1). It is rather surprising that unlike the usual quadratic Pell's equation where there are definite and constructive methods of solution like the continued fraction algorithm (for quadratic irrationals), there is no such technique for the cubic Pell's equation which works for all m. If m is the discriminant of a pure cubic field, then Voronoi's algorithm, which is a continued fraction algorithm, will solve the Diophantine equation (3.1) for every such m. By Dirichlet's units theorem, the unit group of $\mathfrak{O}_K$ has rank 1 and is a cyclic group generated by a fundamental unit. The fundamental unit of $\mathfrak{O}_K$ can be found by solving a Pell like equation but it does not always correspond directly to the fundamental solution of cubic Pell's equation itself. If we could express ε_m in terms of m then we get all solutions to (3.1). There is no method as yet to find ε_m that works for all m. Many authors tried to find formula for ε_m by putting some constraint on m. The Jacobi- Perron Algorithm is one of the well-known methods to find ε_m for some m. Till now there is no algorithm to find ε_m for all m.

3.4.1 JACOBI-PERRON ALGORITHM

In 1848 Charles Hermite wrote a letter to Carl Gustav Jacob Jacobi asking Jacobi to find an algorithm to develop irrationals of any degree into periodic sequences. This is known as the **Hermite problem.** Jacobi in 1869 extended the continued fractions method to represent some cubic irrationals by means of periodic sequences. He proposed an algorithm for pairs of numbers in cubic fields with the hope that his algorithm will become eventually periodic. Jacobi found some examples, but he could not show that Lagrange's theorem is true for this algorithm always. In 1907, Perron generalized the work of Jacobi. This generalization is known as the Jacobi-Perron algorithm (JPA) which proceeds as follows:
Let $a^{(0)}$ be a vector in R^{n-1}; then the sequence $\langle a^{(v)} \rangle$ is called the JPA, if for $a^{(v)} = (a_1^{(v)}, a_2^{(v)}, ..., a_{n-1}^{(v)})$ where $v = 0, 1, 2...$

$$a^{(v+1)} = \frac{1}{a_1^{(v)} - b_1^{(v)}} (a_2^{(v)} - b_2^{(v)}, ..., a_{n-1}^{(v)} - b_{n-1}^{(v)}, 1)$$

$(b_1^{(v)} \neq a_1^{(v)} : v = 0, 1...)$ and $b_i^{(v)} = f(a_i^{(v)})$ where $i = 1, 2, ..., n-1; v = 0, 1, ...$ for some transformation f on R^{n-1}. The JPA of a point $a^{(0)} \in R^{n-1}$ is completely characterized by its transformation function f. The JPA is said to be periodic, if there exist two rational integers L and M, $L \geq 0, M \geq 1$, such that $a^{(M+L)} = a^{(L)}$. If min $L = l$, min $M = m$, then the sequence of vectors $a^{(0)}, a^{(1)}, ..., a^{(L-1)}$ is called the primitive **pre-period** of the Jacobi-Perron algorithm, and the vectors $a^{(L)}, a^{(L+1)}, ..., a^{(L+M-1)}$ is called primitive period. The l and m are called respectively the lengths of the primitive preperiod and period. If $l = 0$, the algorithm is said to be **purely periodic**. Perron proved that if the JPA of a vector $a^{(0)} = (a_1^{(0)}, a_2^{(0)}, ..., a_{n-1}^{(0)})$ becomes periodic, then the components $a_1^{(0)}, a_2^{(0)}..., a_{n-1}^{(0)}$ belong to an algebraic number field of degree $\leq n$, and if they are linearly independent, the degree of that field is exactly n. The converse of the above, i.e., whether the JPA of a vector $a^{(0)}$ whose components belong to an algebraic number field of degree $\leq n$ always becomes periodic, is still **challengingly open**. Leon Bernstein has stated a few classes of infinitely many real algebraic number fields, for which the Jacobi-Perron algorithm of a properly chosen vector $a^{(0)}$ becomes periodic. One of the applications of periodic JPA is calculation of units in the corresponding fields. The following result is due to Hasse and Bernstein

(Bernstein, 1971):

THEOREM 3.4.1. *Let the JPA of $a^{(0)}$ be periodic with L as the length of its primitive preperiod, M the length of its primitive period then $\varepsilon = \prod\limits_{i=L}^{L+M-1} a_{n-1}^{(i)}$ is a unit in the field generated by the components of $a^{(0)}$ over $\mathbb{Q}$.*

By applying the above theorem to the periodic JPA , Bernstein found;

COROLLARY 3.4.1.1. *[Bernstein, 1971] Let D, k, n be natural numbers $n \geq 2$ with $\alpha = \sqrt[n]{D^n \pm k}$ then $\varepsilon = \frac{(\alpha-D)^n}{\alpha^n - D^n}$ is a unit in $\mathbb{Q}(\alpha)$ for the following values of k,*

i) $k = d^r D$ or d^r, $\quad d \mid D \qquad r = 0, 1, 2, ..., n-1$

ii) $n = p^v$ (p prime, v=1,2,...), $\quad k = pd^r D \quad$ or $\quad pd^r, \quad d \mid D$

Bernstein conjectured that $e = \frac{(\alpha-D)^n}{\alpha^n - D^n}$ in the field $\mathbb{Q}(w)$ where $w = \sqrt[n]{D^n \pm k}$ are always fundamental units, with at most a finite number of exceptions. A major progress in the problem of finding fudamental unit of a cubic, not totally real field, with one fundamental unit, has been achieved by H.J. Stender for the following cases;

i) $w = \sqrt[3]{D^3 + d}, d|D$

ii) $w = \sqrt[3]{D^3 + 3d}, d|D, 3d \leq D$

iii) $w = \sqrt[3]{D^3 + 3D}, D \geq 2$

iv) $w = \sqrt[3]{D^3 - d}, d|D, 4d \leq D$

v) $w = \sqrt[3]{D^3 - 3d}, d|D, 12d \leq D$

THEOREM 3.4.2. *In the field $\mathbb{Q}(w)$, w from (i) to (v) above, the unit $e = \frac{(w-D)^n}{w^n - D^n}$, $|w^3 - D^3| > 1$ is always fundamental, with the only exception in (i) for $D = d = 2, w = \sqrt[3]{10}$, where $\frac{1}{3}(-7 - w + 2w^2) = \sqrt{e}$ is the fundamental unit.*

The results of Stender have been extended and the following result is proved;

THEOREM 3.4.3. *Let $a = D^3 + d$, where $a, D, d \in \mathbb{Z}$, with $a, D > 0$, $|d| > 1$, and a cubefree. Then $\epsilon = \frac{(\omega-D)^3}{d}$, where $\omega = \sqrt[3]{a}$, is a unit of $K = \mathbb{Q}(\omega)$ if and only if $d|3D^2$. Moreover, in this case $\epsilon = \eta$, the fundamental unit of K, except for $(D, d) = (2, -6), \quad (1, 3), \quad (2, 2) \quad (3, 1)$ and $(5, -25)$, where $\epsilon = \eta^2$, and $(2, -4)$, where $\varepsilon = \eta^3$.*

Since JPA becomes periodic very rarely, calculating a unit using above formula is not easy. But in, [Bernstein, 1975] it is shown that the JPA can be used to find units of infinitely many algebraic number fields, without the JPA being periodic.

THEOREM 3.4.4. *Let w be a real root of an nth degree polynomial and $\mathbb{Q}(w)$ the algebraic number field generated by adjunction of w to $\mathbb{Q}$; let*

$$a^{(0)} = (a_1^{(0)}(w), a_2^{(0)}(w), ..., a_{n-1}^{(0)}(w))$$

be a vector whose components $a_i^{(0)}(w)$ $(i = 1, 2, 3, ...)$ in the JPA of $a^{(0)}$ be rationalized, i.e.,

$$a_i^{(0)}(\omega) = \frac{C_{0,i}^{(v)} + C_{1,i}^{(v)} w + ... + C_{n-1,i}^{v} w^{n-1}}{M_v};$$

$M_v \in \mathbb{N}$, $C_{j,i}^{(v)} \in \mathbb{Z}$ $(j = 0, 1, ..., n-1; i = 1, ..., n-1)$.
If, for a certain $v > 1$, $\quad M_v = 1$, then

$$e = \prod_{i=1}^{v} a_{n-1}^{(i)} = A_0^{(v)} + a_1^{(v)} A_0^{(v+1)} + a_2^{(v)} A_0^{(v+2)} + ... + a_{n-1}^{(v)} A_0^{(v+n-1)},$$

where the $A_0^{(v)}$ are obtained from the recursion formula

$$A_0^{(0)} = 1; \quad A_0^{(1)} = A_0^{(2)} = ... = A_0^{(n-1)} = 0;$$
$$A_0^{(v+n)} = A_0^{(v)} + b_1^{(v)} A_0^{(v+1)} + ... + b_{n-1}^{(v)} A_0^{(v+n-1)} \qquad (v = 0, 1, 2, ...)$$

is a unit in $\mathbb{Q}(w)$.

When the above theorem is applied for a cubic field, we find that successive vectors $a^{(v)}$ of $a^{(0)} = (w, w^2)$ are of the form

$$a_1^{(v)} = \frac{pw^2 + qw + r}{\alpha w^2 + \beta w + \gamma}$$

$$a_2^{(v)} = \frac{1}{\alpha w^2 + \beta w + \gamma}$$

After rationalising the denominators, we get

$$a_1^{(v)} = \frac{\alpha_v w^2 + \beta_v w + \gamma_v}{M_v}$$

$$a_2^{(v)} = \frac{a_v w^2 + b_v w + c_v}{M_v} \qquad (v = 0, 1, 2....)$$

The coefficients of their corresponding components with rationalized denominators are related by the equations

$$\beta_v^2 - \alpha_v(\gamma_v - M_v b_1^{(v)}) = M_v a_{v+1}$$

$$m\alpha_v^2 - \beta_v(\alpha_v - M_v b_1^{(v)}) = M_v b_{v+1}$$

$$(\gamma_v - M_v b_1^{(v)})^2 - m\alpha_v\beta_v = M_v c_{v+1}$$

$$m(\alpha_v b_{v+1} + \beta_v a_{v+1}) + (\gamma_v - M_v b_1^{(v)})c_{v+1} = M_v M_{v+1}$$

$$a_v c_{v+1} + b_v b_{v+1} + (c_v - M_v b_2^{(v)})a_{v+1} = M_v \alpha_{v+1}$$

$$m a_v a_{v+1} + b_v c_{v+1} + (c_v - M_v b_2^{(v)})b_{v+1} = M_v \beta_{v+1}$$

$$m(a_v b_{v+1} + b_v a_{v+1}) + (c_v - M_v b_2^{(v)})c_{v+1} = M_v \gamma_{v+1}$$

Convergents of the Jacobi Perron Algorithm are given by $\frac{A_1^{(v)}}{A_0^{(v)}}$ and $\frac{A_2^{(v)}}{A_0^{(v)}}$.

We implemented this algorithm in Python and found units in various cubic fields. It is shown that for $m = (n^3+1)(n^3+2)$ where $n \in \mathbb{N}$, the fundamental unit is given by $\varepsilon_m = 1 - 3n(n^3+1)\omega + 3n^2\omega^2$. Delone and Nagell also restricted their study to the equation with $z = 0$, i.e., $x^3 + my^3 = 1 \ \ x, y \in \mathbb{Z}$. The following is proved [Delone and Faddeev, 1964]:

THEOREM 3.4.5. *(Delone-Nagell)*
Let $\mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field with ring of integers $\mathfrak{O}_K$. Then the equation

$$x^3 + my^3 = 1 \tag{3.4}$$

has atmost one solution. If x_1, y_1 with $y_1 \neq 0$ is a solution, then $x_1 + y_1\sqrt[3]{m}$ is either the fundamental unit of $\mathfrak{O}_K$ or its square.

When does the equation (3.4) have nontrivial solution is still an open problem. We next consider a method of solving cubic Pell's equation.

An Algorithm that Sometimes Works (Barbeau's algorithm)

In this section we will explain an algorithm outlined in [Barbeau, 2003] to calculate a solution to (3.1). There is no mathematical certanity that this algorithm will always give the fundamental solution.
Barbeau's algorithm is given as follows;

(i) Let $\theta = (\sqrt[3]{m})$. Consider $p = \lfloor \theta \rfloor$, $q = \lfloor p\theta \rfloor$ and $r = \lfloor (p+1)\theta \rfloor$

(ii) Construct a table as follows.

Table 3.4.1: First Four Steps

(x, y, z)	sign $(x^3 - my^3)$	sign $(y^3 - mz^3)$	value$(x^3 + my^3m^2z^3 - 3mxyz)$
$(q, p, 1)$	$-$	$-$	...
$(q+1, p, 1)$	$+$	$-$	...
$(r, p+1, 1)$	$-$	$+$	...
$(r+1, p+1, 1)$	$+$	$+$	...

(iii) Let (u, v, w) be the last entry in the above table. Let (u_1, v_1, w_1) be that among the previous entries for which $u^3 - mv^3$ and $u_1^3 - mv_1^3$ have opposite signs as well as $v^3 - mw^3$ and $v_1^3 - mw_1^3$ have opposite signs.

(iv) Then next entry in the table is $(u + u_1, v + v_1, w + w_1)$

(v) Continue the above process until we get $x^3 + my^3 + m^2z^3 - 3mxyz = 1$

If (3.1) has solution triple consisting of large positive x, y and z values and $\omega = \sqrt[3]{m} \in \mathbb{R}$, then by (3.1)

$$x^3 + my^3 + m^2z^3 - 3mxyz = \frac{1}{2}(x + y\omega + z\omega^2)[(x - y\omega)^2 + (y - z\omega)^2(\omega)^2 + (z\omega^2 - x)^2]$$

the factor $x + y\omega + z\omega^2 \rightarrow \infty$ and so the other factor approaches 0. Thus, the terms $(x - y\omega)^2$, $(y - z\omega)^2$ and $(z\omega^2 - x)^2$ will be close to zero. This implies $x - y\omega \longrightarrow 0$, $y - z\omega \longrightarrow 0$ & $z\omega^2 - x \longrightarrow 0$. Hence $\frac{x}{y}$, and $\frac{y}{z}$ approximate ω. Hence, in the algorithm, by considering opposite signs of $x^3 - my^3$ and $y^3 - mz^3$ and applying intermediate value property we get a solution to equation (3.1).

This algorithm always gives a solution to (3.1) but not the fundamental solution. Even when it gives the fundamental solution, it will not give all its powers. Using Python code we implemented above algorithm for cube free integers $2 \leq m \leq 300$ and compared with table of units given in [Wada et al., 1970] and those obtained through PARI/GP.

Table 3.4.2: Algorithm for $m = 15$

(x, y, z)	sign$(x^3 - 15y^3)$	sign $(y^3 - 15z^3)$	$x^3 + 15y^3 + 225z^3 - 45xyz$
$(4, 2, 1)$	$-$	$-$	49
$(5, 2, 1)$	$+$	$-$	20
$(7, 3, 1)$	$-$	$+$	28
$(8, 3, 1)$	$+$	$+$	62
$(12, 5, 2)$	$-$	$+$	3
$(17, 7, 3)$	$-$	$-$	68
$(91, 37, 15)$	$-$	$+$	16
$(170, 69, 28)$	$-$	$-$	35
...	...	...	...
$(2153, 873, 354)$	$-$	$-$	62
$(2518, 1021, 414)$	$-$	$-$	7
$(2883, 1169, 474)$	$-$	$+$	12
$(2962, 1201, 487)$	$+$	$-$	88
$(5845, 2370, 961)$	$+$	$-$	100
...	...	...	...

Table 3.4.3: Algorithm for $m = 3$

(x, y, z)	sign$(x^3 - 3y^3)$	sign $(y^3 - 3z^3)$	$x^3+3y^3+9z^3-9xyz$
$(1, 1, 1)$	$-$	$-$	4
$(2, 1, 1)$	$+$	$-$	2
$(2, 2, 1)$	$-$	$+$	5
$(3, 2, 1)$	$+$	$+$	6
$(23, 16, 11)$	$-$	$+$	2
$(29, 20, 14)$	$+$	$-$	5
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(52, 36, 25)$	$+$	$-$	1
$(75, 52, 36)$	$+$	$+$	3
...	...	...	...
$(3584, 2485, 1723)$	$+$	$+$	2
$(3871, 2684, 1861)$	$+$	$-$	16

In the case $m = 15$, the fundamental solution is $(5401, 2190, 888)$, **but this is not picked up** by the algorithm; but for $m = 3$ smallest positive solution $(4, 3, 2)$ is picked up. Similarly when $m = 16$, the smallest positive solution is $(16001, 6350, 2520)$ and this too is *not picked up* by the algorithm. Even when it gives fundamental solution it will not give all its powers.

In the following table we have listed those cubefree values of m, $2 < m \leq 300$ for which the algorithm does not give the fundamental solution.

Table 3.4.4: Cube-free values of m for which algorithm does not pickup the fundamental solution

$m \not\equiv \pm1$ (mod9)	Prime Factors	$m \not\equiv \pm1$ (mod9)	Prime Factors	$m \equiv \pm1$(mod9)	Prime Factors
15	3×5	187	11×17	17	17×1
20	$2^2 \times 5$	191	191×1	19	19×1
23	23×1	193	193×1	53	53×1
28	23×1	201	3×67	82	2×41
47	47×1	204	$2^2 \times 3 \times 17$	89	89×1
89	89×1	212	$2^2 \times 53$	116	$2^2 \times 29$
90	$2 \times 3^2 \times 1$	220	$2^2 \times 5 \times 11$	118	2×59
101	101×1	221	13×17	134	2×67
102	$2 \times 3 \times 17$	223	223×1	143	11×13
148	$2^2 \times 37$	263	263×1	179	179×1
150	$2 \times 3 \times 5^2$	265	53×5	181	181×1
151	151×1	266	$2 \times 7 \times 19$	190	$2 \times 5 \times 19$
155	3×5	273	$3 \times 7 \times 13$	199	199×1
156	$2^2 \times 3 \times 13$	275	$5^2 \times 11$	262	2×131
165	$3 \times 5 \times 11$	292	$2^2 \times 73$		
166	2×83	294	$2 \times 3 \times 7^2$		
167	1×167	295	5×59		
173	173×1	300	$2^2 \times 3 \times 5^2$		
175	$5^2 \times 7$	186	$2 \times 3 \times 31$		
182	$2 \times 7 \times 13$	183	3×61		

Samples of observations obtained by both algorithms are tabulated below for m in $1 \leqslant m < 60$. We denote by f.s. the fundamental solution and f.u. the fundamental unit.

Table 3.4.5: Fundamental solution obtained from above Algorithm

m	fundamental unit ε	Barbeau's algorithm	JPA	comparison	Fundamental unit ?
2	$1+\theta+\theta^2$	ε	ε	both give f.s.	yes
3	$4+3\theta+2\theta^2$	ε	ε	both give f.s.	yes
5	$41+24\theta+14\theta^2$	ε	ε	both give f.s.	yes
6	$109+60\theta+33\theta^2$	ε	ε	both give f.s.	yes
7	$4+2\theta+\theta^2$	ε	ε	both give f.s.	yes
10	$(23+11\theta+5\theta^2)/3$	ε^2	ε^2	both give f.s.	No
11	$89+40\theta+18\theta^2$	ε	ε	both give f.s.	yes
12	$(110+48\theta+21\theta^2)/2$	ε^2	ε^2	both give f.s.	No
13	$94+40\theta+17\theta^2$	ε	ε	both give f. s.	yes
14	$29+12\theta+5\theta^2$	ε	ε	both give f.s.	yes
15	$5401+2190\theta+888\theta^2$	ε^5	ε	only JPA gives f.s.	only JPA gives f.u
17	$324+126\theta+49\theta^2$	ε^2	ε^4	both do not give f.s.	No
19	$(14+5\theta+2\theta^2)/3$	ε^4	ε^2	only JPA gives f.s	No
20	$(22+8\theta+3\theta^2)/2$	ε^4	ε^2	both do not give f. s	No
21	$1705+618\theta+224\theta^2$	ε	ε	both give f.s.	yes
22	$793+283\theta+101\theta^2$	ε	ε	both give f.s	yes
23	$2166673601+7618758860\theta+2679013700\theta^2$	ε^2	ε^2	both do not give f.s.	No
26	$9+3\theta+\theta^2$	ε	ε	both give f.s.	yes
28	$(10+4\theta+\theta^2)/6$	ε^2	ε^2	both give f.s.	No
30	$811+261\theta+84\theta^2$	ε	ε	both give f.s.	yes
31	$101209+322218\theta+10256\theta^2$	ε	ε	both give f.s.	yes
33	$15270674074129+47608762691400\theta+14842791313620\theta^2$	ε	$-$	JPA does not give any solution	Barbeau's algorithm gives f.u.
34	$334153+1031460\theta+318390\theta^2$	ε	$-$	JPA does not give any solution	Barbeau's algorithm gives f.u.
35	$(278+85\theta+26\theta^2)/3$	ε^2	ε^2	both give f.s.	No
37	$100+30\theta+9\theta^2$	ε	ε	both give f.s.	yes
38	$29071+8647\theta+2572\theta^2$	ε	ε	both give f.s.	yes
39	$529+156\theta+46\theta^2$	ε	ε	both give f.s.	yes
41	$931197095781897587447729+2700517487345259540342600\theta+78316338533401657636358\theta^2$	ε	$-$	JPA do not give solution	Barbeau's algorithm gives f.u.

42	$21169 + 60090\theta + 1752\theta^2$	ε	ε	both give f.s.	yes
43	$49 + 14\theta + 4\theta^2$	ε	ε	both give f.s.	yes
44	$(8014 + 2270\theta + 643\theta^2)/6$	ε^2	$-$	JPA does not give f.s. but Barbeau's algorithm gives f.s	no
45	$1477441 + 415374\theta + 116780\theta^2$	ε	ε	both give f.s.	yes
52	$209 + 56\theta + 15\theta^2$	ε	ε	both give f.s.	yes
53	$113015453598 + 300870223392\theta + 80097799969\theta^2$	ε^4	ε^4	both do not give f.s.	No
55	$32947340560201 + 86636214625574\theta + 2278130361072\theta^2$	ε	ε	both give f.s.	Yes
57	$1460968 + 379620\theta + 98641\theta^2$	ε	ε	both give f.s.	yes
58	$929 + 240\theta + 62\theta^2$	ε	ε	both give f.s.	yes
59	$2161836123797351105087 3 + 555314182921593350157 6\theta + 142644411556322429 54\theta^2$	ε	$-$	JPA does not give any solution but Barbeau's algorithm gives f.s.	Barbeau's algorithm gives f.u.

In the following table we have listed those cubefree values of m, $2 \le m \le 200$ for which the algorithm does not give the fundamental unit. In these cases we have found the smallest unit obtained by the algorithm as power of fundamental unit.

m	fundamental unit ε	smallest unit obtained through Barbeau's algorithm as power of f.u ε
10	$(23+11\omega+5\omega^2)/3$	ε^2
12	$(110+48\omega+21\omega^2)/2$	ε^2
15	$5401+2190\omega+888\omega^2$	ε^5
17	$324+126\omega+49\omega^2$	ε^2
19	$(14+5\omega+2\omega^2)/3$	ε^4
20	$(22+8\omega+3\omega^2)/2$	ε^4
23	$2166673601+761875860\omega+267901370\omega^2$	ε^2
28	$(10+4\omega+\omega^2)/6$	ε^2
35	$(278+85\omega+26\omega^2)/3$	ε^2
44	$(8014+2270\omega+643\omega^2)/6$	ε^2
47	$562944292769+155990973316\omega+43224852030\omega^2$	ε^2
53	$113015453598+30087022392\omega+8009779969\omega^2$	ε^4
82	$(7644966923903+17596960532245\theta+4050416739905\theta^2)/3$	ε^4
84	$(332642+759954\theta+173430\theta^2)/2$	ε^2
89*	$(112410587+2517738807\theta+563915300\theta^2)/3$	ε^{10}
90	$58321+130014\theta+2904\theta^2$	ε^{15}
92	$(214312438+474735220\theta+105161119\theta^2)/2$	ε^2
102	$86538093769+185214052235\theta+39640629557\theta^2$	ε^3
107	$(1132477878552072000198554+2385439839473521274845 0\theta+50246661197681085867830\theta^2)/3$	ε^2
116	$(16628482262+34095726480\theta+6991128851\theta^2)/2$	
118	$(698690155699793+1424483058391010\theta+290422294788826\theta^2)/3$	ε^4
133	$4593394+8998770\theta+1762920\theta^2$	ε^2
134	$(62652683111+122434762090\theta+2392598400\theta^2)/3$	ε^4
143	$(7305401975+13970076100\theta+2671489220\theta^2)/3$	ε^6
148	$1878269+35507890\theta+671300\theta^2$	ε^2
150	$(1355+255\theta+48\theta^2)/5$	ε^{20}

151	$58886554777961 + 11058354219854\theta + 20766573713328\theta^2$	ε^2
154	$(2155235855 + 4020881109\theta + 750149221\theta^2)/3$	ε^2
155	$807243088561096721 + 1502774334721597724\theta + 279758443658327758\theta^2$	ε^2
156	$(3789756830 + 7039953384\theta + 1307760069\theta^2)/2$	ε^2
165	$130681 + 238826\theta + 4344\theta^2$	ε^4
166	$1767569 + 3216118\theta + 585520\theta^2$	ε^4
167	$2070166880101044205370118762758521169120826289178053244249389075109893279095936785424371760003290 + 375923837843038705205801495539929446097617578623742913276693580044695372277492842458148859205536\theta + 682644154039125269466796648093864988591615740084512664223119594452807551629620093695048419811 0\theta^2$	ε^2
172	$(117310 + 210094\theta + 3793\theta^2)/6$	ε^2
175	$(378005 + 675580\theta + 12082\theta^2)/5$	ε^2
179	$156588214241986238447085624519593091119 4 + 2778485028863886009422470036481777159976\theta + 4930115010884886652419980776368134208 1\theta^2$	ε^2
181	$(1696672432984275627 8 + 2999428257712544915\theta + 5302478957202395530\theta^2)/3$	ε^4
182	$289 + 51\theta + 9\theta^2$	ε^2
183	$4233504031039334302315890452620079552467606161001 + 7456750540887644295860697272153441211572833277710\theta + 13134067718220050603631140306486604520275732 2400\theta^2$	ε^7
186	$2152107793 + 3770159334\theta + 660473349\theta^2$	ε^2
187	$317918976327167993137411436881 + 555950232082072309243009715516\theta + 97219947083006933481964505 46\theta^2$	ε^2
188	$(829001404477710769250 + 1447113682815299821 02\theta + 2526097060487627843 1\theta^2)/2$	ε^2

204	$(5510 + 936\theta + 159\theta^2)/2$	ε^2
223	$2904036133327413893894\,09 +$ $47888775020014619589782\theta +$ $78970600489391896653 72\theta^4$	ε^4
190	$(72361501175463503 + 125870232466824465\theta + 218946748808255 3\theta^6)/3$	ε^6
193	$3107480913226581015267 00649 +$ $53771980623158197557987634\theta +$ $93047261781410440790436 80\theta^2$	ε^2
197	$32607673372238124198043171656460053404341532 0035464220797168 +$ $560399496838174221354514458565276788 79031271436671660719670\theta +$ $963109487976704584528915713080310713 8502912631297689022961\theta^2$	ε^8
199	$(29927 + 5126\theta + 878\theta^2)/3$	ε^2
199	$(29927 + 5126\theta + 878\theta^2)/3$	ε^2
201	$282914974686875109517742143969 +$ $482974182578913942880112649 18\theta +$ $8245023484385805591032095740\theta^2$	ε^2
204	$(5510 + 936\theta + 159\theta^2)/2$	ε^2
206	$(5808269975 + 9834623311\theta + 1665208861\theta^2)/3$	ε^2
212	$(51518 + 86640\theta + 1449\theta^2)/2$	ε^{34}
220	$(53462 + 88560\theta + 1467\theta^2)/2$	ε^6
221	$35814491624731602750530952006993621204 41 +$ $592372241916916996898572116020362358424\theta +$ $979784598565565006206066836133696932 74\theta^2$	ε^2

3.5 DIOPHANTINE APPROXIMATION

The above method is partially based on the rational approximation of $\sqrt[3]{m}$. Also, a solution $(x,\ y,\ z)$ of the Cubic Pell's equation with large positive $x,\ y$ and z will give rational approximations $\frac{x}{y}$ and $\frac{y}{z}$ to $\sqrt[3]{m}$.

EXAMPLE 2. *Consider the cubic Pell's equation* $x^3+7y^3+49z^3-21xyz = 1$ *then algorithm gives* $(41, 24, 14), (5041, 2948, 1724), (619921, 362532, 212010), (1152906139441, 674223600444, 394288353444)$, *ect as units.*

Let us consider the rational approximation to $\sqrt[3]{7}$:

(i) $\left|\frac{x}{y} - \sqrt[3]{7}\right| = \left|\frac{41}{24} - \sqrt[3]{7}\right| \approx 0.0016426133.$

$\left|\frac{y}{z} - \sqrt[3]{7}\right| = \left|\frac{24}{14} - \sqrt[3]{7}\right| \approx 0.00595238095.$

(ii) $\left|\frac{x}{y} - \sqrt[3]{7}\right| = \left|\frac{5041}{2948} - \sqrt[3]{7}\right| \approx 3.0837187592 \times 10^{-6}.$

$$\left|\frac{y}{z}-\sqrt[3]{7}\right| = \left|\frac{2948}{1724}-\sqrt[3]{7}\right| \approx 8.514671547832364 \times 10^{-7}.$$

(iii) $$\left|\frac{x}{y}-\sqrt[3]{7}\right| = \left|\frac{1152906139441}{674223600444}-\sqrt[3]{7}\right| \approx 2.220446049250313 \times 10^{-16}.$$

$$\left|\frac{y}{z}-\sqrt[3]{7}\right| = \left|\frac{674223600444}{394288353444}-\sqrt[3]{7}\right| \approx 2.220446049250313 \times 10^{-16}.$$

3.6 CONCLUSION

It is not known for which values of m Barbeau's algorithm gives the fundamental unit. From above table it is clear that JPA does not always give a solution. Our computations so far have shown that Barbeau's algorithm always produces a solution to (3.1), though not the fundamental solution in some cases. Thus, the question arises whether one can prove that this is true.

Chapter 4

ELLIPTIC CURVES

Let $f(x, y) = 0$ be a Diophantine equation in two variables. The set of all real solutions to this equation forms a curve in the xy plane and is called an **algebraic curve.** Linear and quadratic equations in two variables define curves of genus zero. The arithmetic of such curves are fairly well understood. The next simplest case is cubic equations in two variables. They are curves of genus one. In contrast to linear and quadratic equations, the rational and integer solutions to cubic equations of the form $y^2 = f(x)$ where $f(x)$ is a cubic polynomial in one variable are still not completely understood. The real solutions to these equations are called **cubic curves** or **elliptic curves.** Currently there is no general method to answer whether such equations have (i) rational solution? (ii) infinitely many rational solutions? In 1922 L J Mordell proved that there exists finite set of rational solutions which generates all other rational solutions. Eventhough Mordell's theorem gives a procedure which works often to find a finite generating set for the set of rational solutions it is only conjectured that his method always yields a generating set.

Over the last two or three decades, elliptic curves have been playing an increasingly important role both in number theory and in related fields such as cryptography. In the 1980s, elliptic curves were used in cryptography, factorization and primality testing. In 1990s, elliptic curves played an important role in the proof of Fermat's Last Theorem.

Most of the results stated in this chapter are well known and can be found in the standard books, such as [Silverman and Tate, 1992], [Silverman, 2009] and [Cohen, 2008].

Let K be a fixed field with an algebraic closure $\overline{K}$. The Weierstrass form of the equation for an elliptic curve is given by

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

with an extra point $\mathcal{O} = [0, 1, 0]$ called the **point at infinity.** If $a_1, ..., a_6 \in K$, then E is said to be defined over K and is denoted by E/K. This form of equation is useful when working with fields of characteristic 2 and characteristic 3.
If $\text{char}(K) \neq 2$, then we can divide by 2 and complete the square:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

This can be written as

$$y_1^2 = x^3 + a_2^{'}x^2 + a_4^{'}x + a_6^{'},$$

with $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ and $a_2^{'} = \left(a_2 + \frac{a_1^2}{4}\right), a_4^{'} = \left(a_4 + \frac{a_1a_3}{2}\right), a_6^{'} = \left(\frac{a_3^2}{4} + a_6\right)$.
If $\text{char}(K) \neq 3$ then the substitution $x_1 = x + \frac{a_2^{'}}{3}$ eliminates the x^2 term yielding the simpler equation as

$$E : y_1^2 = x_1^3 + Ax_1 + B$$

for some constants A, B.
Since we are working over fields K of $\text{char}(K) = 0$ this allows us to consider the equation as $E : y^2 = x^3 + Ax + B$ where $A, B \in K$.

DEFINITION 4.0.1. *A point P is a **singular point** of the curve $C : g(x, y) = 0$ if*

$$\frac{\partial g}{\partial x}(P) = \frac{\partial g}{\partial y}(P) = 0.$$

Otherwise it is a nonsingular point.

A curve C is a non-singular curve (or smooth curve) if every point of C is non-singular.
Let $F(x, y) = y^2 - f(x) = 0$ where $f(x) = x^3 + Ax + B$. By taking partial derivatives, we get,

$$\frac{\partial F}{\partial x} = -f^{'}(x), \quad \frac{\partial F}{\partial y} = 2y.$$

If these partial derivatives vanish simultaneously at a point (x_0, y_0) then $y_0 = 0$ and $f(x)$ and $f^{'}(x)$ have a common root at x_0. Conversely, if f has a multiple root at x_0 then $(x_0, 0)$ is a singular point. Thus the curve $F(x, y) = 0$ is non-singular iff $f(x)$ has distinct roots.

DEFINITION 4.0.2. *(Discriminant of a polynomial)*
*Let $f(x) = x^3 + ax^2 + bx + c \in \overline{K}[x]$. Let $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$ be the roots of $f(x)$. Then the **discriminant** of $f(x)$ is $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \in \overline{K}$. On*

simplification, we get

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

If $a = 0$ then $D = -4b^3 - 27c^2$. It is clear that $f(x)$ has distinct roots iff $D \neq 0$.

DEFINITION 4.0.3. *The* ***j-invariant*** *of an elliptic curve* $E : y^2 = x^3 + Ax + B$ *is defined to be* $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$.

Let E/K be an elliptic curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$. Consider the collection

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

One nice property of this elliptic curve is that $E(K)$ can be equipped with a group structure, where the addition law is defined geometrically via the chord and tangent method as explained below:

4.0.1 THE GROUP LAW

Let E be an elliptic curve given by the Weierstrass equation. Let L be a line. By applying special case of Bezout's theorem, the number of intersecting points of E and L taken with multiplicities consists of exactly three points, say $P,\ Q,\ R$, not necessarily distinct.

DEFINITION 4.0.4. ***(Composition Law)***
Let $P = (x_1, y_1),\quad Q = (x_2, y_2)$ *be two points on an elliptic curve* E*. Let* L *be the line through* P *and* Q *(If* $P = Q$*, let* L *be the tangent line to* E *at* P*). Let* R *be the third point of intersection of* L *with* E*. Let* $L^{'}$ *be the line through* R *and* $\mathcal{O}$*. Then* $L^{'}$ *intersects* E *at* $R,\ \mathcal{O}$ *and a third point. Denote the third point as* $P + Q$*.*

PROPOSITION 4.0.1. *The above composition law has the following properties:*

(a) If a line L *intersects* E *at the points* $P,\ Q,\ R$ *then* $(P + Q) + R = \mathcal{O}$*.*

(b) $P + \mathcal{O} = P$ *for all* $P \in E$*.*

(c) $P + Q = Q + P$ *for all* $P,\quad Q \in E$*.*

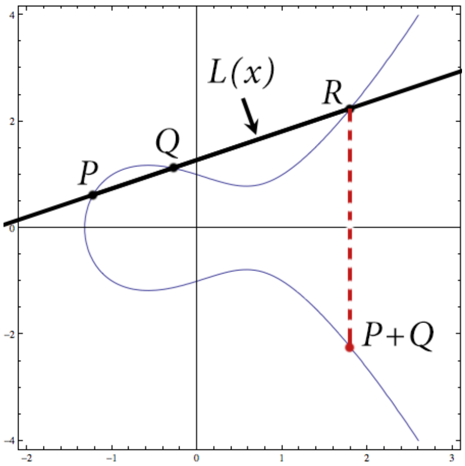

Figure 4.0.1: when $P \neq Q$

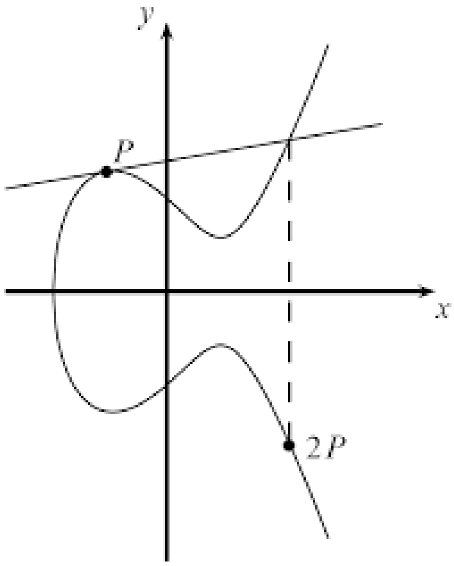

Figure 4.0.2: when $P = Q$

(d) Let $P \in E$. There is a point of E, denoted by $-P$, satisfying

$$P + (-P) = \mathcal{O}.$$

(e) Let $P,\ Q,\ R \in E$. Then $(P+Q)+R = P+(Q+R)$.

Thus the composition law makes $E(K)$ into an abelian group with identity element as $\mathcal{O}$, i.e.,

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

is an abelian group.

EXPLICIT FORMULAS FOR THE GROUP OPERATION

Let E be an elliptic curve given by Weierstrass equation $E : y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \mathcal{O}$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

(a) Let $P_1 = (x_1, y_1)$. Then $-P_1 = (x_1, -y_1)$.

(b) If $x_1 \neq x_2$, then $x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

(c) If $P_1 = P_2$ and $y_1 \neq 0$, then $x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{3x_1^2 + A}{2y_1}$.

(d) If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \mathcal{O}$.

For $m \in \mathbb{Z}$ and $P \in E(K)$, we have $[m]P = \overbrace{P + ... + P}^{\text{m terms if } m>0}$, $\quad [m]P = \overbrace{-P + ... - P}^{|m| \text{ terms if } m<0}$

DEFINITION 4.0.5. *An element $P \in E(K)$ is said to have* ***order*** *m if $[m]P = \mathcal{O}$, but $[n]P \neq \mathcal{O}$ for all integers $1 \leq n < m$.*

If such an m exists, then P has finite order and is called a **torsion point.** Otherwise P is of infinite order.

DEFINITION 4.0.6. *Let E be an elliptic curve over K and $m \in \mathbb{Z}$ with $m \geq 1$. The m-* ***torsion subgroup*** *of E, denoted by $E[m]$, is the set of points of E of order m,*

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

We then define the torsion subgroup of $E(K)$ denoted by $E_{tors}(K)$ to be the set of all points of finite order:

$$E_{tors}(K) = \{P \in E(K) : [m]P = \mathcal{O} \textit{ for some } m \in \mathbb{Z}\}.$$

The structure of $E_{\text{tors}}(K)$ depends on the field upon which the points are considered.

4.1 ELLIPTIC CURVES OVER FINITE FIELDS

Let $\mathbb{F}_q$ be a finite field with q elements. Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. As the number of pairs (x, y) with $x, y \in \mathbb{F}_q$ is finite, the number of points in $E(\mathbb{F}_q)$ denoted as N_q is one more than the number of solutions to the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad \text{with} \qquad (x, y) \in \mathbb{F}_q^2.$$

As each value of x yields at most two values of y, a trivial upper bound is

$$N_q \leq 2q + 1.$$

The following theorem provides a sharp bound for N_q. This result was conjectured by Emil Artin and was proved by Helmut Hasse in the 1930's:

THEOREM 4.1.1. *(Hasse)*

Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then

$$\mid N_q - q - 1 \mid \leq 2\sqrt{q}.$$

THEOREM 4.1.2. *([Washington, 2008])*
Let E be an elliptic curve over the finite field $\mathbb{F}_q$ and $\mathbb{Z}_n$ is additive cyclic group of order n. Then

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad or \qquad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

4.2 ELLIPTIC CURVES OVER THE FIELD OF RATIONALS

For an elliptic curve E over $\mathbb{Q}$, it is relatively easy to determine the $E_{\text{tors}}(\mathbb{Q})$ using the Lutz and Nagell theorem. This was proved independently by Lutz and Nagell in the 1930's.

THEOREM 4.2.1. *(Nagell-Lutz Theorem)([Silverman, 2009])*
Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation

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

Let $P \in E(\mathbb{Q})$ be a torsion point.

(i) $x(P),\ y(P) \in \mathbb{Z}$.

(ii) Either $[2]P = \mathcal{O}$ or else $y(P)^2$ divides $4A^3 + 27B^2$.

COROLLARY 4.2.1.1. *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup of $E(\mathbb{Q})$ is finite.*

Sometimes application of the Nagell-Lutz theorem would be lengthier and much more tedious, in that situation we can apply following theorem which gives the connection between N_p and $E(\mathbb{Q})$.

PROPOSITION 4.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve, p a prime number and m a natural number, not divisible by p. Suppose that $E/\mathbb{Q}$ has good reduction at p. Then the reduction map modulo p :*

$$E(\mathbb{Q})[m] \longrightarrow E(\mathbb{F}_p)$$

is an injective homomorphism of abelian groups. In particular, the number of elements of $E(\mathbb{Q})[m]$ divides the number of elements of $E(\mathbb{F}_p)$.

Eventhough the torsion subgroup of a given elliptic curve is relatively easy to compute, the study of all possible structures of torsion subgroups for elliptic curves over $\mathbb{Q}$ was a difficult problem. This problem was solved only in 1977 by Mazur. The following theorem due to Mazur for $K = \mathbb{Q}$ provides the characterization of the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$:

THEOREM 4.2.3. *(Mazur's Theorem)([Silverman, 2009])*
Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following groups :

$$\mathbb{Z}/N\mathbb{Z} \quad \textit{with} \;\; 1 \leq N \leq 10 \quad \textit{or} \;\; N = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \quad \textit{with} \quad 1 \leq N \leq 4.$$

In particular, its cardinality is at most 16.

Mazur's theorem was generalized to number fields of degree up to 14 by Kamienny and others. This result was further generalized to all number fields by Merel.

THEOREM 4.2.4. *(Merel)([Silverman, 2009])*
Let $d \geq 1$ be an integer. Then there exists a constant $N(d)$ such that for every elliptic curve E/K, where K is a number field of degree atmost d, the following holds:

$$|E_{tors}(K)| \leq N(d).$$

4.3 MAPS BETWEEN ELLIPTIC CURVES

In this section we shall study maps between elliptic curves.

DEFINITION 4.3.1. *Let E_1 and E_2 be two elliptic curves. An **isogeny** from E_1 to E_2 is a nonconstant homomorphism $\phi : E_1(\overline{K}) \longrightarrow E_2(\overline{K})$ that is given by rational functions, i.e., $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P,\ Q \in E_1(\overline{K})$ and there exist rational functions $R_1(x, y)$ and $R_2(x, y)$ with coefficients in $\overline{K}$ such that $\phi(x, y) = (R_1(x, y), R_2(x, y))$ for all $(x, y) \in E_1(\overline{K})$.*

We can write ϕ in the form

$$\phi(x, y) = (r_1(x), yr_2(x))$$

where $r_1(x), \quad r_2(x)$ are rational functions. Write

$$r_1(x) = p(x)/q(x)$$

with polynomials $p(x)$ and $q(x)$ that do not have a common factor. If the coefficients of $r_1(x), r_2(x)$ lie in K, then ϕ is defined over K.

DEFINITION 4.3.2. *The* ***degree*** *of ϕ is defined to be*

$$deg(\phi) = Max\{deg(p(x)), deg(q(x))\}.$$

where $p(x)$ and $q(x)$ as defined above.

If the derivative $r_1^{'}(x)$ is not identically 0, then ϕ is said to be **separable.**

PROPOSITION 4.3.1. *([Washington, 2008])*
Let $\phi : E_1 \to E_2$ be an isogeny. If ϕ is separable, then

$$deg(\phi) = \sharp Ker(\phi).$$

If ϕ is not separable,then

$$deg(\phi) > \sharp Ker(\phi).$$

Thus kernel of an isogeny is a finite subgroup of $E_1(\overline{K})$.

DEFINITION 4.3.3. *An* ***endomorphism*** *of E is a homomorphism $\psi : E(\overline{K}) \to E(\overline{K})$ that is given by rational functions.*

When $E_1(\overline{K}) = E_2(\overline{K})$, an isogeny is just a nonzero endomorphism.
An important map of an elliptic curve E is multiplication by m, defined as below:
For each $m \in \mathbb{Z}$ we define the multiplication-by-m

$$[m] : E \to E$$

in the natural way as follows:

$$[m](P) = \begin{cases} P + P + ... + P & \text{if} \quad m > 0 \\ [-m](-P) & \text{if} \ \ m < 0 \\ \mathcal{O} & \text{if} \quad m = 0 \end{cases}$$

This is an endomorphism of E.

THEOREM 4.3.2. *Let E be an elliptic curve defined over a field K, and let m be a positive integer. Then the endomorphism of E given by map $[m]$ (multiplication by m) has degree m^2.*

PROPOSITION 4.3.3. *([Washington, 2008])*
Let E_1 and E_2 be two elliptic curves with identity elements $\mathcal{O}$ and $\mathcal{O}'$ respectively, and let $\phi : E_1(\overline{K}) \longrightarrow E_2(\overline{K})$ be a nonconstant map given by rational functions. If $\phi(\mathcal{O}) = \mathcal{O}'$, then ϕ is a homomorphism, and therefore an isogeny.

A very important property of isogenies is the existence of dual isogenies.

THEOREM 4.3.4. *([Washington, 2008])*
Let $\phi : E \to \widehat{E}$ be an isogeny of elliptic curves. Then there exists a dual isogeny $\widehat{\phi} : \widehat{E} \to E$ such that $\widehat{\phi} \circ \phi$ is the multiplication map by deg(ϕ) on E.

The map $\widehat{\phi}$ is unique, its degree is $\deg(\phi)$, and $\phi \circ \widehat{\phi}$ is the multiplication map by $\deg(\phi)$ on $\widehat{E}$.

THEOREM 4.3.5. *([Washington, 2008])*
Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. Then $\phi : E_1(\overline{K}) \to E_2(\overline{K})$ is surjective.

EXAMPLE 3. *Let $E : y^2 = x^3 + ax^2 + bx$ and $\widehat{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ be elliptic curves over a field of characteristic different from 2 where we assume that b and $a^2 - 4b$ are both non-zero. Then the map $\phi : E \to \widehat{E}$ given by $(x, y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right)$ is an isogeny of degree 2 with dual isogeny as $\widehat{\phi} : \widehat{E} \to E$ given by $(\widehat{x}, \widehat{y}) \longmapsto \left(\frac{\widehat{y}^2}{4\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^2-\widehat{b})}{8\widehat{x}^2}\right)$.*

The collection of all endomorphisms forms a ring denoted as End(E). The maps $[m]$ are elements of End(E). Usually they are the only distinct endomorphisms on E, i.e., End(E) $\simeq \mathbb{Z}$. Sometimes it may so happen that End(E) is larger than $\mathbb{Z}$.

DEFINITION 4.3.4. *The elliptic curve E is said to have **complex multiplication** if End(E) contains elements other than $[m]$, i.e., if as a ring End(E) is strictly larger than $\mathbb{Z}$.*

EXAMPLE 4. *(i) Let char(K) $\neq 2$ and let $i \in \overline{K}$ be primitive fourth root of unity. The elliptic curves $E : y^2 = x^3 - ax$ has End(E) strictly larger than $\mathbb{Z}$, since it contains a map $[i]$, given by*

$$[i] : (x, y) \to (-x, iy).$$

Thus $\mathbb{Z}[i] \subset$ End(E).

(ii) *Similarly the curves $E : y^2 = x^3 - m$ also have complex multiplication by $\mathbb{Z}[\rho]$, where ρ is a primitive cube root of unity the map is given by $[\rho] : (x, y) \to (\rho x,\ y)$.*

The two elliptic curves E_1 and E_2 are isomorphic over $\overline{K}$ if and only if they both have the same j- invariant.

DEFINITION 4.3.5. *If two different elliptic curves defined over a field K have the same j-invariant, then the two curves are said to be **twists** of each other.*

The only change of variables fixing the point at infinity and preserving above Weierstrass form is given by

$$x = \mu^2 x_1,\ y = \mu^3 y_1,$$

where $\mu \in \overline{K}^*$. Then we obtain

$$E^{'} : y_1^2 = x_1^3 + A_1 x_1 + B_1$$

where $A = \mu^4 A_1,\ B = \mu^6 B_1$.
This change of variables leaves the j- value unchanged, i.e., $j(E) = j(E^{'})$.
Conversely, let E and $E^{'}$ be elliptic curves with the same j-invariant, say $E_1 : y^2 = x^3 + Ax + B$ and $E_2 : y_1^2 = x_1^3 + A_1 x_1 + B_1$. Since $j(E) = j(E^{'})$, we have

$$\frac{4A^3}{4A^3 + 27B^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2},$$

and on simplifying,

$$A^3 B_1^2 = A_1^3 B^2.$$

We want an isomorphism of the form $(x, y) = (\mu^2 x_1, \mu^3 y_1)$ and hence the following three cases arise;

Case 1. Consider $A = 0$ then $j = 0$ and $B \neq 0$, since $\Delta \neq 0$. Thus $A_1 = 0$, and by taking $\mu = (B/B_1)^{1/6}$ we obtain an isomorphism.

Case 2. Consider $B = 0$. Then $j = 1728$ and $A \neq 0$. So, $B_1 = 0$, and $\mu = (A/A_1)^{1/4}$ gives an isomorphism.

Case 3. Consider $AB \neq 0, (j \neq 0, 1728)$. Then $A_1 B_1 \neq 0$ and $\mu = (BA_1/AB_1)^{1/2}$ gives an isomorphism .

Twists may not be isomorphic over K, but they are always isomorphic over some extension field of K. This degree of extension determines the degree of the twist. There are twists of degree 1, in which case E and $E^{'}$ are K-isomorphic. A quadratic twist of an elliptic curve is a twist of degree ≤ 2.
Given a squarefree d in K consider the quadratic twist of $E : y^2 = x^3 + Ax + B$ given by curve $E^d : y^2 = x^3 + d^2Ax + d^3B$. These two elliptic curves have the same j invariant. However, they are not isomorphic over K, but over the field extension $K(\sqrt{d})$ they are isomorphic.
For curves with $j = 0$, or 1728, higher degree twists are possible and for all the other curves only quadratic twist is possible. By Case 1, it is clear that curves with $j = 0$ will have quadratic, cubic as well as sextic twists and for $j = 1728$ only quadratic and quartic twists are possible.

4.4 MORDELL-WEIL THEOREM

For Diophantine aspects of elliptic curves studying these curves over $\mathbb{Q}$ is more interesting. The situation in this case and in more general number fields is much more difficult.

THEOREM 4.4.1. *(Mordell-Weil) Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}$. If $P = (x, y) \in E(\mathbb{Q})$ be an affine rational point then there exist integers r, s, t such that*

$$x = \frac{r}{t^2}, \quad y = \frac{s}{t^3}, \quad \textit{with} \quad gcd(r,t) = gcd(s,t) = 1.$$

In 1922 Mordell proved a conjecture on elliptic curves over $\mathbb{Q}$ due to Henri Poincare. Later Andre Weil generalized this theorem to number fields. Now this theorem is known as the Mordell-Weil theorem, stated below:

THEOREM 4.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Then the Mordell- Weil group $E(\mathbb{Q})$ is finitely generated, i.e.,*

$$E(\mathbb{Q}) \simeq E_{tors}(\mathbb{Q}) \oplus \mathbb{Z}^r$$

where $r \geq 0$.

DEFINITION 4.4.1. *The nonnegative integer r in the above theorem is called the **rank** of $E(\mathbb{Q})$.*

The rank r of the given elliptic curve is, in general, difficult to compute. The rank r is much more mysterious, in general there is no known procedure that is guaranteed to yield the rank of the curve. Even the simple question whether the curve has a finite or an infinite number of rational points is still not fully solved. This is the subject of active research. There are very few general facts known concerning the rank of elliptic curves, but there are a large number of fascinating conjectures. One of the conjectures is:

CONJECTURE 4.4.1. *([Silverman, 2009]) There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.*

Many people have worked in this direction. Neron constructed an infinite family of elliptic curves over $\mathbb{Q}$ having rank at least 10. Elkies has produced an elliptic curve with rank $E(\mathbb{Q}) \geq 28$. However there is a method, known as *method of descent,* which is used in the proof of the Mordell-Weil theorem which facilititates the search of points of infinite order in $E(\mathbb{Q})$. Unfortunately, this method is not always successful. The proof of the Mordell-Weil theorem relies on proving the following two important theorems:

THEOREM 4.4.3. *(Weak Mordell-Weil Theorem)([Silverman, 2009])*
Let $E/\mathbb{Q}$ be an elliptic curve, and let $m \geq 2$ be an integer. Then $E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite group.

THEOREM 4.4.4. *(Descent Theorem)([Silverman, 2009])*
Suppose there there exists a function

$$h : E(\mathbb{Q}) \to \mathbb{R}$$

with the following three properties:

(i) Let $Q \in E(\mathbb{Q})$. There is a constant C_1, depending on $E(Q)$, and Q such that

$$h(P+Q) \leq 2h(P) + C_1 \qquad \textit{for all} \quad P \in E(\mathbb{Q}).$$

(ii) There is an integer $m \geq 2$ and a constant C_2 such that

$$h(mP) \geq m^2 h(P) - C_2 \quad \textit{for all} \;\; P \in E(\mathbb{Q})$$

(iii) For every constant C_3, the set $\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$ is a finite set . Suppose further that for the integer m in (ii), the quotient group $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite. Then $E(\mathbb{Q})$ is finitely generated.

Proof. Choose points $P_1, ..., P_r \in E(\mathbb{Q})$ to represent the finitely many cosets in $E(\mathbb{Q})/3E(\mathbb{Q})$. Let $R \in E(\mathbb{Q})$ be an arbitrary point. Write

$$R = mR_1 + P_{i_1} \quad \text{for some } \ 1 \leq i_1 \leq r.$$

continuing in this fashion

$$\begin{aligned} R \quad &= mR_1 + P_{i_1}, \\ R_1 \quad &= mR_2 + P_{i_2}, \\ \vdots \\ R_{n-1} \quad &= mR_n + P_{i_n} \end{aligned}$$

For any index j, we have

$$\begin{aligned} h(R_j) \qquad &\leq \tfrac{1}{m^2}[h(mR_j) + C_2], \qquad \mathit{from\ (ii)} \\ &= \tfrac{1}{m^2}[h(R_{j-1} - P_{i_j}) + C_2] \\ &\leq \tfrac{1}{m^2}[2h(R_{j-1} + C_1^{'} + C_2] \qquad\qquad from(i) \end{aligned}$$

where $C_1^{'}$ is the maximum of the constants from (i) for $P \in \{-P_1, ..., -P_r\}$. Note that $C_1^{'}$ and C_2 do not depend on R.
We use this inequality repeatedly, starting from R_n and working back to R. This yields

$$\begin{aligned} h(R_n) \quad &\leq (\tfrac{2}{m^2})^n h(R) + [\tfrac{1}{m^2} + \tfrac{2}{m^2} + \tfrac{4}{m^2} + ... + \tfrac{2^{n-1}}{m^2}](C_1^{'} + C_2), \\ &< (\tfrac{2}{m^2})^n h(R) + \tfrac{C_1^{'} + C_2}{m^2 - 2} \\ &\leq \tfrac{1}{2^n} h(R) + \tfrac{1}{2}(C_1^{'} + C_2) \quad \mathit{since} \ \ m \geq 2 \end{aligned}$$

It follows that if n is sufficiently large, then

$$h(R_n) \leq 1 + \frac{1}{2}(C_1^{'} + C_2).$$

Since R is a linear combination of R_n and $P_1, ..., P_r$,

$$R = m^n R_n + \sum_{j=1}^{n} m^{j-1} P_{i_j},$$

it follows that every R in $E(\mathbb{Q})$ is a linear combination of points in the set

$$\{P_1, ..., P_r\} \cup \{P \in E(\mathbb{Q}) : h(P) \leq 1 + \frac{1}{2}(C_1^{'} + C_2)\}.$$

Property (iii) of the function h tells us that this is a finite set. Hence $E(\mathbb{Q})$ is finitely generated. □

An important consequence of this method is that once $E(\mathbb{Q})/mE(\mathbb{Q})$ is known to be finite for some m, obtaining a system of generators for $E(\mathbb{Q})$ is completely algorithmic. Thus the only obstruction to the existence of an algorithm to compute $E(\mathbb{Q})$ lies in the computation of the finite group $E(\mathbb{Q})/mE(\mathbb{Q})$ for some m. Unfortunately, at present there is no known procedure that is guaranteed to give generators for $E(\mathbb{Q})/mE(\mathbb{Q})$. In this chapter we explain elementary 3- descent with 3-isogenies for elliptic curves which has rational 3-torsion subgroup and apply it to prove our result in next chapter. The existence of rational 3-torsion subgroup means there exists a subgroup of order 3 that is invariant under the action of galois conjugation, but not necessarily contains three rational points.

4.5 DESCRIPTION OF 3- DESCENT WITH 3-ISOGENIES

In this section we explain 3- descent with 3-isogenies for elliptic curves. This method is applicable for curves with rational 3-torsion subgroup. A number of authors have studied various aspects of 3-descent [Top, 1991], [Cohen and Pazuki, 2009]. In [Cohen and Pazuki, 2009] authors have given explicit formulas for performing 3-descent on elliptic curves $E/\mathbb{Q}$ which admit a $\mathbb{Q}$-rational isogeny.

DEFINITION 4.5.1. *[Cohen, 2008] Let E be an elliptic curve defined over K, and let $\mathcal{T}$ be a finite subgroup of $E(L)$ for some extension L/K, which without loss of generality we may assume to be finite and galois. We say that $\mathcal{T}$ is a $K-$ rational subgroup of E if it is globally stable by $\sigma \in Gal(L/K)$, i.e., if $T \in \mathcal{T}$ implies that $\sigma(T) \in \mathcal{T}$.*

EXAMPLE 5. *Let $E : y^2 = x^3 - m,\quad L = \mathbb{Q}(\sqrt{-m})$ and $K = \mathbb{Q}$. Consider the subgroup $\mathcal{T} = \{\mathcal{O},\ T,\ -T\}$ where $T = (0,\ -\sqrt{-m})$, of $E(L)$ then $\mathcal{T}$ is a $\mathbb{Q}-$ rational subgroup of order* 3.

PROPOSITION 4.5.1. *[Cohen, 2008] Let E be an elliptic curve defined over a K and having a K-rational subgroup of order* 3, *of the form $\mathcal{T} = \{\mathcal{O},\ T,\ -T\}$ then,* *(i) The abscissa $x(T)$ of T is in K.*

(ii) Up to a change of x into $x - x_0$ for some $x_0 \in K$ the equation of E is $y^2 = x^3 + D(ax+1)^2$ for some $D \in K^*$ and $a \in K$, and then $T = (0, \sqrt{D})$.

(iii) If in addition E has a K-rational point T of order 3, up to the same change the equation of E is $y^2 = x^3 + (ax+b)^2$ for some $a \in K$ and $b \in K^*$, and then $T = (0,\ b)$.

Remark: When E has a K-rational subgroup of order 3 then it can be written in the form $y^2 = x^3 + D(ax+b)^2$. Conversely whenever E is of this form then there is a K-rational subgroup of order 3 generated by $T = (0,\ b\sqrt{D})$.

Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational subgroup of order 3. Up to translation of the $x -$ cordinate assume that E is of the form $y^2 = x^3 + D(ax+b)^2$ with rational 3-torsion subgroup $\{\mathcal{O}, T, -T\}$ where $T = (0,\ b\sqrt{D})$. Now consider another elliptic curve $\widehat{E}$ defined by the equation $y^2 = x^3 + \widehat{D}(\widehat{a}x + \widehat{b})^2$, where $\widehat{D} = -3D$, $\widehat{a} = a$, $\widehat{b} = \frac{27b - 4a^3D}{9}$. Then it also has a rational subgroup of order 3 generated by $\widehat{T} = \left(0,\ \frac{27b-4a^3D}{9}\sqrt{-3D}\right)$.

PROPOSITION 4.5.2. *[Cohen, 2008] Consider a map $\phi : E \longrightarrow \widehat{E}$ as*

$$\phi(P) = (\widehat{x}, \widehat{y}) = \left(\frac{x^3 + 4D[(a^2/3)x^2 + abx + b^2]}{x^2}, \frac{y(x^3 - 4Db(ax+2b))}{x^3} \right)$$

for $P = (x,y) \neq \pm T$ or $\mathcal{O}$ and $\phi(T) = \phi(-T) = \phi(\mathcal{O}) = \widehat{\mathcal{O}}$. Then ϕ is a group homomorphism with kernel as $\{\mathcal{O}, T, -T\}$.

Dually, there exists a homomorphism $\widehat{\phi} : \widehat{E} \longrightarrow E$ defined as

$$\widehat{\phi}(\widehat{P}) = (x, y) = \left(\frac{\widehat{x}^3 + 4\widehat{D}((\widehat{a}^2/3)\widehat{x}^2 + \widehat{a}\widehat{b}\widehat{x} + \widehat{b}^2)}{9\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^3 - 4\widehat{D}\widehat{b}(\widehat{a}\widehat{x} + 2\widehat{b}))}{27\widehat{x}^3} \right)$$

for $P = (\widehat{x}, \widehat{y}) \neq \pm\widehat{T}$ or $\widehat{\mathcal{O}}$ and by $\widehat{\phi}(\widehat{T}) = \widehat{\phi}(-\widehat{T}) = \widehat{\phi}(\widehat{\mathcal{O}}) = \mathcal{O}$.

Furthermore, for all $P \in E$ we have $\widehat{\phi} \circ \phi(P) = 3P$, and for all $\widehat{P} \in \widehat{E}$ we have $\phi \circ \widehat{\phi}(\widehat{P}) = 3\widehat{P}$.

It follows from the definition that ϕ is an isogeny from E to $\widehat{E}$, and that $\widehat{\phi}$ is its dual isogeny. Since ϕ is separable and kernels have three elements, these maps are called 3-isogenies.

By Theorem 4.3.5, clearly $\widehat{\phi} : \widehat{E}(\overline{\mathbb{Q}}) \to E(\mathbb{Q})$ is surjective. But when $\widehat{\phi}$ is restricted to $\widehat{E}(\mathbb{Q})$ the image $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ is as follows:

PROPOSITION 4.5.3. *[Cohen, 2008] Let* $I = \widehat{\phi}(\widehat{E}(\mathbb{Q}))$ *be the image of* $\widehat{E}(\mathbb{Q})$ *in* $E(\mathbb{Q})$ *under the map* $\widehat{\phi}$, *then,*

(i) $\mathcal{O} \in I$, *and* $\pm T \in I$ *if and only if* D *is a square and* $D/(2b)$ *is a cube in* $\mathbb{Q}^*$.

(ii) a general point $P = (x,\ y) \in E(\mathbb{Q})$ *different from* $\pm T$ *belongs to* I *if and only if there exists* $\beta \in K = \mathbb{Q}(\sqrt{D})$ *such that* $\beta^3 = y - (ax+b)\sqrt{D}$.

4.6 THE 3-DESCENT MAP

Let $K = \mathbb{Q}(\sqrt{D})$ where D is a squarefree integer be a quadratic field. Then the 3-torsion point $T = (0,\ b\sqrt{D}) \in K$. The image of $\widehat{\phi}$ restricted to $\widehat{E}(\mathbb{Q})$ consists of points $(x,\ y) \in E(\mathbb{Q})$ such that $y - (ax+b)\sqrt{D}$ is a cube in K. Hence we can define a map from $E(\mathbb{Q})$ to K^*/K^{*3} as follows:

DEFINITION 4.6.1. *The* 3*-descent map* α *from the group* $E(\mathbb{Q})$ *to the multiplicative group* K^*/K^{*3} *where* $T \notin E(\mathbb{Q})$ *is as follows:*

$$\alpha(P) = \begin{cases} (y - (ax+b)\sqrt{D})\ K^{*3}, & \textit{if} \quad P = (x,\ y) \\ K^{*3}, & \textit{if} \ \ P = \mathcal{O}. \end{cases}$$

The properties of the α map is given in the following proposition:

PROPOSITION 4.6.1. *[Cohen, 2008]*

(i) The 3-descent map α *is a group homomorphism.*

(ii) The kernel of α *is equal to* $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$.

(iii) The map α *induces an injective group homomorphism from* $E(\mathbb{Q})/\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ *to the subgroup of* K^*/K^{*3} *of elements whose norm is trivial in* $\mathbb{Q}^*/\mathbb{Q}^{*3}$ *when* $\sqrt{D} \notin \mathbb{Q}$.

Proof. (i) If $P = (x,y)$, then $\alpha(P) = \alpha((x,-y)) = -y - (ax+b)\sqrt{D}K^{*3}$. Thus $\alpha(P)\alpha(-P) = -(y^2 - D(ax+b)^2)K^{*3} = (-x)^3 \in \mathbb{Q}^{*3}$. So, α sends inverses to inverses. Thus it is safficient to show that if $P_1 + P_2 + P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in K^{*3}$. This is because once we know this, then $\alpha(P_1 + P_2) = \alpha(-P_3) = [\alpha(P_3)]^{-1} = \alpha(P_1)\alpha(P_2)$.

If one of the P_i is $\mathcal{O}$ case is already treated. Let us consider the general case where none of the P_i's are equal to $\mathcal{O}$. Let $y = kx + n$ be the equation of the line passing through the points $P_i = (x_i,\ y_i)$. Then x_i are the three roots of the polynomial $f(x) = x^3 + D(ax+b)^2 - (kx+n)^2$. Thus

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \prod_i (y_i - (ax_i+b)\sqrt{D}) = \prod_i (kx_i+n-(ax_i+b)\sqrt{D}) = (n-b\sqrt{D})^3 \in K^3.$$

Hence α is a group homomorphism.
(ii) By definition, clearly $\mathcal{O}$ is in the kernel of α. A point $P = (x, y) \neq \mathcal{O},\ T$ is in the kernel of α if and only if there exists $\gamma \in K^*$ such that, $y - (ax+b)\sqrt{D} = \gamma^3$ hence by Proposition 4.5.3 if and only if $P \in I$.
(iii)As α is a group homomorphism with kerα as $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$. Thus we have an injective map $\overline{\alpha}$ from $E(\mathbb{Q})/\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ to K^*/K^{*3}. If $T \notin E(\mathbb{Q})$ and for $P = (x, y) \neq \mathcal{O} \in E(\mathbb{Q})$ we have $N(\alpha(P)) = x^3$ is a cube in $\mathbb{Q}^*$. □

Now to prove the weak Mordell-Weil theorem we require following lemma:

LEMMA 4.6.2. *Let A and B be abelian groups with respect to addition. Let ϕ from A to B and $\widehat{\phi}$ from B to A be two group homomorphisms. Suppose the indices $[B : \phi(A)]$ and $[A : \widehat{\phi}(B)]$ are finite. Then the index $[A : \widehat{\phi} \circ \phi(A)]$ is also finite, and*

$$[A : \widehat{\phi} \circ \phi(A)] \mid [A : \widehat{\phi}(B)][B : \phi(A)].$$

PROPOSITION 4.6.3. *[Cohen and Pazuki, 2009] Let $E : y^2 = x^3 + D(ax+b)^2$ and $\widehat{E} : y^2 = x^3 - 3D(ax + (27b - 4a^3D)/9)^2$ be 3- isogenous elliptic curves as above, and let α and $\widehat{\alpha}$ be the corresponding 3-descent maps. Then $|Im(\alpha)||Im(\widehat{\alpha})|= 3^{r+\delta}$, where r is the rank of E (and of $\widehat{E}$), and $\delta = 1$ if $D = 1$ or $D = -3$ and $\delta = 0$ otherwise.*

Applying Lemma 4.6.2 with $A = E(\mathbb{Q})$, $B = \widehat{E}(\mathbb{Q}), \phi$ and $\hat{\phi}$ as in Proposition 4.5.2 we get $\hat{\phi} \circ \phi(E(\mathbb{Q})) = 3E(\mathbb{Q})$. Also, $[E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))] =\mid \mathrm{Im}(\alpha) \mid$ and $[\widehat{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] =\mid \mathrm{Im}(\widehat{\alpha}) \mid$. Both are finite by Proposition 4.6.3. Hence by Lemma 4.6.2 we have $E(\mathbb{Q})/3E(\mathbb{Q})$ is finite.

In order to apply the descent theorem we need to define height function on $E(\mathbb{Q})$, given below:

DEFINITION 4.6.2. *Let $a = u/v \in \mathbb{Q}$ be a rational number with $gcd(u, v) = 1$. Then the height of a, denoted by $H(a)$, is defined by*

$$H(a) = max(\mid u \mid, \mid v \mid)$$

DEFINITION 4.6.3. *Let E be an elliptic curve over $\mathbb{Q}$. The height function on $E(\mathbb{Q})$ is defined as*

$$h : E(\mathbb{Q}) \longrightarrow \mathbb{R},$$

$$h(P) = \begin{cases} logH(x(P)) & if \quad P = (x, y) \neq \mathcal{O} \\ 0, & if \;\; P = \mathcal{O}. \end{cases}$$

This is the height function which will satisfy all the properties of the descent Theorem 4.4.4. Thus, by the above proposition it is clear that to compute the rank it is sufficient to compute the cardinality of Im(α) and of Im($\widehat{\alpha}$).
As in the case of 2-descent there is no algorithm to find Im(α) and Im($\widehat{\alpha}$) as there is obstruction due to nontrivial 3-part of the Tate-Shafarevich group of E. But the method works in many cases. For the proof of the above proposition as well as for the method to find the cardinality of Im(α) and of Im($\widehat{\alpha}$) we refer to [Cohen and Pazuki, 2009].

Chapter 5

RELATION BETWEEN IMAGINARY QUADRATIC FIELDS AND ELLIPTIC CURVES VIA 3-DESCENT

5.1 INTRODUCTION

The arithmetic of elliptic curves is well known and there is a well known analogy between elliptic curve and number fields. In this analogy, the group of K-rational points on an elliptic curve corresponds to the unit group of the number field K, and the Tate-Shafarevich group is the analog of the ideal class group of K. A conic is a plane affine curve of degree 2. The conic $\mathcal{P} : Q_0(y, z) = 1$ associated to the principal quadratic form of discriminant Δ,

$$Q_0(y,z) = \begin{cases} y^2 - \dfrac{\Delta}{4}z^2, & \text{if } \Delta \equiv 0 \ (mod\ 4) \\ y^2 + yz + \dfrac{1-\Delta}{4}z^2, & \text{if } \Delta \equiv 1 \ (mod\ 4) \end{cases}$$

is called the Pell conic of discriminant Δ. Franz Lemmermeyer gave an extremely close analogy between the arithmetic of Pell conics and of elliptic curves. In particular he has considered conics as group of integral points in the affine curve $Q_0(y, z) = 1$. He has proved many general results of elliptic curves such as theory of 2-descent, Selmer and Tate-Shafarevich group, Birch and Swinnerton-Dyer conjecture to Pell conics. For further reading refer to series of articles in [Lemmermeyer, 2003b][Lemmermeyer, 2003a]. Later in [Hambleton and Lemmermeyer, 2011] he and Sam Hambleton generalized their study to the arithmetics of Pell surfaces: $Q_0(y, z) = x^n$.

Let m be a cubefree integer, let $K = \mathbb{Q}(\omega)$ with $\omega^3 = m$ denote the pure cubic field. Let E_m denote the elliptic curve $y^2 = x^3 - m$. Let $E_m(\mathbb{Q})$ be the group of rational points on E_m. Any element in $E_m(\mathbb{Q})$ is of the form $(\frac{r}{t^2}, \frac{s}{t^3})$ where $\gcd(r,t) = \gcd(s,t) = 1$. Let $Cl(K)[2]$ be the group of ideal classes of order dividing 2 in K. A method to obtain a quadratic unramified extension of K where m is of the form $a^3 + 3$, with $a \equiv 2 \pmod 4$ just by using rational points on E_m is given in [Lemmermeyer, 2012] and [Lemmermeyer, 2013]. Also in [Lemmermeyer, 2013] using class field theory, he explained why the class number of K is even when $m = 8b^3 + 3$ and b is odd.

While proving the above result he observed following interesting result:

If $P = (\frac{r}{t^2}, \frac{s}{t^3})$, such that $\gcd(r,t) = 1$ is a rational point on the elliptic curve E_m, with $m \not\equiv 0, \pm 1 (\text{mod } 9)$, then the ideal $(r - t^2\omega)$ is the square of an ideal, say $(r - t^2\omega)$ $= \mathfrak{a}^2$ and the map $\kappa : E_m(\mathbb{Q}) \to Cl(K)[2]$ such that $P \longmapsto [\mathfrak{a}]$ is a homomorphism.

Later in [Lemmermeyer, 2012], the above result is proved.

In the same paper, following interesting questions are posed:

- Let $P = (x, y)$ with $y = s/t^3$ is a rational point on the elliptic curve $E_m : y^2 = x^3 - m$. Is the map sending P to the ideal class $[\mathfrak{b}]$, where $\langle s + t^3\sqrt{-m}\rangle = \mathfrak{b}^3$ a homomorphism from $E_m(\mathbb{Q})$ to the 3- part of the class group $\mathrm{Cl}(F)[3]$ of the quadratic field $F = \mathbb{Q}(\sqrt{-m})$?

- Is there any relation between above map with the homomorphism given in [Soleng, 1994] from group of rational points on elliptic curves to the class groups of certain quadratic number fields?

- How is this map related to the group structure on Pell surfaces $y^2 + mz^2 = x^3$ studied in [Hambleton and Lemmermeyer, 2011].

In this Chapter we have answered the above questions.

Let $S_n : y^2 + mz^2 = x^n$ with $n \geq 2$, a fixed integer, be a Pell surface. In an interesting paper [Hambleton and Lemmermeyer, 2011] it is shown that with respect to a binary operation defined on the primitive integral points of S_n, denoted by $S_n(\mathbb{Z})$, it forms an abelian group. They have also shown that there is a surjective homomorphism $\psi : S_n(\mathbb{Z}) \longrightarrow Cl^+(F)[n]$, the n-torsion subgroup of the narrow class group of the quadratic field $F = \mathbb{Q}(\sqrt{\Delta})$, where Δ is a fundamental discriminant, more generally $S_n : y^2 + \sigma yz + \frac{\sigma - \Delta}{4} z^2 = x^n$ and σ is the remainder of the discriminant Δ modulo 4. In the case we study $\sigma = 0$ and $\Delta < 0$.

On the other hand some questions about the class number of a quadratic field are related to solutions of Diophantine equations. For example it is well known that the study of integer solutions to the Diophantine equation

$$X^2 - \Delta Y^2 = 4Z^n, \quad \gcd(X, Z) = 1, \ \ \Delta = \text{a fundamental discriminant}, \tag{5.1}$$

gives rise to a quadratic number field with class number divisible by n. For each integral point (X, Y, Z), there is a corresponding ideal $\mathfrak{a} = \langle \frac{X+Y\sqrt{\Delta}}{2}, Z \rangle$ in the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$ such that $\mathfrak{a}^n = \langle \frac{X+Y\sqrt{\Delta}}{2} \rangle$. Hence it generates an ideal class of order dividing n. Likewise several authors have related rational points on elliptic curves and ideal classes of quadratic fields, see [Buell, 1976], [Buell, 1977] and [Soleng, 1994].

5.2 QUADRATIC FIELDS

Let m be a squarefree positive integer and $-m \equiv 2, 3 (\text{mod } 4)$. Let $K = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field. Any element of this field is of the form $a + b\omega$, where $\omega = \sqrt{-m}, \quad a, b \in \mathbb{Q}$ and its norm is $N(a+b\omega) = a^2 + mb^2$. Let $\mathfrak{O}_K$ denote the ring of algebraic integers of K. An element $\alpha \in \mathfrak{O}_K$ is primitive if $p \nmid \alpha$ for every rational prime $p \in \mathbb{N}$.

5.3 ELLIPTIC CURVES

Let $E_m : y^2 = x^3 - m$ be the associated elliptic curve. Such a curve has discriminant $\Delta(E) = -2^4 3^3 m^2$, j-invariant $j(E) = 0$ and has complex multiplication by the ring of integers of $\mathbb{Q}(\frac{1+\sqrt{-3}}{2})$. It is well known that the set of rational points on it forms a finitely generated abelian group denoted as $E_m(\mathbb{Q})$. Any rational point on E_m is of the form $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ where $r, s, t \in \mathbb{Z}$ with $\gcd(r, t) = \gcd(s, t) = 1$. For standard definitions and results on elliptic curves,we refer to [Silverman and Tate, 1992] and [Silverman, 2009].

5.4 BINARY QUADRATIC FORMS

A binary quadratic form is a homogeneous polynomial of degree 2 in two variables given by $Q_0(y, z) = ay^2 + byz + cz^2$. If the coefficients a, b, c are integers, then it is called an integral binary quadratic form. The quadratic form $Q_0(y, z)$ is said to be primitive if $\gcd(a, b, c) = 1$. Binary quadratic forms come naturally from quadratic fields. Let $F = \mathbb{Q}(\sqrt{\Delta})$ be any quadratic field of discriminant Δ. Then

$$Q_0(y,z) = \begin{cases} y^2 - \dfrac{\Delta}{4}z^2, & \text{if } \Delta \equiv 0 \ (mod\ 4) \\ y^2 + yz + \dfrac{1-\Delta}{4}z^2, & \text{if } \Delta \equiv 1 \ (mod\ 4) \end{cases}$$

is the canonical principal binary quadratic form associated with F.

Let $K = \mathbb{Q}(\sqrt{-m})$ with $m > 0$, $-m \equiv 2, 3 \,(\text{mod } 4)$, discriminant : $-4m$, m squarefree. $(\bigstar)$

From here on we will always use K to mean a quadratic field satisfying the conditions of $(\bigstar)$ Thus, the binary quadratic form associated with the quadratic field K is $Q_0(y,z) = y^2 + mz^2$.

5.5 PELL SURFACES

An equation of the form $S_n : Q_0(y,z) = x^n$ with $n \geq 2$, a fixed integer, defines a Pell Surface. The Pell surface associated with the quadratic field K will be denoted as $S_n : y^2 + mz^2 = x^n$, and we are interested in the Pell surfaces with $n = 3$, i.e., $S_3 : y^2 + mz^2 = x^3$.

Let

$$E_m : y^2 = x^3 - m \tag{5.2}$$

be the associated elliptic curve of K. From now E_m denotes the elliptic curve (5.2).

An integral point (x,y,z) satisfying $S_n : Q_0(y,z) = x^n$ is said to be primitive if $x, y, z \in \mathbb{Z}$ with $\gcd(y,z) = 1$. The set $S_n(\mathbb{Z})$ denotes the primitive integral points of the surface S_n. A correspondence between integral points in $S_n(\mathbb{Z})$ and integral solutions to the Diophantine equation (5.1) which in fact is a bijection, is given in [Hambleton and Lemmermeyer, 2011]:

$$(X,Y,Z) = \begin{cases} (2y, z, x), & \text{if } \ \Delta = 4m \\ (2y+z, z, x), & \text{if } \ \Delta = 4m+1 \end{cases}$$

Let $\mathfrak{O}_K^*$ denote the nonzero elements of the ring of integers $\mathfrak{O}_K$ of K. For the quadratic field K an algebraic integer may be written as $y + z\sqrt{-m}$ and there is a natural map $\pi_0 : S_n(\mathbb{Z}) \to \mathfrak{O}_K^*$ defined by $\pi_0(x,y,z) = y + z\sqrt{-m}$. Let $\mathbb{N}^n = \{\alpha^n \mid \alpha \in \mathbb{N}\}$. Then the set $\mathfrak{O}_K^*/\mathbb{N}^n$ forms a group with respect to coset multiplication: the identity element is $1\mathbb{N}^n$, the inverse of $\alpha\mathbb{N}^n$ is $\frac{1}{\alpha} \mid N(\alpha) \mid^n \mathbb{N}^n$. The norm map induces a group homomorphism $N : \mathfrak{O}_K^*/\mathbb{N}^n \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*n}$ defined as $N(\alpha\mathbb{N}^n) = N(\alpha)\mathbb{Z}^{*n}$, where $\mathbb{Z}^{*n}$ denotes the set of nonzero integer n-th powers. As we make use of some results from [Hambleton and Lemmermeyer, 2011] in the course of proving our results they are stated below for the sake of clarity and completeness.

LEMMA 5.5.1. *Let $\alpha \in \mathfrak{O}_K^*$. If $N(\alpha) = a^n$ for some $n \geq 2$, then α is primitive if and only if $\langle\alpha\rangle + \langle\alpha'\rangle = \langle 1\rangle$.*

LEMMA 5.5.2. *Let α be a primitive element. If $\alpha\mathbb{N}^n \in Ker\ N$, then $\langle\alpha\rangle = \mathfrak{a}^n$ is an n^{th} ideal power.*

THEOREM 5.5.3. *The cosets of primitive elements in the kernel of the norm map $N : \mathfrak{O}_K^*/\mathbb{N}^n \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*n}$ form a subgroup Π_n of $\mathfrak{O}_K^*/\mathbb{N}^n$.*

THEOREM 5.5.4. *The map $\pi : S_n(\mathbb{Z}) \longrightarrow \Pi_n$ defined by $\pi(x, y, z) = (y + z\sqrt{-m})\mathbb{N}^n$ is bijective; thus $S_n(\mathbb{Z})$ becomes an abelian group by transport of structure.*

DEFINITION 5.5.1. *For (x_1, y_1, z_1), $(x_2, y_2, z_2) \in S_n(\mathbb{Z})$ the group law on $S_n(\mathbb{Z})$ defined as $(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_3, y_3, z_3)$ where*

$$(x_3, y_3, z_3) = \Big(\frac{x_1x_2}{e^2}, \frac{y_1y_2 + \frac{\Delta-\sigma}{4}z_1z_2}{e^n}, \frac{y_1z_2 + y_2z_1 + \sigma z_1z_2}{e^n}\Big)$$

and

$$gcd\Big(y_1y_2 + \frac{\Delta - \sigma}{4}z_1z_2,\ y_1z_2 + y_2z_1 + \sigma z_1z_2\Big) = e^n,\quad \sigma \in \{0, 1\} \textit{is defined as } \Delta = 4m + \sigma.$$

In the case $\Delta = -4m$, the group law is

$$(x_3, y_3, z_3) = \Big(\frac{x_1x_2}{e^2}, \frac{y_1y_2 - mz_1z_2}{e^n}, \frac{y_1z_2 + y_2z_1}{e^n}\Big) \text{ and } \sigma = 0,$$

where

$$\gcd(y_1y_2 - mz_1z_2,\ y_1z_2 + y_2z_1) = e^n.$$

PROPOSITION 5.5.5. *The map $\psi : S_n(\mathbb{Z}) \to Cl^+(F)[n]$ given by $\psi(x, y, z) = [\mathfrak{a}]$ where $\langle y + z\omega\rangle = \mathfrak{a}^n$ is a surjective group homomorphism where $\omega = \frac{\sigma+\sqrt{\Delta}}{2}$ and $\sigma \in \{0, 1\}$.*

For proofs see [Hambleton and Lemmermeyer, 2011] .

5.6 RELATION BETWEEN QUADRATIC FIELDS, ELLIPTIC CURVES AND PELL SURFACES

As before E_m denotes the elliptic curve

$$y^2 = x^3 - m. \tag{5.3}$$

On the elliptic curve E_m, points $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ and $\left(\frac{r}{(-t)^2}, \frac{-s}{(-t)^3}\right)$ are the same and similarly the points $\left(\frac{r}{t^2}, \frac{-s}{t^3}\right)$ and $\left(\frac{r}{(-t)^2}, \frac{s}{(-t)^3}\right)$ are also identical. So, by taking $s > 0$, we see that all rational points on E_m are considered. Hence

$$E_m(\mathbb{Q}) = \left\{\left(\frac{r}{t^2}, \frac{s}{t^3}\right) \text{ such that } r, t, s \in \mathbb{Z},\ s > 0,\ \gcd(r,t) = \gcd(s,t) = 1\right\} \cup \left\{\mathcal{O}\right\}$$

where $\mathcal{O}$ is the point at infinity.
On substituting $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ in E_m we get,

$$s^2 + mt^6 \quad = \quad r^3. \tag{5.4}$$

On the Pell surface $S_3 : y^2 + mz^2 = x^3$ when $z = 1$, we obtain integer points of the elliptic curve E_m. The set of all primitive integral points on S_3 will be denoted by $S_3(\mathbb{Z})$. Comparing with equation (5.4), we see that points on the elliptic curve E_m correspond to integral points on the Pell surface S_3 in a natural way, by the map

$$f : E_m(\mathbb{Q}) \longrightarrow S_3(\mathbb{Z})$$

$$f(P) = \begin{cases} (1,1,0), & \text{if} \quad P = \mathcal{O} \\ (r, s, t^3), & \text{if} \quad P = \left(\dfrac{r}{t^2}, \dfrac{s}{t^3}\right) \end{cases} \tag{$\spadesuit$}$$

It is clear that this map is well-defined. As $\gcd(s,t) = 1$, integral points (r, s, t^3) on S_3 coming from the elliptic curve are all primitive integral points. Denote the image, $f(E_m(\mathbb{Q}))$, as $S_3^E(\mathbb{Z})$. Clearly $S_3^E(\mathbb{Z}) \subseteq S_3(\mathbb{Z})$. Also, any point $(r, s, t^3) \in S_3^E(\mathbb{Z})$ gives an integral solution $(2s, t^3, r)$ of (5.1) with $n = 3$.
Again from (5.4) we note that $r^3 =$ Norm of $(s + t^3\sqrt{-m})$ in $\mathfrak{O}_K$. So, it is natural to consider the map $g : E_m(\mathbb{Q}) \longrightarrow \mathfrak{O}_K$ defined by

$$g(P) = \begin{cases} 1, & \text{if} \quad P = \mathcal{O} \\ s + t^3\sqrt{-m}, & \text{if} \quad P = \left(\dfrac{r}{t^2}, \dfrac{s}{t^3}\right) \end{cases}$$

As discussed earlier, by considering $s > 0$, the map g is also well defined. Denote $g(E_m(\mathbb{Q}))$ as H^E.

Now we prove that elements in H^E are all primitive in $\mathfrak{O}_K$. For this it is sufficient to show that for $\alpha \in H^E$, ideals $\langle\alpha\rangle$ and $\langle\alpha'\rangle$ are coprime in $\mathfrak{O}_K$ where α' is the conjugate of α. Then, by Lemma 5.5.1, elements in H^E are primitive. We prove this below:

LEMMA 5.6.1. *Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a rational point on E_m for a squarefree positive integer m, and $-m \not\equiv 1(\text{mod } 4)$. Assume, as before, $gcd(r,t) = gcd(s,t) = 1$. Then the ideals $\langle\alpha\rangle$ and $\langle\alpha'\rangle$ are co-prime in $\mathfrak{O}_K^*$, where $\alpha = g(P) = s + t^3\sqrt{-m}$ and $\alpha' = g(-P) = s - t^3\sqrt{-m}$.*

Proof. Let $\alpha = s + t^3\sqrt{-m}$ and $\alpha' = s - t^3\sqrt{-m}$. Let $\mathfrak{p}$ be a prime ideal such that

$$\mathfrak{p}|\langle s + t^3\sqrt{-m}\rangle, \quad \mathfrak{p}|\langle s - t^3\sqrt{-m}\rangle.$$

Hence

$$s + t^3\sqrt{-m} \in \mathfrak{p}, \quad s - t^3\sqrt{-m} \in \mathfrak{p}.$$

Thus $\mathfrak{p}$ divides the sum $2s$. This implies $\mathfrak{p}|2$ or $\mathfrak{p}|s$. Also,

$$2t^3\sqrt{-m} = (s + t^3\sqrt{-m}) - (s - t^3\sqrt{-m}) \in \mathfrak{p}$$

and so

$$2t^3(-m) = \sqrt{-m}(2t^3\sqrt{-m}) \in \mathfrak{p}.$$

If $\mathfrak{p}|s$, as $\gcd(s,t) = 1$, $\mathfrak{p}$ must divide $2m$. Suppose $\mathfrak{p}$ divides m and s; then it also divides r, as $s^2 + t^6 m = r^3$. Also norm of $\mathfrak{p}$ divides both r and s. Hence the square of the norm divides $r^3 - s^2 = mt^6$. As $\gcd(s,t) = 1$, the square of the norm divides m, a contradiction since m is squarefree.

So, the only possibility for the prime ideal $\mathfrak{p}$ is either it is above 2 or $\mathfrak{p} = \langle 1\rangle$. Suppose $\mathfrak{p}$ is an ideal above 2, then $\mathfrak{p}|N(\alpha) = r^3$. Thus $2|r$. We have $s^2 \equiv 0, 1 \pmod 4$, $-m \equiv 2, 3 \pmod 4$. This implies $r^3 = s^2 - (-m)t^6 \equiv 1, 2, 3 \pmod 4$. But $r^3 \equiv 1, 3 \pmod 4$ $\Rightarrow r \equiv 1 \pmod 2$. Thus r is odd, a contradiction. Hence $\langle\alpha\rangle$ and $\langle\alpha'\rangle$ are coprime. □

Now we show that $\alpha \in H^E$ has an interesting property by using Lemma 5.5.2 : $\langle\alpha\rangle$ is a cube of an ideal in $\mathfrak{O}_K$.

THEOREM 5.6.2. *Let m be a squarefree positive integer with $-m \not\equiv 1(\text{mod } 4)$. Let $K = \mathbb{Q}(\sqrt{-m})$ and $E_m : y^2 = x^3 - m$ be the corresponding elliptic curve. For any*

$P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \in E_m(\mathbb{Q}) \setminus \mathcal{O}$, with gcd$(r,t) =$ gcd$(s,t) = 1$, the ideal $\langle s + t^3\sqrt{-m}\rangle$ is the cube of an ideal, i.e., $\langle s + t^3\sqrt{-m}\rangle = \mathfrak{a}^3$.

Proof. Let $\alpha = s + t^3\sqrt{-m} \in H^E$. Then $N(\alpha) = r^3$ by equation (5.4). As before the norm map induces a group homomorphism $N : \mathfrak{O}_K^*/\mathbb{N}^3 \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*3}$ defined as $N(\alpha\mathbb{N}^3) = N(\alpha)\mathbb{Z}^{*3}$. The kernel of this map is

$$\begin{aligned} \mathit{ker}\ N &= \{\alpha\mathbb{N}^3 \text{ such that } N(\alpha)\mathbb{Z}^{*3} = \mathbb{Z}^{*3}\}, \\ &= \{\alpha\mathbb{N}^3 \text{ such that } N(\alpha) \in \mathbb{Z}^{*3}\}. \end{aligned}$$

Let $\Pi_3^E = \{\alpha\mathbb{N}^3 \text{ such that } \alpha \in H^E\}$. Clearly $\Pi_3^E \subseteq \ker N$. Also by Lemmas 5.6.1 and 5.5.1, α is primitive, and so by Lemma 5.5.2, the ideal $\langle\alpha\rangle = \mathfrak{a}^3$ is the cube of an ideal. □

In [Hambleton and Lemmermeyer, 2011] it is shown that $S_3(\mathbb{Z})$ is an abelian group with respect to the binary operation given in Definition 5.5.1. Observe that the neutral element of $S_3(\mathbb{Z})$ is $(1,1,0)$. Similarly the inverse of $(x,y,z) \in S_3(\mathbb{Z})$ is given as

$$-(x,y,z) = \begin{cases} (x,y,-z), & \text{if} \quad x > 0 \\ (x,-y,z), & \text{if} \ \ x < 0. \end{cases}$$

In fact, the identity $(1,1,0) \in S_3^E(\mathbb{Z})$ as this corresponds to the point at infinity on the elliptic curve E_m. Also, for $(r,s,t^3) \in S_3^E(\mathbb{Z})$, the inverse point is $(r,\ s,\ -t^3)$, since we must have $r > 0$, because $s^2 = r^3 - mt^6 > 0$ and $m > 0$. This coincides with the inverse $\left(\frac{r}{t^2}, \frac{s}{-t^3}\right)$ of the point $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ of $E_m(\mathbb{Q})$. Thus, the set $S_3^E(\mathbb{Z})$ has the identity, and every element in it has an inverse with respect to the binary operation $\oplus$ of $S_3(\mathbb{Z})$. However, with this binary operation the set $S_3^E(\mathbb{Z})$ is **not** a group. We illustrate it with the following example:

EXAMPLE 6. *For $m = 26$, $E_{26} : y^2 = x^3 - 26$. The two points $P = (3,1)$ and $Q = (35,207)$ on E_{26} correspond to $(3,1,1)$ and $(35,207,1)$ respectively in $S_3^E(\mathbb{Z})$. The discriminant of $K = \mathbb{Q}(\sqrt{-26})$ is equal to -104. Thus the group law on the Pell surface S_3 corresponding to this discriminant is*

$$(x_1,y_1,z_1) \oplus (x_2,y_2,z_2) = \left(\frac{x_1x_2}{e^2}, \frac{y_1y_2 - 26z_1z_2}{e^3}, \frac{y_1z_2 + y_2z_1}{e^3}\right)$$

where

$$\mathit{gcd}(y_1y_2 - 26z_1z_2,\ y_1z_2 + y_2z_1) = e^3.$$

Therefore

$$\begin{aligned}(3,1,1)\oplus(35,207,1) &= \left(\tfrac{3\times 35}{e^2}, \tfrac{1\times 207-26\times 1\times 1}{e^3}, \tfrac{1\times 1+207\times 1}{e^3}\right)\\ &= (105,181,208) \textit{ since } \ gcd(181,208)=1.\end{aligned}$$

This shows that $S_3^E(\mathbb{Z})$ is ***not*** *closed under the binary operation $\oplus$ of $S_3(\mathbb{Z})$. Clearly $(105,181,208)\in S_3(\mathbb{Z})$ but $(105,181,208)\notin S_3^E(\mathbb{Z})$. Hence $S_3^E(\mathbb{Z}) \subsetneq S_3(\mathbb{Z})$.*

Let F be any quadratic field. An element $\beta \in F$ is said to be totally positive if $N(\beta) > 0$. Let P_F^+ be the group of principal fractional ideals $\langle\beta\rangle = \beta\mathfrak{O}_F$ where $N(\beta) > 0$. The quotient group I_F/P_F^+ is called the narrow class group $Cl^+(F)$ of F. For imaginary quadratic fields, the norm of any element is positive, thus the class group and the narrow class group are identical. The collection of ideal classes of order dividing n in F forms a subgroup of $Cl(F)$ and is called the $n-$part of the ideal class group, denoted as $Cl(F)[n]$.

By applying Proposition 5.5.5 to $S_3(\mathbb{Z})$ and the field K we get a surjective homomorphism ψ from $S_3(\mathbb{Z})$ to $Cl(K)[3]$.

Consider the diagram

$$\begin{tikzcd} E_m(\mathbb{Q}) \arrow[d, "f"'] & \\ S_3(\mathbb{Z}) \arrow[r, "\psi"'] & Cl(K)[3] \end{tikzcd}$$

Here f is as defined in (♠) and ψ is the surjective homomorphism defined in §2 (Proposition 5.5.5). We note that f is injective but not a homomorphism since $f(E_m(\mathbb{Q})) = S_3^E(\mathbb{Z})$ is not a subgroup of $S_3(\mathbb{Z})$. Also, the image of f is not equal to the kernel of ψ. The following example illustrates it.

EXAMPLE 7. *Let $K = \mathbb{Q}(\sqrt{-53})$ and $E_{53} : y^2 = x^3 - 53$, where $-53 \not\equiv 1 (mod\ 4)$. Let $P = (29,156) \in E_{53}(\mathbb{Q})$. Then $f(P) = (29,156,1) \in f(E_{53}(\mathbb{Q}))$. However, $\psi(f(P)) = \langle 156+\sqrt{-53}\rangle = \mathfrak{b}^3$, where $\mathfrak{b} = \langle 29, 11+\sqrt{-53}\rangle$. We show that the ideal $\langle 29, 11+\sqrt{-53}\rangle$ in $\mathfrak{O}_K$ is not a principal ideal. Say $\langle 29, 11+\sqrt{-53}\rangle = \langle\beta\rangle$. Then, since $29 \in \langle 29, 11+\sqrt{-53}\rangle$ we have $29 \in \langle\beta\rangle$, so $\beta|29$ in $\mathfrak{O}_K$. Writting $29 = \beta\gamma$ in $\mathfrak{O}_K$ and taking norms, we have $841 = 29^2 = N(\beta)N(\gamma)$ in $\mathbb{Z}$. So, $N(\beta)|841$ in $\mathbb{Z}$.*

Similarly, since $11+\sqrt{-53} \in \langle\beta\rangle$ *we get* $N(\beta)|174$ *in* $\mathbb{Z}$*. Thus* $N(\beta)$ *is a common divisor of* 841 *and* $174 = 29 \cdot 6$ *in* $\mathbb{Z}$*. So,* $N(\beta)$ *is* 1 *or* 29*. Since* $N(\beta) = a^2 + 53b^2$ *where* a*,* b *are in* $\mathbb{Z}$*,* $N(\beta) \neq 29$*. Therefore* $N(\beta) = 1$*, so* β *is a unit and* $\langle 1\rangle = \langle\beta\rangle$*. Thus* $1 \in \langle\beta\rangle$*. Hence there exist* α *and* δ *in* $\mathfrak{O}_K$ *such that* $29\alpha + (11+\sqrt{-53})\delta = 1$*. Multiplying both sides by* $11-\sqrt{-53}$*, we have* $29\{(11-\sqrt{-53})\alpha + 6\delta\} = 11-\sqrt{-53}$*, so that* 29 *divides* $11-\sqrt{-53}$ *in* $\mathfrak{O}_K$*. Thus* $N(29) = 841$ *divides* $N(11-\sqrt{-53}) = 174$ *which is a contradiction. So,* $\langle 29, 11+\sqrt{-53}\rangle$ *is not a principal ideal in* $\mathfrak{O}_K$*. Hence* $f(P)$ *is not in the kernel of* ψ*.*

5.7 A GROUP LAW ON $S_3^E(\mathbb{Z})$ FROM $E_m(\mathbb{Q})$

By using the binary operation on $E_m(\mathbb{Q})$ we define a binary operation on $S_3^E(\mathbb{Z})$ with respect to which $S_3^E(\mathbb{Z})$ becomes an abelian group. We recall that $E_m(\mathbb{Q})$ is an abelian group with respect to the group law given by the following formulae:-
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be rational points on E_m and define λ as

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if} \quad P_1 \neq P_2 \\ \dfrac{3x_1^2}{2y_1}, & \text{if} \quad P_1 = P_2 \end{cases}$$

Then $P_3 = P_1 + P_2 = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$.
The map $f : E_m(\mathbb{Q}) \longrightarrow S_3^E(\mathbb{Z})$ is as defined in (♠) and is given by

$$f(P) = \begin{cases} (1,1,0), & \text{if} \quad P = \mathcal{O} \\ (r, s, t^3), & \text{if} \quad P = \left(\dfrac{r}{t^2}, \dfrac{s}{t^3}\right) \end{cases}$$

This is indeed a bijection. Thus, by transporting the group structure of $E_m(\mathbb{Q})$ to $S_3^E(\mathbb{Z})$, the set $S_3^E(\mathbb{Z})$ becomes an abelian group. We now define the binary operation on $S_3^E(\mathbb{Z})$: Let $u_i = (r_i, s_i, t_i^3) \quad (i = 1, 2)$ be elements in $S_3^E(\mathbb{Z})$. These elements correspond to $P_i = (\frac{r_i}{t_i^2}, \frac{s_i}{t_i^3})$ on the elliptic curve E_m. We show that the sum $P_3 = P_1 + P_2$ corresponds to an element $u_3 \in S_3^E(\mathbb{Z})$, with $u_3 = u_1 * u_2$ where $*$ is defined using the group law on elliptic curves as follows :
Case I : $\frac{r_1}{t_2^2} \neq \frac{r_2}{t_2^2}$, and $\lambda = \left(\frac{s_2}{t_2^3} - \frac{s_1}{t_1^3}\right)/\left(\frac{r_2}{t_2^2} - \frac{r_1}{t_1^2}\right)$. Hence

$$\begin{aligned} x_3 &= \lambda^2 - \frac{r_1}{t_1^2} - \frac{r_2}{t_2^2} = \left(\frac{s_2 t_1^3 - s_1 t_2^3}{t_1 t_2 (r_2 t_1^2 - r_1 t_2^2)}\right)^2 - \frac{r_1}{t_1^2} - \frac{r_2}{t_2^2}, \\ y_3 &= \lambda(x_1 - x_3) - y_1 = \frac{s_2 t_1^3 - s_1 t_2^3}{t_1 t_2 (r_2 t_1^2 - r_1 t_2^2)}\left(\frac{r_1}{t_1^2} - x_3\right) - \frac{s_1}{t_1^3} \end{aligned}$$

This enables one to find $u_3 \in S_3^E(\mathbb{Z})$.
Define $S_- = s_2t_1^3 - s_1t_2^3$, $R_- = r_2t_1^2 - r_1t_2^2$, $R_+ = r_2t_1^2 + r_1t_2^2$ and $T = t_1t_2$.
On simplification and by using above notations we get

$$\begin{aligned} x_3 &= \frac{S_-^2 - R_+R_-^2}{R_-^2T^2} \\ y_3 &= \frac{R_-^2R_+S_- + T^2R_-^2(s_2r_1t_1 - s_1r_2t_2) - S_-^3}{R_-^3T^3} \end{aligned}$$

Hence (r_3, s_3, t_3^3) is given by

$$\begin{aligned} r_3 &= S_-^2 - R_+R_-^2 \\ s_3 &= R_-^2R_+S_- + T^2R_-^2(s_2r_1t_1 - s_1r_2t_2) - S_-^3 \\ t_3^3 &= R_-^3T^3, \end{aligned}$$

Case II : $\frac{r_1}{t_2^2} = \frac{r_2}{t_2^2} = \frac{r}{t^2}$, and $P = (\frac{r}{t^2}, \frac{s}{t^3})$, $\lambda = \frac{3r^2}{2st}$.
Hence

$$\begin{aligned} x_3 &= \frac{9r^4}{4s^2t^2} - \frac{2r}{t^2} = \frac{9r^4 - 8rs^2}{4s^2t^2} \\ y_3 &= \frac{3r^2}{2st}\left(\frac{r}{t^2} - \frac{9r^4 - 8rs^2}{4s^2t^2}\right) - \frac{s}{t^3} = \frac{36r^3s^2 - 27r^6 - 8s^4}{8s^3t^3} \end{aligned}$$

Thus for $u_1 = u_2 = (r, s, t^3)$ we have (r_3, s_3, t_3^3) where

$$\begin{aligned} r_3 &= 9r^4 - 8rs^2 \\ s_3 &= 36r^3s^2 - 27r^6 - 8s^4 \\ t_3^3 &= (2st)^3. \end{aligned}$$

In both the cases, certainly (r_3, s_3, t_3^3) satisfies the equation of the Pell surface S_3, but it need not be primitive.
Now, if (x, y, z) is any primitive point on the Pell surface S_3 then $(x^{'}, y^{'}, z^{'}) = (d^2x, d^3y, d^3z)$ will also lie on S_3 for any integer d. Thus, if (x, y, z) is not a primitive point, then $\gcd(x, z) = d^2$ and $\gcd(y, z) = d^3$ for some integer $d \geq 1$. Let $(r_4, s_4, t_4^3) = (r_3/d^2, s_3/d^3, t_3^3/d^3)$. Define $u_3 = (r_4, s_4, t_4^3)$.
With this binary operation, $S_3^E(\mathbb{Z})$ is an abelian group: the identity element is $(1, 1, 0)$, the inverse of (r, s, t^3) is $(r, s, -t^3)$. We illustrate it with an example:

EXAMPLE 8. *Let $E_{26} : y^2 = x^3 - 26$, $u_1 = (3, 1, 1)$ and $u_2 = (35, 207, 1)$ be in $S_3^E(\mathbb{Z})$, which correspond to the elements $P = (3, 1)$ and $Q = (35, 207)$ respectively*

in $E_{26}(\mathbb{Q})$. *Thus, we have* $r_1 = 3,\ s_1 = 1,\ t_1 = 1,\ r_2 = 35,\ s_2 = 207,\ t_2 = 1,$ *and* $S_- = 206, T = 1,\ R_- = 32,\ R_+ = 38$. *Hence* $r_3 = 3524 = 881 \cdot 2^2,\ s_3 = -125880 = -2^3 \cdot 3 \cdot 5 \cdot 1049,\ t_3^3 = 32768 = 2^{15}$. *As* (r_3, s_3, t_3^3) *is not a primitive point, we consider* $u_3 = (r_4, s_4, t_4^3) = (r_3/d^2, s_3/d^3, t_3^3/d^3) = (881, -15735, 4096)$. *Clearly* $u_3 \in S_3^E(\mathbb{Z})$. *Also* u_3 *corresponds to the rational point* $P_3 = \left(\frac{881}{256}, \frac{-15735}{4096}\right) \in E_{26}$.
Similarly for $u_1 = u_2 = (3, 1, 1)$ *we get* $r_3 = 705 = 3 \cdot 4 \cdot 47,\ s_3 = -18719,\ t_3^3 = 2^3$. *As* (r_3, s_3, t_3^3) *is a primitive point,* $u_3 = (r_3, s_3, t_3^3) = (705, -18719, 8)$. *This corresponds to* $\left(\frac{705}{4}, \frac{-18719}{8}\right) = 2P \in E_{26}(\mathbb{Q})$, *where* $P = (3, 1)$.

It is easy to see that the 3-torsion subgroup of $E_m(\overline{\mathbb{Q}})$ contains the cyclic subgroup $\mathcal{T} = \{\mathcal{O},\ (0, \sqrt{m}),\ (0, -\sqrt{m})\}$ which is invariant under the action of $\mathrm{Gal}\Big(\overline{\mathbb{Q}}/\mathbb{Q}\Big)$. Then there exists a curve $\widehat{E}$ and an isogeny $\phi : E \longrightarrow \widehat{E}$, both defined over $\mathbb{Q}$, such that Ker $(\phi) = \mathcal{T}$. Explicitly we have $\widehat{E} : \widehat{y}^2 = \widehat{x}^3 + 27m$ and $\phi(x, y) = \left(\frac{x^3-4m}{x^2}, \frac{y(x^3+8m)}{x^3}\right)$.

5.8 A HOMOMORPHISM FROM $E_m(\mathbb{Q})$ TO Cl(K)[3]

In this section we give a group homomorphism from $E_m(\mathbb{Q})$ to $Cl(K)[3]$ using 3-descent on $E_m(\mathbb{Q})$. There is a natural norm map $N : K^* \longrightarrow \mathbb{Q}^*$ given by $N(a + b\sqrt{-m}) = a^2 + b^2 m$ for $a, b \in \mathbb{Q}$. This induces a homomorphism: $K^*/K^{*3} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$, which will also be denoted by N. Let $G_3 = \{\gamma K^{*3}$ such that $N(\gamma) = t^3, t \in \mathbb{Q}^*\}$. Then ker $N = G_3$. Since $E_m : y^2 = x^3 - m$ is of the form $y^2 = x^3 + D(ax + b)^2$ with $a = 0,\ b = -1$ and $D = -m$, it has the rational 3-torsion subgroup $\mathcal{T} = \{\mathcal{O}, T, -T\}$ where $T = (0, -\sqrt{-m})$. Let $\widehat{E}_m : \widehat{y}^2 = \widehat{x}^3 + 27m$, then by Proposition 4.5.2 we get a 3-isogeny between E_m and $\widehat{E}_m$ defined by

$$\phi(P) = (\widehat{x}, \widehat{y}) = \begin{cases} \Big(\dfrac{x^3 - 4m}{x^2}, \dfrac{y(x^3 + 8m)}{x^3}\Big), & \text{if} \quad P = (x, y) \\ \mathcal{O}, & \text{if} \quad P = \mathcal{O}, T, -T. \end{cases}$$

with dual 3-isogeny as,

$$\widehat{\phi}(P) = (x, y) = \begin{cases} \Big(\dfrac{\widehat{x}^3 + 108m}{9\widehat{x}^2}, \dfrac{\widehat{y}(\widehat{x}^3 - 216m)}{27\widehat{x}^3}\Big), & \text{if} \quad P = (x, y) \\ \mathcal{O}, & \text{if} \quad P = \mathcal{O}. \end{cases}$$

Now applying 3− descent map with 3-isogeny to E_m as given in the section 4.6 we get:

LEMMA 5.8.1. *Let m be a squarefree positive integer with $-m \not\equiv 1 (mod\ 4)$. Let $K = \mathbb{Q}(\sqrt{-m})$ and let $E_m : y^2 = x^3 - m$ be the corresponding elliptic curve. Let $P = (\frac{r}{t^2}, \frac{s}{t^3}) \in E_m(\mathbb{Q})$, with $gcd(r,t) = gcd(s,t) = 1$, and $G_3 = \{\gamma K^{*3}$ such that $N(\gamma) = t^3,\ t \in \mathbb{Q}^*\}$. The map*

$$\alpha : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}, \quad \alpha : \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \longmapsto (s + t^3\sqrt{-m})K^{*3}$$

is a group homomorphism.

Proof. The 3-descent map, given in Definition 4.6.1 applied to the elliptic curve E_m is:

$$\delta : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}$$

$$\delta(P) = \begin{cases} (y + \sqrt{-m})K^{*3}, & \text{if} \quad P = (x,y) \\ K^{*3}, & \text{if} \quad P = \mathcal{O}. \end{cases}$$

Observe that $(s + t^3\sqrt{-m})K^{*3} = (\frac{s}{t^3} + \sqrt{-m})K^{*3} = (y + \sqrt{-m})K^{*3}$. By Proposition 4.6.1 the 3-descent map δ is a group homomorphism, it follows that α is a group homomorphism. □

Let $E_m : y^2 = x^3 - m$ and $\widehat{E}_m : \widehat{y}^2 = \widehat{x}^3 + 27m$. Then there exists a 3-isogeny map ϕ between E_m and $\widehat{E}_m$ given by $\phi : (x,y) \longmapsto (\frac{x^3-4m}{x^2}, \frac{y(x^3+8m)}{x^3})$ with dual isogeny as $\widehat{\phi} : \widehat{E}_m \longrightarrow E_m$ given by $\widehat{\phi} : (\widehat{x}, \widehat{y}) \longmapsto \left(\dfrac{\widehat{x}^3 + 108m}{9\widehat{x}^2}, \dfrac{\widehat{y}(\widehat{x}^3 - 216m)}{27\widehat{x}^3}\right)$.

LEMMA 5.8.2. *Let m be a squarefree positive integer with $-m \not\equiv 1 (mod\ 4)$, let $K = \mathbb{Q}(\sqrt{-m})$, $E_m : y^2 = x^3 - m$, and $\widehat{E}_m : \widehat{y}^2 = \widehat{x}^3 + 27m$. Let $P = (\frac{r}{t^2}, \frac{s}{t^3}) \in E_m(\mathbb{Q})$ with $gcd(r,t) = gcd(s,t) = 1$. There is an exact sequence of group homomorphisms*

$$\begin{tikzcd} 1 \arrow[r] & \widehat{\phi}(\widehat{E}_m(\mathbb{Q})) \arrow[r] & E_m(\mathbb{Q}) \arrow[r, "\alpha"] & \dfrac{K^*}{K^{*3}} \arrow[r, "N"] & \dfrac{\mathbb{Q}^*}{\mathbb{Q}^{*3}} \end{tikzcd}$$

where $\alpha : P \longmapsto (s + t^3\sqrt{-m})K^{*3}$ and $\widehat{\phi} : (\widehat{x}, \widehat{y}) \longmapsto \left(\dfrac{\widehat{x}^3 + 108m}{9\widehat{x}^2}, \dfrac{\widehat{y}(\widehat{x}^3 - 216m)}{27\widehat{x}^3}\right)$ with $3E_m(\mathbb{Q})$ as a proper subgroup of $\widehat{\phi}(\widehat{E}_m(\mathbb{Q}))$.

Proof. Clearly there is an exact sequence of group homomorphisms:

$$\begin{tikzcd} 1 \arrow[r] & \widehat{\phi}(\widehat{E}_m(\mathbb{Q})) \arrow[r] & E_m(\mathbb{Q}) \arrow[r, "\alpha"] & \dfrac{K^*}{K^{*3}} \arrow[r, "N"] & \dfrac{\mathbb{Q}^*}{\mathbb{Q}^{*3}} \end{tikzcd}$$

where, $\widehat{E}_m : \widehat{y}^2 = \widehat{x}^3 + 27m$ and $\widehat{\phi}$ is as given in [Cohen, 2008] (pp. 558-559),

$$\widehat{\phi}(\widehat{P}) \;=\; \Big(\frac{\widehat{x}^3 + 108m}{9\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^3 - 216m)}{27\widehat{x}^3}\Big).$$

This point satisfies $y^2 = x^3 - m$ since when we replace x with $\frac{\widehat{x}^3+108m}{9\widehat{x}^2}$ and y with $\frac{\widehat{y}(\widehat{x}^3-216m)}{27\widehat{x}^3}$ in $y^2 - x^3 + m = 0$ and factorize the result, we obtain

$$\frac{(\widehat{y}^2 - \widehat{x}^3 - 27m)(\widehat{x}^3 - 216m)^2}{729\widehat{x}^6} = 0.$$

Let us compute $3P$ on E_m, where $P = (x, y)$ and $3P \neq \mathcal{O}$.

$$\begin{aligned}
3P &= (x, y) + \Big(\frac{x^4 + 8mx}{4y^2}, \frac{x^6 - 20mx^3 - 8m^2}{8y^3}\Big), \\
&= \Big(\lambda^2 - x - \frac{x^4 + 8mx}{4y^2},\ \lambda(x - x_3) - y\Big), \text{ where} \\
\lambda &= \frac{\frac{x^6-20mx^3-8m^2}{8y^3} - y}{\frac{x^4+8mx}{4y^2} - x}, \\
\lambda &= \frac{\frac{x^6-20mx^3-8m^2}{8y^3} - y}{\frac{x^4+8mx}{4y^2} - x}, \\
&= \frac{\frac{x^6-20mx^3-8m^2-8y^4}{8y^3}}{\frac{x^4+8mx-4xy^2}{4y^2}}, \\
&= \frac{x^6 - 20mx^3 - 8m^2 - 8y^4}{2y(x^4 + 8mx - 4xy^2)}, \\
&= \frac{x^6 - 20mx^3 - 8m^2 - 8(x^3 - m)^2}{2y(x^4 + 8mx - 4x(x^3 - m))}, \\
&= \frac{x^6 - 20mx^3 - 8m^2 - 8x^6 + 16mx^3 - 8m^2}{2y(x^4 + 8mx - 4x^4 + 4mx)}, \\
&= \frac{7x^6 + 4mx^3 + 16m^2}{6xy(x^3 - 4m)}.
\end{aligned}$$

Therefore

$$\begin{aligned}
3P &= (x,y)+\Big(\frac{x^4+8mx}{4y^2},\ \frac{x^6-20mx^3-8m^2}{8y^3}\Big),\\
&= \Big(\lambda^2-x-\frac{x^4+8mx}{4y^2},\ \lambda(x-x_3)-y\Big),\\
&= \Big(\frac{x^9+96mx^6+48m^2x^3-64m^3}{9x^2(x^3-4m)^2},\ \frac{y(x^3+8m)(x^9-228mx^6+48m^2x^3-64m^3)}{27x^3(x^3-4m)^3}\Big),\\
&= \Big(\frac{p^3+108m}{9p^2},\ \frac{q(p^3-216m)}{27p^3}\Big),\ \text{where}\\
(p,q) &= \Big(\frac{x^3-4m}{x^2},\ \frac{y(x^3+8m)}{x^3}\Big)\in \widehat{E}_m(Q),\ \text{see } \textit{Cohen}\ [2008].
\end{aligned}$$

Since

$$\begin{aligned}
\ker\,\alpha &= \widehat{\phi}(\widehat{E}_m(\mathbb{Q}))\\
&= \Big\{P=\Big(\frac{\widehat{x}^3+108m}{9\widehat{x}^2},\frac{\widehat{y}(\widehat{x}^3-216m)}{27\widehat{x}^3}\Big)\in E_m(\mathbb{Q}):\widehat{y}^2=\widehat{x}^3+27m\Big\},
\end{aligned}$$

This shows that $3E_m(\mathbb{Q})\subseteq\ker\,\alpha$.
Conversely, let $P=(x,y)\in\ker\,\alpha$. Then there exist $p,q\in\mathbb{Q}$ satisfying $q^2=p^3+27m$ and

$$\begin{aligned}
x &= \frac{p^3+108m}{9p^2},\\
y &= \frac{q(p^3-216m)}{27p^3}.
\end{aligned}$$

However if we try to solve for p,q we do **not** get $(p,q)=\Big(\frac{x^3-4m}{x^2},\frac{y(x^3+8m)}{x^3}\Big)$. This shows that $3E_m(\mathbb{Q})\neq\ker\,\alpha$. □

THEOREM 5.8.3. *Let m be a squarefree positive integer with $-m\not\equiv 1(mod\ 4)$. Let $K=\mathbb{Q}(\sqrt{-m})$, and $E_m: y^2=x^3-m$ be the corresponding elliptic curve. Let $P=(\frac{r}{t^2},\frac{s}{t^3})\in E_m(\mathbb{Q})\setminus\mathcal{O}$, with $gcd(r,t)=gcd(s,t)=1$, then $\langle s+t^3\sqrt{-m}\rangle$ is the cube of an ideal, i.e., $\langle s+t^3\sqrt{-m}\rangle=\mathfrak{a}^3$, where $\mathfrak{a}=\langle r,s+t^3\sqrt{-m}\rangle$. There is a group homomorphism $\kappa: E_m(\mathbb{Q})\longrightarrow Cl(K)[3]$ defined as $\kappa(P)=[\mathfrak{a}]$, whose kernel contains $3E_m(\mathbb{Q})$.*

Proof. The first part is already proved in Theorem 5.6.2, i.e., $\langle s+t^3\sqrt{-m}\rangle=\mathfrak{a}^3$. Now, let us prove that the map κ is a group homomorphism. Let $y_{P_1}=s_1/t_1^3$, $y_{P_2}=s_2/t_2^3$ and $y_{P_3}=s_3/t_3^3$ for $P_1,P_2,P_3\in E_m(\mathbb{Q})$. Let $\langle s_1+t_1^3\omega\rangle=\mathfrak{a}^3$, $\langle s_2+t_2^3\omega\rangle=\mathfrak{b}^3$ and $\langle s_3+t_3^3\omega\rangle=\mathfrak{c}^3$, where $\omega=\sqrt{-m}$. Then $\kappa(P_1)=[\mathfrak{a}]$, $\kappa(P_2)=[\mathfrak{b}]$ and $\kappa(P_3)=[\mathfrak{c}]$. To show κ is a homomorphism we need to prove $\kappa(P_1+P_2) = [\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}][\mathfrak{b}] = \kappa(P_1)\kappa(P_2)$. This is equivalent to proving $\kappa(P_1)\kappa(P_2)\kappa(P_3) = \langle 1\rangle$ for collinear rational points $P_1, P_2, P_3 \in E_m(\mathbb{Q})$. We know by Lemma 5.8.1 that the map $\alpha : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}$ is a homomorphism. Hence, $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in K^{*3}$, i.e., $(s_1+t_1^3\omega)(s_2+t_2^3\omega)(s_3+t_3^3\omega)$ is a cube in K^*. Hence, $(s_1+t_1^3\omega)(s_2+t_2^3\omega)(s_3+t_3^3\omega) = \beta^3$(say). This gives, $\mathfrak{a}^3\mathfrak{b}^3\mathfrak{c}^3 = \langle\beta\rangle^3$. This implies $\mathfrak{a}\mathfrak{b}\mathfrak{c} = \langle\beta\rangle$. Hence $\kappa(P_1)\kappa(P_2)\kappa(P_3) = \langle\beta\rangle$, a principal ideal, the identity of $Cl(K)[3]$.

We know that $3P \in \ker\alpha$. Thus, $\alpha(3P)$ is a cube, say γ^3 for some $\gamma \in K^*$. Hence for any $P \in E_m(\mathbb{Q})$, $\kappa(3P) = [\mathfrak{b}]$ where $\mathfrak{b}$ is the principal ideal generated by γ. Hence $3E_m(\mathbb{Q}) \subseteq \ker\kappa$. □

EXAMPLE 9. *Let $K = \mathbb{Q}(\sqrt{-79})$ and $E_{79} : y^2 = x^3 - 79$, where $-m \equiv 1(mod\ 4)$. Then $E_{79}(\mathbb{Q})$ is generated by $P = (20, 89)$. The ideal $\langle 89 + \sqrt{-79}\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}^3$, where $\langle 2\rangle = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{q}$ is a prime ideal above 5. This shows that the condition $-m \not\equiv 1(mod\ 4)$ in the above theorem cannot be dropped.*

EXAMPLE 10. *Let $K = \mathbb{Q}(\sqrt{-26})$ and $E_{26} : y^2 = x^3 - 26$, where $-m \not\equiv 1(mod\ 4)$. Then $E_{26}(\mathbb{Q})$ is generated by $P = (3, 1)$ and $Q = (35, 207)$. Also $P + Q = (881/256, -15735/4096)$. Then we have $\langle 1 + \sqrt{-26}\rangle = \mathfrak{p}_3^3$, $\langle 207 + \sqrt{-26}\rangle = \mathfrak{a}^3$, $\langle -15735 + 4096\sqrt{-26}\rangle = \mathfrak{p}_{881}^3$. The ideals $\mathfrak{p}_3 = \langle(3, \sqrt{-26}+1)\rangle$ and $\mathfrak{p}_{881} = \langle(881, \sqrt{-26}+624)\rangle$ generate ideal classes of order 3, whereas the ideal $\mathfrak{a} = \langle\sqrt{-26}-3\rangle$ is principal.*

5.9 RELATION BETWEEN THE MAPS ϕ, κ AND ψ

Soleng's homomorphism given in [Soleng, 1994] applied to $E_m(\mathbb{Q})$ is $\phi : \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \mapsto [\langle r, -ks + \sqrt{-m}\rangle]$, where $kt^3 + lr = 1$. Let $\mathfrak{a} = \langle r, s + t^3\sqrt{-m}\rangle$, $\mathfrak{b} = \langle r, -ks + \sqrt{-m}\rangle$ and $\mathfrak{c} = \langle r, -ks - \sqrt{-m}\rangle$. Then $\mathfrak{c} \subseteq \mathfrak{a}$ since

$$-ks - \sqrt{-m} = -l\sqrt{-m}(r) - k(s + t^3\sqrt{-m}).$$

Also since $s + t^3\sqrt{-m} = ls(r) - t^3(-ks - \sqrt{-m})$, $\mathfrak{a} \subseteq \mathfrak{c}$. It follows that $\mathfrak{a} = \mathfrak{c}$. To show that $\mathfrak{b}\mathfrak{c}$ is principal, observe that the conjugate ideal $\bar{\mathfrak{c}} = \bar{\mathfrak{a}}$ of $\mathfrak{c} = \mathfrak{a}$ is equal to $\mathfrak{b}$. It follows that $\mathfrak{a}\mathfrak{b} = \langle N\mathfrak{a}\rangle$, the principal ideal generated by the norm of $\mathfrak{a}$, see [conrad2014factoring]. It follows that the classes of the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are inverses in the ideal class group of K. This means that the homomorphism κ and Soleng's homomorphism ϕ are quite similar. The precise relationship, when Soleng's elliptic curve is E_m, is

$$\kappa(P) = (\phi(P))^{-1}.$$

But Soleng did not show that when the elliptic curve is E_m, the image of ϕ belongs to $Cl(K)[3]$.

Similarly there is a relation between the homomorphism ψ given by Hambelton and Lemmermeyer and the homomorphism κ which is given in the following diagram:

$$\begin{tikzcd}
E_m(\mathbb{Q}) \arrow[r, "\kappa"] \arrow[d] \arrow[dr, "f"] & Cl(K)[3] \\
f(E_m(\mathbb{Q})) = S_3^E(\mathbb{Z}) \arrow[r, hook] & S_3(\mathbb{Z}) \arrow[u, "\psi"']
\end{tikzcd}$$

As shown towards the end of §3, f is not a homomorphism. However, the diagram commutes, i.e., $\psi \circ f = \kappa$.

All computations were done using Sage.

Chapter 6

CONCLUSION

In this thesis we have given a relation between imaginary quadratic fields, rational points on elliptic curves and Pell surfaces. We have shown that the collection of primitive integral points on $S_3 : y^2 + mz^2 = x^3$ coming from the elliptic curve $E_m : y^2 = x^3 - m$ do not form a group with respect to the binary operation given in [Hambleton and Lemmermeyer, 2011].The main result is: we have given a group homomorphism κ from the rational points of E_m to $Cl(K)[3]$. This is done using 3-descent on E_m.

Future Work

Let m be a cubefree integer, let $K = \mathbb{Q}(\sqrt[3]{m})$ be the pure cubic field. Let $E_m(\mathbb{Q})$ be the group of rational points on E_m. In [Lemmermeyer, 2013] and [Lemmermeyer, 2012] the Hilbert class field of the pure cubic field K and rational points on E_m are related. A method to obtain a quadratic unramified extension of K where m is of the form $a^3 + 3, \quad \text{with} \quad a \equiv 2 \pmod 4$ just by using rational points on E_m is also described. He has also explained why the class number of K is even when $m = 8b^3 + 3$ and b is odd. It is well known that $K = \mathbb{Q}(\sqrt[3]{m})$ has class number divisible by 3 when $m = p^2q$ for primes $p \equiv q \equiv 2(\text{mod } 3)$ such that $p^2q \not\equiv \pm 1(\text{mod } 9)$. We would like to work on the following question posed by him:
Is it possible to construct the $3-$ class group of a pure cubic field K of the above type from $k-$ rational points on the elliptic curves $x^3 + y^3 = m$, where $k = \mathbb{Q}(\sqrt{-3})$, the field of cube roots of unity.

References

(2013). *PARI/GP version* `2.5.5`. The PARI Group, Bordeaux. `http://pari.math.u-bordeaux.fr/`.

Alaca, Ş. and Williams, K. S. (2004). *Introductory algebraic number theory.* Cambridge University Press Cambridge.

Barbeau, E. J. (2003). *Pell's Equation.* Springer.

Bernstein, L. (1964). "Periodical continued fractions for irrationals of degree n by Jacobi's algorithm". *Journal für die reine und angewandte Mathematik*, 213, 31–38.

Bernstein, L. (1971). *The Jacobi-Perron Algorithm.* Springer.

Bernstein, L. (1972b). "A 3-dimensional periodic Jacobi-Perron algorithm of period length 8." *J. Number Theory*, 4, 48–69.

Bernstein, L. (1974). "Fundamental units from the preperiod of a generalized Jacobi-Perron algorithm." *J. Reine Angew. Math.*, 268/269, 391–409.

Bernstein, L. (1975). "Units and periodic jacobi-perron algorithms in real algebraic number fields of degree 3." *Transactions of the American Mathematical Society*, 212, 295-306.

Buell, D. A. (1976). "Class groups of quadratic fields." *Mathematics of Computation*, 30(135), 610-623.

Buell, D. A. (1977). "Elliptic curves and class groups of quadratic fields." *Journal of the London Mathematical Society*, 2(1), 19-25.

Buell, D. A. (1989). *Binary quadratic forms: classical theory and modern computations.* Springer.

Cohen, H. (2008). *Number theory: Volume I: Tools and diophantine equations.* Springer.

Cohen, H. (2013). *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media.

Cohen, H. and Pazuki, F. (2009). "Elementary 3-descent with a 3-isogeny." *Acta Arithmetica*, 140, 369-404.

Conrad, K. Factoring in quadratic fields, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf`.

Delone, B. N. and Faddeev, D. K. (1964). *The theory of irrationalities of the third degree.* Translations of Mathematical Monographs. American Mathematical Society.

Hambleton, S. (2012). "Generalized lucas-lehmer tests using pell conics." *Proceedings of the American Mathematical Society*, 140(8), 2653-2661.

Hambleton, S. and Lemmermeyer, F. (2011). "Arithmetic of Pell surfaces." *Acta Arithmetica*, 146(1), 1-12.

Hambleton, S. and Scharaschkin, V. (2012). "Pell conics and quadratic reciprocity." *Rocky Mountain Journal of Mathematics*, 42(1), 91-96.

Jacobson, M. J., Williams, H. C., Taylor, K., and Dilcher, K. (2009). *Solving the Pell equation.* Springer.

Lemmermeyer, F. (2003a). "Conics-a poor man's elliptic curves." *arXiv preprint math/0311306.*

Lemmermeyer, F. (2003b). "Higher descent on pell conics I two centuries of missed opportunities." *arXiv preprint*

Lemmermeyer, F. (2012). "Binomial squares in pure cubic number fields." *Journal de Théorie des Nombres de Bordeaux*, 24(3), 691-704.

Lemmermeyer, F. (2013). "Why is the class number of $\mathbb{Q}(\sqrt[3]{11})$ even?" *Math. Bohem.*, 138(2), 149-163.

Lenstra Jr, H. W. (2008). "Solving the pell equation." *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44, 1-23.

Murty, M. R. and Esmonde, J. (2005). *Problems in algebraic number theory*, volume 190. Springer Science & Business Media.

Rudman, R. J. et al. (1973). "On the fundamental unit of a purely cubic field." *Pacific J. Math*, 46, 253-256.

Silverman, J. and Tate, J. (1992). *Rational points on elliptic curves.* Springer.

Silverman, J. H. (2009). *The arithmetic of elliptic curves.* Springer.

Soleng, R. (1994). Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields. *J. Number Theory*, 46(2), 214-229.

Stewart, I. and Tall, D. (2002). *Algebraic number theory and Fermat's last theorem.*

Stillwell, J. (2002). Mathematics and its history. *The Australian Mathem. Soc*, page 168.

Top, J. (1991). *"Descent by 3-isogeny and 3-rank of quadratic fields".* Erasmus University, Econometric Institute.

Wada, H. et al. (1970). "A table of fundamental units of purely cubic fields." *Proceedings of the Japan Academy*, 46(10, Supplement), 1135-1140.

Washington, L. C. (2008). *Elliptic curves: number theory and cryptography.* CRC press.

Whitford, E. E. (1912). *The Pell Equation.* EE Whitford.

LIST OF PUBLICATIONS/CONFERENCE PAPERS

Publications:

1. K. J. Manasa and B. R. Shankar, “Pell surfaces and elliptic curves”, J. Ramanujan Math. Soc. 31, No.1 (2016) 63-77.

2. Manasa K J and B R Shankar,"Cubic Pell’s Equation and Pure Cubic Fields", Materials Today Proceedings, Elsevier. (communicated).

Conference Papers:

1. Manasa K J and B R Shankar, *On Higher Order Pell Equations*, Proceedings of IMBIC, vol.2, pp.56-63, 2013, 7th International Conference of IMBIC on Mathematical Sciences for Advancement of Science and Technology, MSAST 2013 Kolkata, India.

2. B R Shankar and Manasa K J, *A Study of Lemmermeyer’s Work Relating Pure Cubic Fields and Elliptic Curves*, UGC Sponsored Two Day National Seminar on Number Theory and Its Applications, MGM College, Udupi. December 12-13, 2014 (Presented).

3. Manasa K J and B R Shankar, *Pure Cubic Fields and Elliptic Curves*, 23^{rd} International Conference on, Interdisplinary Mathematical, Statastical and Compuational Techniques , IMSCT 2014, NITK Surathkal, India . December 18-20, 2014 (Presented).

4. Manasa K J and B R Shankar, *Cubic Pell’s Equations and Units in the Pure Cubic Fields*, International Conference on Engineering and Material Sciences, ICEMS 2016, Jaipur National University, Jaipur, India. March 17-19, 2016 (Presented).

BIO DATA

Name : Manasa K J

Email Id : manasakj123@gmail.com

Permanent Address : Manasa K J
D/o K Jayavarma Shetty,
Swasthi, Near Jain Temple ,
Nellikar post,
Mangalore (Dist)- 574 107.

Educational Qualifications:

Degree	**Year of Passing**	**Institute**
B.Sc.Ed	2003	Regional Institute of Education, Mysore.
M.Sc. (Mathematics)	2005	Mangalore University, Mangalore.
Lecturer	2005-2012	NMAM Institute of Technology, Nitte.