จำนวนเต็มในรูปแบบ $x^2 + dy^2$ ในฟิลด์ควอดราติกบางชนิด

นายสารัตน์ ศิลปวงษา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

INTEGERS OF THE FORM $x^2 + dy^2$ IN SOME QUADRATIC FIELDS

Mr. Sarat Sinlapavongsa

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2012

Thesis Title	INTEGERS OF THE FORM $x^2 + dy^2$ IN SOME QUADRATIC FIELDS
By	Mr. Sarat Sinlapavongsa
Field of Study	Mathematics
Thesis Advisor	Associate Professor Ajchara Harnchoowong, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctoral Degree

.....Dean of the Faculty of Science
(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.....Chairman
(Assistant Professor Yotsanan Meemark, Ph.D.)

.....Thesis Advisor
(Associate Professor Ajchara Harnchoowong, Ph.D.)

.....Examiner
(Assistant Professor Tuangrat Chaichana, Ph.D.)

.....Examiner
(Ouamporn Phuksuwan, Ph.D.)

.....External Examiner
(Associate Professor Utsanee Leerawat, Ph.D.)

สารัตน์ ศิลปวงษา : จำนวนเต็มในรูปแบบ $x^2 + dy^2$ ในฟิลด์ควอดราติกบางชนิด.
(INTEGERS OF THE FORM $x^2 + dy^2$ IN SOME QUADRATIC FIELDS)
อ. ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร. อัจฉรา หาญชูวงศ์, 37 หน้า.

การเขียนจำนวนเต็มให้เป็นผลบวกของจำนวนเต็มกำลังสองสองจำนวนเป็นปัญหาที่น่าสนใจ เดวิด คอกซ์ได้ขยายปัญหาดังกล่าวและศึกษาว่าเมื่อกำหนดให้ d เป็นจำนวนเต็มบวกแล้วจำนวนเฉพาะใดบ้างที่สามารถเขียนได้ในรูปแบบ $x^2 + dy^2$ เมื่อ x และ y เป็นจำนวนเต็ม

ในวิทยานิพนธ์ฉบับนี้เราขยายแนวคิดดังกล่าวจากเซตของจำนวนตรรกยะไปยังฟิลด์ควอดราติกบางชนิดและได้หาเงื่อนไขที่บอกได้ว่าเมื่อไรจำนวนเฉพาะจะสามารถเขียนได้ในรูปแบบ $x^2 + dy^2$ ในฟิลด์ควอดราติกดังกล่าว นอกจากนี้เรายังศึกษาจำนวนวิธีการเขียนของจำนวนเต็มที่สามารถเขียนได้ในรูปแบบ $x^2 + dy^2$ ในฟิลด์จำนวนใด ๆ อีกด้วย

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต .....
ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....
สาขาวิชา คณิตศาสตร์
ปีการศึกษา 2555

##5173868023 : MAJOR MATHEMATICS
KEYWORDS : QUADRATIC FIELDS / TOTALLY REAL

SARAT SINLAPAVONGSA : INTEGERS OF THE FORM $x^2 + dy^2$ IN SOME QUADRATIC FIELDS. ADVISOR : ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 37 pp.

Writing an integer as a sum of two squares is an interesting problem. David A. Cox has generalized the problem and study that when a positive integer d is given, which prime integers can be written in the form $x^2 + dy^2$ where x and y are integers

In this thesis, we extend the ideas from the field of rational numbers to some quadratic fields and give the criteria to determine whether an algebraic prime integer can be represented in the form $x^2 + dy^2$. Furthermore, we study the number of representations of an integer which can be represented in the form $x^2 + dy^2$ in a number field.

Department : Mathematics and Computer Science Student's Signature .....
Advisor's Signature .....
Field of Study : Mathematics
Academic Year : 2012

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Associate Professor Dr. Ajchara Harnchoowong, my thesis advisor, for her helpful comments and suggestions in my thesis. Moreover, I would like to thank Assistant Professor Dr. Yotsanan Meemark, Assistant Professor Dr. Tuangrat Chaichana, Dr. Ouamporn Phuksuwan and Associate Professor Dr. Utsanee Leerawat, my thesis commitee, for valuable suggestions. Next, I am grateful to all of my teachers and lecturers during my study.

In particular, my sincere appreciation goes to Chulalongkorn University for Chulalongkorn University Graduate Scholarship to Conference Grant for Ph.D. student and the Institue for the Promotion of Teaching Science and Technology for Development and Promotion of Science and Technology Talents Project Scholarship.

Finally, I wish to thank my beloved parents for their encouragement throughout my study.

CONTENTS

page

CHAPTER I
INTRODUCTION

Most first courses in number theory prove a theorem of Fermat which states that for an odd prime p,

$$p = x^2 + y^2, x, y \in \mathbb{Z} \Leftrightarrow p \equiv 1 \bmod 4. \tag{1.1}$$

Fermat also states that if p is an odd prime

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \Leftrightarrow p \equiv 1, 3 \bmod 8 \tag{1.2}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \Leftrightarrow p = 3 \text{ or } p \equiv 1 \bmod 3. \tag{1.3}$$

B. Fine [8] gave a new proof of (1.1) by using the structure of the modular group which is group theoretically a free product. Later G. Kern-Isberner and G. Rosenberger [10] extended Fine's method to solve (1.2) and (1.3) by using the Hecke groups. To this direction, many mathematicians can deal with primes of the form $x^2 + dy^2$ for a positive integer d. Also, G. Kern-Isberner and G. Rosenberger [10] extended these results for $d = 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 37, 58$ and as is well known, Cox [6] answered this problem completely by using class field theory.

It is significantly more difficult to study primes of the form $x^2 + y^2$ where x, y are algebraic integers in a number field than that over $\mathbb{Z}$. I. Niven [17] determined which algebraic integers can be written as the sum of two integral squares in $\mathbb{Q}(i)$. M. Elia and C. Monico [7] described completely which prime integers in $\mathbb{Q}(\sqrt{2})$ can be represented as the sum of two squares. T. Nagell [14], [15] further studied the question for the twenty two quadratic fields $\mathbb{Q}(\sqrt{m})$ where

$$m = \pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 19, \pm 37, \pm 43, \pm 67, \pm 163.$$

Q. Hourong [9] also studied the problem when an element in a quadratic field, not necessary an algebraic integer can be represented as the sum of two squares of elements in the field.

Let m and d be rational integers such that m is squarefree and d is positive. The first objective of this thesis is determining all algebraic prime integers that can be represented in the form $x^2 + dy^2$ where x and y are algebraic integers in a quadratic field $\mathbb{Q}(\sqrt{m})$. The second objective of this thesis is studying the number of representations of algebraic integers of the form $x^2 + dy^2$ where x and y are algebraic integers in number fields.

In Chapter II, we begin by collecting those definitions and results about the ring of integers, ideal class groups, unit groups, and the Hilbert class field, mainly without proofs, to be used throughout the entire thesis. We describe the imaginary quadratic fields with class number $1, 2$ and 4 and describe the imaginary biquadratic fields with class number 1 and 2.

In Chapter III, we give some conditions on n and d in order that the class number of $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{m}, \sqrt{-d})$ are 1 and we can determine the primes that can be written in the form x^2+dy^2 where x and y are algebraic integers in $\mathbb{Q}(\sqrt{m})$. Moreover, we use Hilbert class field to determine which primes can be written in the form $x^2 + dy^2$ where x and y are algebraic integers in $\mathbb{Q}(\sqrt{m})$ for some m and d.

In Chapter IV, we study the numbers of representations of integers of the form $x^2 + dy^2$ where x and y are algebraic integers in number fields.

CHAPTER II
PRELIMINARIES

In this chapter, we give notations, definitions and theorems used throughout the thesis. Details and proofs can be found in [12], [13] and [19] unless otherwise stated.

2.1 The Ring of Integers

Definition 2.1.1. A *number field* is a finite extension of $\mathbb{Q}$ (in $\mathbb{C}$).

Definition 2.1.2. Let K be a number field. An $\alpha \in K$ is an *algebraic integer* if and only if there exist $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Remark 2.1.3. An $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Definition 2.1.4. All algebraic integers in a number field K form a ring, called the *ring of integers* in K and denoted by $\mathcal{O}_K$.

Definition 2.1.5. An *embedding* of L over K in $\mathbb{C}$ is a one to one homomorphism $\sigma : L \to \mathbb{C}$ fixing K pointwise. An *embedding* of L in $\mathbb{C}$ is an embedding of L over $\mathbb{Q}$ in $\mathbb{C}$.

Let K and L be number fields with $K \subseteq L$ and $[L : K] = n$. Then there exist n embeddings of L over K in $\mathbb{C}$ denoted by $\sigma_1 = id_L, \sigma_2, \ldots, \sigma_n$.

Definition 2.1.6. For $\alpha \in L$, define the *relative trace* of α by

$$\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$$

and the *relative norm* of α by

$$\mathrm{N}_{L/K}(\alpha) = \sigma_1(\alpha)\,\sigma_2(\alpha)\ldots\sigma_n(\alpha).$$

If $K = \mathbb{Q}$, then denote $\mathrm{Tr}_{L/\mathbb{Q}}$ by Tr_L and $\mathrm{N}_{L/\mathbb{Q}}$ by N_L and call the *absolute trace* and *absolute norm*, respectively.

Definition 2.1.7. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. The *discriminant* of $\alpha_1, \alpha_2, \ldots, \alpha_n$ in L over K denoted by $\mathrm{disc}_{L/K}\ (\alpha_1, \alpha_2, \ldots, \alpha_n) := \det[\sigma_i(\alpha_j)]^2$.

Theorem 2.1.8. *Let K be a number field of degree n over $\mathbb{Q}$. Then $\mathcal{O}_K$ is a free abelian group (or $\mathbb{Z}$-module) of rank n, i.e., it is isomorphic to the direct sum of n subgroups each of which is isomorphic to $\mathbb{Z}$.*

Definition 2.1.9. A $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathcal{O}_K$ is called an *integral basis* of K.

Note. An integral basis of K is also a basis of K over $\mathbb{Q}$.

Proposition 2.1.10. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be any integral bases of K. Then* $\mathrm{disc}_K(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_K(\beta_1, \ldots, \beta_n)$.

Definition 2.1.11. The *discriminant of the field* $K = \mathrm{disc}_K(\alpha_1, \ldots, \alpha_n)$ where $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K over $\mathbb{Q}$, we denote it by $\mathrm{disc}(K)$ or δ_K.

2.2 Factorization of Elements in the Ring of Integers

Definition 2.2.1. Let D be an integral domain.
(1) $u \in D$ is a *unit* if and only if $u \mid 1$.
(2) $x, y \in D$ are *associates* or y is an *associate* of x, in notation $x \sim y$, if and only if there exists a unit $u \in D$ such that $x = yu$.
(3) A nonzero nonunit $x \in D$ is *prime* if and only if for all $m, n \in D$, if $x \mid mn$ then $x \mid m$ or $x \mid n$.

Note. If x is prime, then y is prime for every associate y of x.

Proposition 2.2.2. *Let D be an integral domain and $x, y \in D \setminus \{0\}$. Then*
(i) x and y are associates if and only if $\langle x \rangle = \langle y \rangle$.
(ii) x is prime if and only if $\langle x \rangle$ is a prime ideal.

2.3 Decomposition of Ideals

This section will be used for theorems about quadratic and biquadratic fields in the next chapter.

Theorem 2.3.1. *Every nonzero proper ideal in $\mathcal{O}_K$ can be written uniquely as a product of prime ideals.*

Definition 2.3.2. The *norm* of a nonzero ideal A in $\mathcal{O}_K$, denoted by $\mathrm{N}(A)$, is defined to be $|\ \mathcal{O}_K/A\ |$.

Theorem 2.3.3. *For any $\alpha \neq 0$ in $\mathcal{O}_K$, $\mathrm{N}(\langle\alpha\rangle) = |\mathrm{N}_K(\alpha)|$.*

Remark 2.3.4. If P is a nonzero ideal such that $\mathrm{N}(P) = p$ a prime number, then P is a prime ideal in $\mathcal{O}_K$.

Let $L \supseteq K$ be a finite extension of number fields. Let P be a nonzero prime ideal in $\mathcal{O}_K$. Then $P\mathcal{O}_L$ is a nonzero ideal in $\mathcal{O}_L$. We will consider the prime factorization of $P\mathcal{O}_L$ in $\mathcal{O}_L$. From now on, the term *prime ideal* means *nonzero prime ideal*.

Theorem 2.3.5. *Let P be a prime ideal in $\mathcal{O}_K$ and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_L$. Then the following are equivalent.*
(i) $\mathfrak{p}|P\mathcal{O}_L$.
(ii) $\mathfrak{p} \supset P\mathcal{O}_L$.
(iii) $\mathfrak{p} \supset P$.
(iv) $\mathfrak{p} \cap \mathcal{O}_K = P$.
(v) $\mathfrak{p} \cap K = P$.

Definition 2.3.6. For P and $\mathfrak{p}$ satisfying any of the above theorem, we say that $\mathfrak{p}$ *lies over* P or P *lies under* $\mathfrak{p}$.

Definition 2.3.7. Let $P\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ be the prime factorization in $\mathcal{O}_L$ where P is a prime ideal in $\mathcal{O}_K$.

(1) g is called the *decomposition number* of P in L.

(2) For each i, e_i is called the *ramification index* of $\mathfrak{p}_i$ over P in L over K,

denoted by $e(\mathfrak{p}_i/P)$.

P is *ramified* in $\mathcal{O}_L$ (in L) if there exists i such that $e_i > 1$.

P is *inert* in L if $g = 1$ and $e_1 = 1$, i.e., $P\mathcal{O}_L$ is a prime ideal.

The field $\mathcal{O}_K/P$ is embedded in the field $\mathcal{O}_L/\mathfrak{p}$ so it can be considered as a subfield of $\mathcal{O}_L/\mathcal{P}$.

Definition 2.3.8. The degree of $\mathcal{O}_L/\mathfrak{p}_i$ over $\mathcal{O}_K/P$ is called the *residue class degree* or *inertial degree* of $\mathfrak{p}_i$ over P, denoted by $f(\mathfrak{p}_i/P)$.

Remark 2.3.9. $\mathrm{N}(\mathfrak{p}_i) = \mathrm{N}(P)^f$ where $f = f(\mathfrak{p}_i/P)$.

Theorem 2.3.10. *Let $L \supseteq K$ be a number field extension of degree n and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be primes in $\mathcal{O}_L$ lying above a prime P of $\mathcal{O}_K$ with ramification indices $e_1, \ldots, e_g$ and residue class degrees $f_1, \ldots, f_g$. Then $n = \sum_{i=1}^{g} e_i f_i$.*

Definition 2.3.11. Let $L \supseteq K$ be a number field extension of degree n and P be a prime ideal in $\mathcal{O}_K$ such that $P\mathcal{O}_L = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_g^{e_g}$ where $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_L$.

(1) P is *totally ramified* in L if $g = 1$ and $e_1 = n$, so $f_1 = 1$ and $P\mathcal{O}_L = \mathfrak{p}_1^n$.

(2) P *splits completely* in L if $g = n$, so $e_i = 1$, $f_1 = 1$ for all i and $P\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_n$.

Theorem 2.3.12. *Let $L \supseteq K$ be a Galois extension number field of degree n and $\mathfrak{p}_i, \mathfrak{p}_j$ be primes in $\mathcal{O}_L$ lying above a prime P of $\mathcal{O}_K$. Then $e(\mathfrak{p}_i/P) = e(\mathfrak{p}_j/P)$ and $f(\mathfrak{p}_i/P) = f(\mathfrak{p}_j/P)$, i.e., $P\mathcal{O}_L = (\mathfrak{p}_1\ldots\mathfrak{p}_g)^e$, hence $n = efg$ where $e = e(\mathfrak{p}_i/P)$ and $f = f(\mathfrak{p}_i/P)$.*

2.4 Quadratic and Biquadratic Fields

We collect necessary results of quadratic and biquadratic fields here. These properties will be used in Chapter III.

Definition 2.4.1. A *quadratic field* is a number field of degree 2 over $\mathbb{Q}$.

Note. A quadratic field is of the form $\mathbb{Q}(\sqrt{m})$ where m is a squarefree integer.

Theorem 2.4.2. *Let $K = \mathbb{Q}(\sqrt{m})$ where m is a squarefree integer.*
(i) If $m \equiv 1 \bmod 4$, then $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ is an integral basis of K, i.e.,

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2}.$$

(ii) If $m \equiv 2$ or $3 \bmod 4$, then $\{1, \sqrt{m}\}$ is an integral basis of K, i.e.,

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{m}.$$

Next, the decomposition of principal ideals generated by 2 in quadratic fields can be determined in the following theorem [12].

Theorem 2.4.3. *Let $K = \mathbb{Q}(\sqrt{m})$ where n is a squarefree integer.*
(i) If $m \equiv 2, 3 \bmod 4$, then $2\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.
(ii) If $m \equiv 1 \bmod 8$, then $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} \neq \mathfrak{p}'$ are prime in $\mathcal{O}_K$.
(iii) If $m \equiv 5 \bmod 8$, then $2\mathcal{O}_K$ is prime in $\mathcal{O}_K$.

Definition 2.4.4. Let p be an odd prime, and let a be an integer such that $(a, p) = 1$. The *Legendre* symbol (a/p) is defined by

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

Theorem 2.4.5. *Let $K = \mathbb{Q}(\sqrt{m})$ where m is a squarefree integer, and let p be an odd prime.*
(i) If $p \mid m$, then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.
(ii) If $p \nmid m$ and $(m/p) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} \neq \mathfrak{p}'$ are prime in $\mathcal{O}_K$.
(iii) If $p \nmid m$ and $(m/p) = -1$, then $p\mathcal{O}_K$ is prime in $\mathcal{O}_K$.

Definition 2.4.6. A *biquadratic field* is an extension of degree four over $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ where m, n are distinct squarefree integers. A biquadratic field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is called *real* if both m and n are positive and is called *imaginary* if m or n are negative.

Theorem 2.4.7. *Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ where m and n are distinct squarefree integers and $k = \frac{mn}{d^2}$ where $d = (m, n)$.*

(i) If $m \equiv 3, n \equiv k \equiv 2 \bmod 4$, *then* $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$ *is an integral basis of* L, *i.e.,*

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{m} \oplus \mathbb{Z} \cdot \sqrt{n} \oplus \mathbb{Z} \cdot \frac{\sqrt{n}+\sqrt{k}}{2}.$$

(ii) If $m \equiv 1, n \equiv k \equiv 2$ *or* $3 \bmod 4$, *then* $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$ *is an integral basis of* L, *i.e.,*

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2} \oplus \mathbb{Z} \cdot \sqrt{n} \oplus \mathbb{Z} \cdot \frac{\sqrt{n}+\sqrt{k}}{2}.$$

(iii) If $m \equiv n \equiv k \equiv 1 \bmod 4$, *then* $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}$ *is an integral basis of* L, *i.e.,*

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{n}}{2} \oplus \mathbb{Z} \cdot \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right).$$

The study of the decomposition of principal ideals generated by an odd prime in biquadratic fields can be found in [5].

Theorem 2.4.8. *Let* $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ *where* m *and* n *are distinct squarefree integers and* $k = \frac{mn}{d^2}$ *where* $d = (m, n)$, *and let* p *be an odd prime.*
(i) If $p \mid m, p \mid n, p \nmid k$ *and* $(k/p) = 1$, *then* $p\mathcal{O}_L = \mathfrak{p}_1^2\mathfrak{p}_2^2$ *where* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$ *are distinct primes in* $\mathcal{O}_L$.
(ii) If $p \mid m, p \mid n, p \nmid k$ *and* $(k/p) = -1$, *then* $p\mathcal{O}_L = \mathfrak{p}_1^2$ *where* $\mathfrak{p}_1$ *is prime in* $\mathcal{O}_L$.
(iii) If $p \nmid mnk, (m/p) = 1$ *and* $(n/p) = 1$, *then* $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ *where* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ *and* $\mathfrak{p}_4$ *are distinct primes in* $\mathcal{O}_L$.
(iv) If $p \nmid mnk, (m/p) = -1$ *and* $(n/p) = -1$, *then* $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$ *where* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$ *are distinct primes in* $\mathcal{O}_L$.

2.5 Ideal Class Groups and Unit Groups

Definition 2.5.1. Let D be an integral domain with the field of quotients K. Let $\mathfrak{I}$ be a $D-$submodule of K. $\mathfrak{I}$ is a *fractional ideal* if there exists $d \in D \setminus \{0\}$ such that $d\mathfrak{I} \subseteq D$.

Let $\mathfrak{I}_K$ be the set of all nonzero fractional ideals of K. Then $\mathfrak{I}_K$ is a group under multiplication of ideals. The most important subgroup of $\mathfrak{I}_K$ is the subgroup

$\mathfrak{P}_K$ of *principal fractional ideals*, i.e., those of the form $\alpha\mathcal{O}_K$ for some nonzero $\alpha \in K$. The quotient $\mathfrak{I}_K/\mathfrak{P}_K$ is the *ideal class group* and is denoted by $C(\mathcal{O}_K)$. The basic fact is that $C(\mathcal{O}_K)$ is a finite abelian group and the order of $C(\mathcal{O}_K)$ is called the *class number* of K, denoted by h_K.

The following theorem can be found in [1] and [19].

Theorem 2.5.2. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field where m is negative squarefree integer. Then*
(i) only for $-m = 1, 2, 3, 7, 11, 19, 43, 67$ and 163, we have $h_K = 1$.
(ii) only for $-m = 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403$ and 427, we have $h_K = 2$.
(iii) only for $-m = 14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97$, 102, $130, 133, 142, 155, 177, 190, 193, 195, 203, 219, 253, 259, 291, 323, 355, 435, 483$, 555, $595, 627, 667, 715, 723, 763, 795, 955, 1003, 1027, 1227, 1243, 1387, 1411, 1435$, 1507 and 1555, we have $h_K = 4$.

This theorem says that there are 9 imaginary quadratic fields of class number 1, exactly 18 imaginary quadratic fields of class number 2 and exactly 54 imaginary quadratic fields of class number 4.

The set of all units in $\mathcal{O}_K$ is denoted by $\mathcal{O}_K^\times$. It is a group under multiplication.

Theorem 2.5.3. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a biquadratic field and let k_1, k_2 and k_3 be the quadratic subfields of K. Let Γ be a subgroup of $\mathcal{O}_K^\times$ generated by units which are also in $\mathcal{O}_{k_i}$ for $i = 1, 2, 3$. Then*

$$h_K = \begin{cases} \frac{1}{4} Q h_{k_1} h_{k_2} h_{k_3} & \text{if } K \text{ is real} \\ \frac{1}{2} Q h_{k_1} h_{k_2} h_{k_3} & \text{if } K \text{ is complex.} \end{cases}$$

where $Q = [\mathcal{O}_K^\times : \Gamma]$ denotes the index of Γ in $\mathcal{O}_K^\times$.

We use Theorem 2.5.2 and Theorem 2.5.3 to determine all imaginary biquadratic fields of class number 1 and 2 and the proofs can be found in [2] and [3].

Theorem 2.5.4. *(i) There are* 47 *imaginary biquadratic fields of class number* 1*. (ii) There are* 160 *imaginary biquadratic fields of class number* 2*.*

The examples of imaginary quadratic fields of class number 1 which we use in this thesis are $\mathbb{Q}(\sqrt{-2},\sqrt{-7})$, $\mathbb{Q}(\sqrt{29},\sqrt{-2})$, $\mathbb{Q}(\sqrt{2},\sqrt{-11})$ and $\mathbb{Q}(\sqrt{5},\sqrt{-2})$ and the example of imaginary quadratic fields of class number 2 which we use in this thesis is $\mathbb{Q}(\sqrt{17},\sqrt{-1})$.

Theorem 2.5.5. *Let $K=\mathbb{Q}(\sqrt{-m})$ where m is a positive squarefree integer.*

(i) If $m=1$, then $\mathcal{O}_K^\times=\{\pm1,\pm i\}$.

(ii) If $m=3$, then $\mathcal{O}_K^\times=\{\pm1,\frac{1\pm\sqrt{-3}}{2},\frac{-1\pm\sqrt{-3}}{2}\}$.

(iii) If $m\neq1,3$, then $\mathcal{O}_K^\times=\{\pm1\}$.

Theorem 2.5.6 (Dirichlet's Unit Theorem)**.** *Let K be a number field of degree $n=r+2s$ over $\mathbb{Q}$ where r is the number of real embeddings of K and s is the number of nonconjugate complex embeddings of K. Then $\mathcal{O}_K^\times\cong\mathcal{W}_K\times V$ where $\mathcal{W}_K$ is the cyclic group of even order of all roots of unity in K and V is a free abelian group of rank $t=r+s-1$, i.e., there are units $u_1,\ldots,u_t$ such that for all $u\in\mathcal{O}_K^\times$, u can be written uniquely in the form $u=wu_1^{a_1},\ldots,u_t^{a_t}$ where $a_i\in\mathbb{Z}$ and $w\in\mathcal{W}_K$.*

Let $K=\mathbb{Q}(\sqrt{m})$ be a real quadratic field where m is a positive squarefree integer. Then K has two real embeddings, so $r=2$ and $s=0$, and $t=r+s-1=1$. Since $K\subset\mathbb{R}$, the only root of unity are ±1, i.e., $\mathcal{W}_K=\langle-1\rangle$. Hence $\mathcal{O}_K^\times\cong\mathcal{W}_K\times V$ where V is a free abelian group of rank 1. It can be shown that there is a positive element $u_1\in\mathcal{O}_K^\times$ such that for each $u\in\mathcal{O}_K^\times, u=\pm u_1^k$ where $k\in\mathbb{Z}$. The element u_1 is called the *fundamental unit* in K.

2.6 The Hilbert Class Field

In this section definitions, theorems and their proofs are found in [6].

Definition 2.6.1. An extension $K \subset L$ is *abelian* if it is Galois and $\mathrm{Gal}(L/K)$ is an abelian group.

Definition 2.6.2. A *real infinite prime* is an embedding $\sigma : K \to \mathbb{R}$ and a *complex infinite prime* is a pair of complex conjugate embeddings $\sigma, \bar{\sigma} : K \to \mathbb{C}, \sigma \neq \bar{\sigma}$. Prime ideals of $\mathcal{O}_K$ are often called *finite primes* to distinguish them from the *infinite primes*.

Definition 2.6.3. Given an extension $K \subset L$, an infinite prime σ of K *ramifies* in L provided that σ is real but it has an extension to L which is complex.

Example 2.6.4. The infinite prime of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\sqrt{2})$ but ramified in $\mathbb{Q}(\sqrt{-2})$.

Definition 2.6.5. An extension $K \subset L$ is *unramified* if it is unramified at all primes, finite or infinite.

Theorem 2.6.6. *Given a number field K, there is a finite Galois extension L of K such that:*
(i) L is an unramified abelian extension of K.
(ii) Any unramified abelian extension of K lies in L.

Definition 2.6.7. The field L of Theorem 2.6.6 is called the *Hilbert class field* of K.

The Hilbert class field is the maximal unramified abelian extension of K and is clearly unique.

Theorem 2.6.8. *If L is the Hilbert class field of K, then the Galois group of L over K is isomophic to the ideal class group of K , i.e.,*

$$\mathrm{Gal}(L/K) \simeq C(\mathcal{O}_K).$$

Theorem 2.6.9. *Let L be the Hilbert class field of a number field K, and let $\mathfrak{p}$ be a prime ideal of K. Then*

$$\mathfrak{p} \text{ splits completely in } L \Leftrightarrow \mathfrak{p} \text{ is a principal ideal.}$$

CHAPTER III
PRIMES OF THE FORM $x^2 + dy^2$ IN SOME QUADRATIC FIELDS

M. Elia and C. Monico [7] described which prime integers in $\mathbb{Q}(\sqrt{2})$ can be represented as the sum of two integral squares. Their method depended on the fact that the class numbers of $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ and $\mathbb{Q}(\sqrt{2})$ are 1. We will generalize this to determine the prime integers in $\mathbb{Q}(\sqrt{m})$ that can be represented in the form $x^2 + dy^2$ where d is a positive integer under some conditions. In Section 3.1, we work for the case that the class numbers of $\mathbb{Q}(\sqrt{m}, \sqrt{-d})$ and $\mathbb{Q}(\sqrt{m})$ are 1. Then we use Hilbert class fields for the case without the class numbers condition.

3.1 The Case of Class Number One

Let $K = \mathbb{Q}(\sqrt{m})$ and $L = \mathbb{Q}(\sqrt{m}, \sqrt{-d})$ where m, d are squarefree integers satisfying the following properties.

(1) $d > 0$.

(2) If $m < 0$, then $-1 = x^2 + dy^2$ has a solution in $\mathcal{O}_K$ and if $m > 0$, then $N(u) = -1$ where u is the fundamental unit of $\mathbb{Q}(\sqrt{m})$.

(3) The units of $\mathbb{Q}(\sqrt{m}, \sqrt{-d})$ are $\pm u^l$ where l is an integer and u is the fundamental unit of $\mathbb{Q}(\sqrt{-md})$ if $m < 0$ and of $\mathbb{Q}(\sqrt{m})$ if $m > 0$.

(4) $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$ or $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$.

(5) The class number of both $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{m}, \sqrt{-d})$ is 1.

(6) $(m, d) = 1$.

Lemma 3.1.1. *(i) If* $m \equiv 1 \bmod 4$ *and* $-d \equiv 2, 3 \bmod 4$, *then*

$$\mathcal{O}_L = \left\{ \frac{r + s\sqrt{m}}{2} + \sqrt{-d}\frac{t + u\sqrt{m}}{2} | r, s, t, u \in \mathbb{Z}, r \equiv s \bmod 2 \text{ and } t \equiv u \bmod 2 \right\}.$$

(ii) If $m \equiv 2, 3 \bmod 4$ *and* $-d \equiv 1 \bmod 4$*, then*

$$\mathcal{O}_L = \left\{ \frac{r + s\sqrt{m}}{2} + \sqrt{-d}\frac{t + u\sqrt{m}}{2} | r, s, t, u \in \mathbb{Z}, r \equiv t \bmod 2 \text{ and } s \equiv u \bmod 2 \right\}.$$

Proof. (i) Assume that $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$.
By Theorem 2.4.7, $\{1, \frac{1+\sqrt{m}}{2}, \sqrt{-d}, \frac{\sqrt{-d}+\sqrt{-dm}}{2}\}$ is an integral basis of L, i.e. $\mathcal{O}_L = \mathbb{Z} \cdot 1 \oplus + \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2} \oplus \mathbb{Z} \cdot \sqrt{-d} \oplus \mathbb{Z} \cdot \frac{\sqrt{-d}+\sqrt{-dm}}{2}$. Then

$$\begin{aligned} e \in \mathcal{O}_L &\Leftrightarrow e = x + y(\frac{1+\sqrt{m}}{2}) + z\sqrt{-d} + w(\frac{\sqrt{-d}+\sqrt{-dm}}{2}) \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = (\frac{2x+y}{2} + \frac{y}{2}\sqrt{m}) + (\frac{2z+w}{2} + \frac{w}{2}\sqrt{m})\sqrt{-d} \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = \frac{r + s\sqrt{m}}{2} + \sqrt{-d}\frac{t + u\sqrt{m}}{2} \text{ where } r \equiv s \bmod 2 \text{ and } t \equiv u \bmod 2. \end{aligned}$$

(ii) Assume that $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$.
By Theorem 2.4.7, $\{1, \frac{1+\sqrt{-d}}{2}, \sqrt{m}, \frac{\sqrt{m}+\sqrt{-dm}}{2}\}$ is an integral basis of L, i.e. $\mathcal{O}_L = \mathbb{Z} \cdot 1 \oplus + \mathbb{Z} \cdot \frac{1+\sqrt{-d}}{2} \oplus \mathbb{Z} \cdot \sqrt{m} \oplus \mathbb{Z} \cdot \frac{\sqrt{m}+\sqrt{-dm}}{2}$. Then

$$\begin{aligned} e \in \mathcal{O}_L &\Leftrightarrow e = x + y(\frac{1+\sqrt{-d}}{2}) + z\sqrt{m} + w(\frac{\sqrt{m}+\sqrt{-dm}}{2}) \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = (\frac{2x+y}{2} + \frac{2z+w}{2}\sqrt{m}) + (\frac{y}{2} + \frac{w}{2}\sqrt{m})\sqrt{-d} \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = \frac{r + s\sqrt{m}}{2} + \sqrt{-d}\frac{t + u\sqrt{m}}{2} \text{ where } r \equiv t \bmod 2 \text{ and } s \equiv u \bmod 2. \end{aligned}$$

□

Lemma 3.1.2. *Let* $K = \mathbb{Q}(\sqrt{m})$ *and* $k \in \mathbb{Z}$*. Let* π *be a prime integer in* $\mathcal{O}_K$ *such that* $\pi\mathcal{O}_K$ *lies over a prime number* p *where* $p \nmid mk$*. Then there exists* $\alpha \in \mathcal{O}_K$ *such that* $\alpha^2 \equiv k \bmod \pi$ *if and only if* $(mk/p) = 1$*.*

Proof. Case 1. $m \equiv 2, 3 \bmod 4$: Assume that $a + b\sqrt{m} \in \mathcal{O}_K$ such that $(a + b\sqrt{m})^2 \equiv k \bmod P$. Then $(a - b\sqrt{m})^2 \equiv k \bmod \pi'$ where π' is the nontrivial conjugate of π, so $[(a + b\sqrt{m})^2 - k][(a - b\sqrt{m})^2 - k] \equiv 0 \bmod \pi\pi'$. Thus $(a^2 - mb^2 - k)^2 - 4mkb^2 \equiv 0 \bmod N(\pi)$. Since $p \mid \mathrm{N}(\pi), (a^2 - mb^2 - k)^2 - 4mkb^2 \equiv 0 \bmod p$. Hence $(mk/p) = (4mkb^2/p) = 1$.

Convesely, assume that $(mk/p) = 1$. Then $(m/p) = (k/p) = 1$ or $(m/p) = (k/p) = -1$.

Case 1.1. $(m/p) = (k/p) = 1$: Since $(k/p) = 1$, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv k \bmod p$. Since $\pi \mid p$, $x^2 \equiv k \bmod \pi$.

Case 1.2. $(m/p) = (k/p) = -1$: Since $(m/p) = -1$, we may let $\pi = p$. Since $(m, p) = 1$, there exists $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \bmod p$. Since $(m/p) = -1$, $(m'/p) = -1$ and so $(km'/p) = 1$. Thus there exists $b \in \mathbb{Z}$ such that $b^2 \equiv km' \bmod p$. Hence $(b\sqrt{m})^2 = b^2 m \equiv k \bmod \pi$.

Case 2. $m \equiv 1 \bmod 4$: Assume that $\frac{a+b\sqrt{m}}{2} \in \mathcal{O}_K$ such that $(\frac{a+b\sqrt{m}}{2})^2 \equiv k \bmod \pi$. Then $(\frac{a-b\sqrt{m}}{2})^2 \equiv k \bmod \pi'$ where π' is the nontrivial conjugate of π. Thus $[(\frac{a+b\sqrt{m}}{2})^2 - k][(\frac{a-b\sqrt{m}}{2})^2 - k] \equiv 0 \bmod \pi\pi'$. Hence $(\frac{a^2-mb^2}{4} - k)^2 - mkb^2 \equiv 0 \bmod N(\pi)$. Since $p \mid N(\pi)$, $(\frac{a^2-mb^2}{4} - k)^2 - mkb^2 \equiv 0 \bmod p$ and so $(mk/p) = (mkb^2/p) = 1$.

Convesely, Assume that $(mk/p) = 1$. Then $(m/p) = (k/p) = 1$ or $(m/p) = (k/p) = -1$.

Case 2.1. $(m/p) = (k/p) = 1$: Since $(k/p) = 1$, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv k \bmod p$. Since $\pi \mid p$, $x^2 \equiv k \bmod \pi$.

Case 2.2. $(m/p) = (k/p) = -1$: Since $(m/p) = -1$, we may let $\pi = p$. Since $(m, p) = 1$, there exists $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \bmod p$. Since $(m/p) = -1$, $(m'/p) = -1$ and so $(km'/p) = 1$. Thus there exists $b \in \mathbb{Z}$ such that $b^2 \equiv km' \bmod p$. Hence $(b\sqrt{m})^2 = b^2 m \equiv k \bmod \pi$.

□

3.1.1 Imaginary Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{m})$ where $m < 0$ so that $-1 = x^2 + dy^2$ has a solution in $\mathcal{O}_K$. Hence the identity

$$(x^2 + dy^2)(z^2 + dw^2) = (xz - dyw)^2 + d(yz + xw)^2$$

implies that prime integers π and $-\pi$ in $\mathbb{Q}(\sqrt{m})$ can or cannot simultaneously be written in the form $x^2 + dy^2$.

Theorem 3.1.3. *Let π be a prime integer in $K = \mathbb{Q}(\sqrt{m})$ such that $\pi\mathcal{O}_K$ lies over an odd prime p where $p \nmid md$ in $\mathbb{Z}$.*
(1) For $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$, we have

$$\pi = x^2 + dy^2 \text{ for some } x, y \in \mathcal{O}_K \Leftrightarrow (m/p) = (-d/p) = 1 \text{ or } (m/p) = -1.$$

(2) For $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$, we have

(2.1) π cannot be written in the form $x^2 + dy^2$ where $x, y \in \mathcal{O}_K$, if $(m/p) = 1$ and $(-d/p) = -1$

(2.2) 4π can be written in the form $(r + s\sqrt{m})^2 + d(t + u\sqrt{m})^2$ where r, s, t and u are rational integers. Furthermore, if one of the numbers r, s, t and u is odd, then P cannot be written in the form $x^2 + dy^2$ where $x, y \in \mathcal{O}_K$, if $(m/p) = 1 = (-d/p) = 1$ or $(m/p) = -1$.

Proof. Let π be a prime integer in $K = \mathbb{Q}(\sqrt{m})$ such that $\pi\mathcal{O}_K$ lies over a prime p where $p \nmid md$ in $\mathbb{Z}$. Assume that $(m/p) = 1$ and $(-d/p) = -1$. Suppose for a contradiction that $\pi = x^2 + dy^2$ for some $x, y \in \mathcal{O}_K$. Then $x^2 \equiv -dy^2 \bmod \pi$. Since $(y, \pi) = 1$, there exists $y' \in \mathcal{O}_K$ such that $yy' \equiv 1 \bmod \pi$ and so $(xy')^2 \equiv -d \bmod \pi$. By Lemma 3.1.2, $(-dm/p) = 1$. This is a contradiction.

Next, suppose that $(m/p) = (-d/p) = 1$ or $(m/p) = -1$. By Lemma 2.4.5 and Lemma 2.4.8, $\pi\mathcal{O}_L$ splits completely in L, i.e. $\pi\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. Since L is a PID, we may let $\mathfrak{p}_1 = (\frac{r+s\sqrt{m}}{2} + \sqrt{-d}\frac{t+u\sqrt{m}}{2})$ and $\mathfrak{p}_2 = (\frac{r+s\sqrt{m}}{2} - \sqrt{-d}\frac{t+u\sqrt{m}}{2})$. Then $\pi\mathcal{O}_L = ((\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2)$. Since a unit of $\mathcal{O}_L$ is of the form $\pm u^l$, $\pi = \pm u^l((\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2)$. Since $\pi, (\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2 \in \mathcal{O}_K$ and $u \in \mathbb{Q}(\sqrt{-md})$, l must be zero and $\pi = \pm(\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2$.
For $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$, $\frac{r+s\sqrt{m}}{2}, \frac{t+u\sqrt{m}}{2} \in \mathcal{O}_K$ and so π can be written in the form $x^2 + dy^2$.
For $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$, we have 4π is of the form $(r + s\sqrt{m})^2 + d(t + u\sqrt{m})^2$.

Next, assume that one of the r, s, t and u is odd. Suppose on the contrary that π can be written in the form $(x + y\sqrt{m})^2 + d(z + w\sqrt{m})^2$. Then $((x + y\sqrt{m}) + \sqrt{-d}(z + w\sqrt{m})) = ((\frac{r+s\sqrt{m}}{2}) + \sqrt{-d}(\frac{t+u\sqrt{m}}{2}))$ which implies that $(\frac{r+s\sqrt{m}}{2}) + \sqrt{-d}(\frac{t+u\sqrt{m}}{2}) = \pm u^l((x + y\sqrt{m}) + \sqrt{-d}(z + w\sqrt{m}))$. This is a contradiction. □

Theorem 3.1.4. *Let π be a prime integer in $K = \mathbb{Q}(\sqrt{-2})$ such that $\pi\mathcal{O}_K$ lies over a prime p in $\mathbb{Z}$.*

(i) If $p = 2$, then π cannot be written in the form $x^2 + 7y^2$ where $x, y \in \mathcal{O}_K$.

(ii) If $p = 7$, then π can be written in the form $x^2 + 7y^2$ where $x, y \in \mathcal{O}_K$.

(iii) If $(-2/p) = 1$ and $(-7/p) = -1$, then π cannot be written in the form x^2+7y^2 where $x, y \in \mathcal{O}_K$.

(iv) If $(-2/p) = (-7/p) = 1$ or $(-2/p) = -1$, then 4π can be written in the form $(r+s\sqrt{-2})^2+7(t+u\sqrt{-2})^2$ where r, s, t and u are rational integers. Furthermore if one of the numbers r, s, t and u is odd, then P cannot be written in the form $x^2 + 7y^2$ where $x, y \in \mathcal{O}_K$.

Proof. First, note that $-1 = (2\sqrt{-2})^2 + 7(1)^2$.

(i) For $p = 2$, p is ramified in K and so $\pi = \pm\sqrt{-2}$. Suppose for a contradiction that $\pm\sqrt{-2}$ can be written in the form x^2+7y^2 where $x, y \in \mathcal{O}_K$. Then $\pm\sqrt{-2} = (r+s\sqrt{-2})^2+7(t+u\sqrt{-2})^2$ for some $r, s, t, u \in \mathbb{Z}$. Then $\pm 1 = 2(rs+7tu)$, which is a contradiction. Hence π cannot be written in the form $x^2 + 7y^2$.

(ii) For $p = 7$, p is inert in K and so $\pi = \pm 7$. Since $7 = 0^2 + 7 \cdot 1^2$, π can be written in the form $x^2 + 7y^2$.

(iii) and (iv) follow immediately from Theorem 3.1.3. □

3.1.2 Real Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{m})$ where $m > 0$ so that $N(u) = -1$ where u is the fundamental unit of $\mathbb{Q}(\sqrt{m})$.

An element $r+s\sqrt{m}$ in K is called *totally positive* if both $r+s\sqrt{m}$ and $r-s\sqrt{m}$ are positive. It is clear that any prime integer in K which can be represented in the form $x^2 + dy^2$ is necessarily totally positive, so we restrict our attention to such primes in the following theorem.

Theorem 3.1.5. *Let π be a totally positive prime integer in $K = \mathbb{Q}(\sqrt{m})$ such that $\pi\mathcal{O}_K$ lies over an odd prime p where $p \nmid md$ in $\mathbb{Z}$.*

(1) For $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$, we have

$$\pi = x^2 + dy^2 \text{ for some } x, y \in \mathcal{O}_K \Leftrightarrow (m/p) = (-d/p) = 1 \text{ or } (m/p) = -1.$$

(2) For $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$, we have

(2.1) If $(m/p) = 1$ and $(-d/p) = -1$, then π cannot be written in the form $x^2 + dy^2$ where $x, y \in \mathcal{O}_K$

(2.2) If $(m/p) = 1 = (-d/p) = 1$ or $(m/p) = -1$, then 4π can be written in the form $(r + s\sqrt{m})^2 + d(t + u\sqrt{m})^2$ where r, s, t and u are rational integers. Furthermore, if one of the numbers r, s, t and u is odd, then π cannot be written in the form $x^2 + dy^2$ where $x, y \in \mathcal{O}_K$.

Proof. Let π be a prime integer in $K = \mathbb{Q}(\sqrt{m})$ such that $\pi\mathcal{O}_K$ lies over a prime p where $p \nmid md$ in $\mathbb{Z}$. Assume that $(m/p) = 1$ and $(-d/p) = -1$. Suppose for a contradiction that $\pi = x^2 + dy^2$ for some $x, y \in \mathcal{O}_K$. Then $x^2 \equiv -dy^2 \bmod \pi$. Since $(y, \pi) = 1$, there exists $y' \in \mathcal{O}_K$ such that $yy' \equiv 1 \bmod \pi$ and so $(xy')^2 \equiv -d \bmod \pi$. By Lemma 3.1.2, $(-dm/p) = 1$. This is a contradiction.

Suppose that $(m/p) = (-d/p) = 1$ or $(m/p) = -1$. By Lemma 2.4.5 and Lemma 2.4.8, π splits completely in L. Thus $\pi\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. Since L is a PID, we may let $\mathfrak{p}_1 = (\frac{r+s\sqrt{m}}{2} + \sqrt{-d}\frac{t+u\sqrt{m}}{2})$ and $\mathfrak{p}_2 = (\frac{r+s\sqrt{m}}{2} - \sqrt{-d}\frac{t+u\sqrt{m}}{2})$. Then $\pi\mathcal{O}_L = ((\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2)$. Since a unit of $\mathcal{O}_L$ is of the form $\pm u^l$ and π is positive, $\pi = u^l((\frac{r+s\sqrt{m}}{2})^2 + d(\frac{t+u\sqrt{m}}{2})^2)$. Since π is totally positive, l is even and $\pi = (\frac{r+s\sqrt{m}}{2}u^{l/2})^2 + d(\frac{t+u\sqrt{m}}{2}u^{l/2})^2$.
For $m \equiv 1 \bmod 4$ and $-d \equiv 2, 3 \bmod 4$, $\frac{r+s\sqrt{m}}{2}u^{l/2}$, $\frac{t+u\sqrt{m}}{2}u^{l/2} \in \mathcal{O}_K$ and so π can be written in the form $x^2 + dy^2$.
For $m \equiv 2, 3 \bmod 4$ and $-d \equiv 1 \bmod 4$, we have 4π is of the form $(r + s\sqrt{m})^2 + d(t + u\sqrt{m})^2$.

Next, assume that one of the r, s, t and u is odd. Suppose on the contrary that π can be written in the form $(x + y\sqrt{m})^2 + d(z + w\sqrt{m})^2$. Then $((x + y\sqrt{m}) + \sqrt{-d}(z + w\sqrt{m})) = ((\frac{r+s\sqrt{m}}{2}) + \sqrt{-d}(\frac{t+u\sqrt{m}}{2}))$ which implies that $(\frac{r+s\sqrt{m}}{2}) + \sqrt{-d}(\frac{t+u\sqrt{m}}{2}) = \pm u^l((x + y\sqrt{m}) + \sqrt{-d}(z + w\sqrt{m}))$. This is a contradiction. □

Example 3.1.6. Let π be a totally positive prime integer in $K = \mathbb{Q}(\sqrt{29})$ such that $\pi\mathcal{O}_K$ lies over a prime p in $\mathbb{Z}$.
(i) If $p = 2$, then π cannot be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$.
(ii) If $p = 29$, then π can be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$.

(iii) If $p \neq 2, 29$, then π can be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$ if and only if $(29/p) = (-2/p) = 1$ or $(29/p) = -1$.

Proof. (i) For $p = 2$, p is inert in K and so $\pi = (\frac{5+\sqrt{29}}{2})^l 2$. Since π is totally positve, l is even. Thus $\pi = x^2 + 2y^2$ by setting $x = 0$ and $y = (\frac{5+\sqrt{29}}{2})^{l/2}$.
(ii) For $p = 29$, p is ramified in K and so $\pi = (\frac{5+\sqrt{29}}{2})^l \sqrt{29}$. Suppose for a contradiction that $\pi = x^2 + 2y^2$ for some $x, y \in \mathcal{O}_K$. Then $(\frac{5+\sqrt{29}}{2})^l \sqrt{29} = (\frac{r+s\sqrt{29}}{2})^2 + 2(\frac{t+u\sqrt{29}}{2})^2$ where $r \equiv s \bmod 2$ and $t \equiv u \bmod 2$. Since π is totally positive, l is odd. Thus $(\frac{5+\sqrt{29}}{2})\sqrt{29} = (\frac{R+S\sqrt{29}}{2})^2 + 2(\frac{T+U\sqrt{29}}{2})^2$ for some $R, S, T, U \in \mathbb{Z}$. Hence $R^2 + 29S^2 + 2T^2 + 58U^2 = 58$ and so $R = S = T = 0$ and $U = \pm 1$. This is a contradiction.
(iii) The result follows immediately from Theorem 3.1.5. □

Theorem 3.1.7. *Let π be a totally positive prime integer in $K = \mathbb{Q}(\sqrt{2})$ such that $\pi\mathcal{O}_K$ lies over a prime p in $\mathbb{Z}$.*
(i) If $p = 2$, then π cannot be written in the form $x^2 + 11y^2$ where $x, y \in \mathcal{O}_K$.
(ii) If $p = 11$, then π can be written in the form $x^2 + 11y^2$ where $x, y \in \mathcal{O}_K$.
(iii) If $(2/p) = 1$ and $(-11/p) = -1$, then π cannot be written in the form $x^2 + 11y^2$ where $x, y \in \mathcal{O}_K$
(iv) If $(2/p) = 1$ and $(-11/p) = 1$ or $(2/p) = -1$, then 4π can be written in the form $(a + b\sqrt{2})^2 + 11(c + d\sqrt{2})^2$ where a, b, c and d are rational integers. Furthermore, if one of the numbers a, b, c and d is odd, then π cannot be written in the form $x^2 + 11y^2$ where $x, y \in \mathcal{O}_K$.

Proof. (i) For $p = 2$, $\pi = (1 + \sqrt{2})^l \sqrt{2}$ where $l \in \mathbb{Z}$. Since the coefficient of $\sqrt{2}$ in π is odd, π cannot be written in the form $x^2 + 11y^2$.
(ii) For $p = 11$, p is inert in K and so $\pi = (1 + \sqrt{2})^l 11$ where $l \in \mathbb{Z}$. Since π is totally positive, l is even. Therefore π can be written in the form $x^2 + 11y^2$ by setting $x = 0$ and $y = (1 + \sqrt{2})^{l/2}$.
(iii) Assume that $(2/p) = 1$ and $(-11/p) = -1$. Suppose for a contradiction that $\pi = x^2 + 11y^2$ for some $x, y \in \mathcal{O}_K$. Then $x^2 \equiv -11y^2 \bmod \pi$. Since $(y, \pi) = 1$, there exists $y' \in \mathcal{O}_K$ such that $yy' \equiv 1 \bmod \pi$ and so $(xy')^2 \equiv -11 \bmod \pi$. By Lemma 3.1.2, $(-22/p) = 1$. This is a contradiction.

(iv) Assume that $(2/p) = (-11/p) = 1$ or $(2/p) = -1$. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{-11})$. By Lemma 2.4.5 and Lemma 2.4.8, π splits completely in L. Thus $\pi\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. Since $\mathbb{Q}(\sqrt{2}, \sqrt{-11})$ is a PID, we may let $\mathfrak{p}_1 = (\frac{A+B\sqrt{2}}{2} + \sqrt{-11}\frac{C+D\sqrt{2}}{2})$ and $\mathfrak{p}_2 = (\frac{A+B\sqrt{2}}{2} - \sqrt{-11}\frac{C+D\sqrt{2}}{2})$. Then $\pi\mathcal{O}_L = ((\frac{A+B\sqrt{2}}{2})^2 + 11(\frac{C+D\sqrt{2}}{2})^2)$. Since a unit of $\mathcal{O}_L$ is of the form $\pm(1+\sqrt{2})^l$, $\pi = \pm(1+\sqrt{2})^l((\frac{A+B\sqrt{2}}{2})^2 + 11(\frac{C+D\sqrt{2}}{2})^2)$. Since π is totally positive, l is even and $\pi = (\frac{A+B\sqrt{2}}{2}(1+\sqrt{2})^{l/2})^2 + 11(\frac{C+D\sqrt{2}}{2}(1+\sqrt{2})^{l/2})^2$. Hence 4π is of the form $(a+b\sqrt{2})^2 + 11(c+d\sqrt{2})^2$.

Next, assume that one of the a, b, c and d is odd. Suppose on the contrary that π can be written in the form $(x+y\sqrt{2})^2 + 11(z+w\sqrt{2})^2$. Then $((x+y\sqrt{2}) + \sqrt{-11}(z+w\sqrt{2})) = ((\frac{a+b\sqrt{2}}{2}) + \sqrt{-11}(\frac{c+d\sqrt{2}}{2}))$ which implies that $(\frac{a+b\sqrt{2}}{2}) + \sqrt{-11}(\frac{c+d\sqrt{2}}{2}) = \pm(1+\sqrt{2})^l((x+y\sqrt{2}) + \sqrt{-11}(z+w\sqrt{2}))$. This is a contradiction.

□

3.2 General Case

In this section we will solve the same problem for more values of n and d without condition on class numbers by using Hilbert class fields.

The Hilbert class field M of a number field L is defined to be the maximal unramified abelian extension of L. The following properties of the Hilbert class field will be used. First, for any prime ideal $\mathfrak{p}$ of L,

$$\mathfrak{p} \text{ splits completely in } M \iff \mathfrak{p} \text{ is a principal ideal} \tag{3.1}$$

and secondly the Galois group of M over L is isomophic to the ideal class group of L, i.e.,

$$\mathrm{Gal}(M/L) \simeq C(\mathcal{O}_L).$$

We use the first property in the main theorem and the second property to compute the Hilbert class field.

Throughout this section, we let $K = \mathbb{Q}(\sqrt{m})$ and $L = \mathbb{Q}(\sqrt{m}, \sqrt{-d})$ where m and d are positive squarefree integers such that $m \equiv 1 \bmod 4$ and $N(u_0) = -1$ where u_0 is a fundamental unit of $\mathbb{Q}(\sqrt{m})$, $-d \equiv 2, 3 \bmod 4$ and $(m, d) = 1$. First, we investigate the ring of integers $\mathcal{O}_L$ and the unit group $\mathcal{O}_L^\times$ of L.

Lemma 3.2.1. $\mathcal{O}_L = \mathcal{O}_K[\sqrt{-d}]$.

Proof. Since $m \equiv 1 \bmod 4, -d \equiv 2, 3 \bmod 4$ and $(m, d) = 1$, $\{1, \frac{1+\sqrt{m}}{2}, \sqrt{-d}, \frac{\sqrt{-d}+\sqrt{-dm}}{2}\}$ is an integral basis of L, i.e. $\mathcal{O}_L = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2} \oplus \mathbb{Z} \cdot \sqrt{-d} \oplus \mathbb{Z} \cdot \frac{\sqrt{-d}+\sqrt{-dm}}{2}$. Then

$$\begin{aligned} e \in \mathcal{O}_L &\Leftrightarrow e = x + y(\frac{1+\sqrt{m}}{2}) + z\sqrt{-d} + w(\frac{\sqrt{-d}+\sqrt{-dm}}{2}) \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = (\frac{2x+y}{2} + \frac{y}{2}\sqrt{m}) + (\frac{2z+w}{2} + \frac{w}{2}\sqrt{m})\sqrt{-d} \text{ for some } x, y, z, w \in \mathbb{Z} \\ &\Leftrightarrow e = a + b\sqrt{-d} \text{ for some } a, b \in \mathcal{O}_K. \end{aligned}$$

Therefore $\mathcal{O}_L = \mathcal{O}_K[\sqrt{-d}]$. □

Lemma 3.2.2. *Let u_0 be the fundamental unit of K. Then*

$$\mathcal{O}_L^\times = \begin{cases} \{\pm u_0^l, \pm i u_0^l \mid l \in \mathbb{Z}\} & , \text{ if } d = 1 \\ \{\pm u_0^l \mid l \in \mathbb{Z}\} & , \text{ if } d > 1 \end{cases}.$$

Proof. Let $u \in \mathcal{O}_L^\times$. Then $u = (\frac{x+y\sqrt{m}}{2}) + \sqrt{-d}(\frac{z+w\sqrt{m}}{2})$ where $x \equiv y \bmod 2$ and $z \equiv w \bmod 2$. Since u is a unit of $\mathcal{O}_L$, $\mathrm{N}_{L/K}(u)$ is a unit of $\mathcal{O}_K$ and so $(\frac{x+y\sqrt{m}}{2})^2 + d(\frac{z+w\sqrt{m}}{2})^2 = u_0^{l_0}$ for some $l_0 \in \mathbb{Z}$. Since the term in the left hand side is totally positive, $u_0^{l_0}$ is also totally positive and so l_0 is even. Thus $l_0 = 2l$ for some $l \in \mathbb{Z}$. Let X, Y, Z and W be integers such that $\frac{X+Y\sqrt{m}}{2} = \frac{x+y\sqrt{m}}{2} u_0^{-l}$ and $\frac{Z+W\sqrt{m}}{2} = \frac{z+w\sqrt{m}}{2} u_0^{-l}$. Then $(\frac{X+Y\sqrt{m}}{2})^2 + d(\frac{Z+W\sqrt{m}}{2})^2 = 1$ and hence $X^2 + mY^2 + dZ^2 + dmW^2 = 4$. Since $m \geq 5, Y = W = 0$. If $d = 1$, then $X = \pm 2, Z = 0$ or $X = 0, Z = \pm 2$ and so $u = \pm u_0^l$ or $u = \pm i u_0^l$. If $d > 1$, then $X = \pm 2, Z = 0$ and so $u = \pm u_0^l$. □

The following lemma is an immediate consequence of Theorem 2.4.5 and Theorem 2.4.8.

Lemma 3.2.3. *Let $E = \mathbb{Q}(\sqrt{m})$ and $F = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ where m and n are distinct squarefree integers and $k = \frac{mn}{d^2}$ where $d = (m, n)$. Let P be a prime in E such that $P\mathcal{O}_E$ lies over an odd prime p in $\mathbb{Z}$ where $p \nmid mn$. Then*

(i) P is unramified in F, and

(ii) P splits completely in $F \iff (n/p) = (m/p) = 1$ or $(m/p) = -1$.

Proposition 3.2.4. *Let $E \subset F$ be a Galois extension, where $F = E(\alpha)$ for some $\alpha \in \mathcal{O}_F$. Let $f(x) \in \mathcal{O}_E[x]$ be the monic minimal polynomial of α over E. If $\mathfrak{p}$ is a prime in $\mathcal{O}_E$ and $f(x)$ is separable modulo $\mathfrak{p}$, then*

$$\mathfrak{p} \text{ splits completely in } F \iff f(x) \equiv 0 \bmod \mathfrak{p} \text{ has a solution in } \mathcal{O}_E.$$

These are the main results of this section

Lemma 3.2.5. *Let M be the Hilbert class field of L and let τ denote the complex conjugation. Then $\tau(M) = M$ and consequently M is Galois over K.*

Proof. Since M is an unramified abelian extension of L, $\tau(M)$ is an unramified abelian extension of $\tau(L) = L$. Since M is the maximal such extension, we have $\tau(M) \subset M$ and then $\tau(M) = M$ since they have the same degree over L. Then $\tau \in \mathrm{Gal}(M/K)$. To show M is Galois over K, it suffices to show that $\mathrm{Fix}(\mathrm{Gal}(M/K)) \subset K$. Let $u \in \mathrm{Fix}(\mathrm{Gal}(M/K))$. Then $u \in M$ and $\sigma(u) = u$ for all $\sigma \in \mathrm{Gal}(M/K)$. Since $K \subset L$ and M is Galois over L, $\mathrm{Fix}(\mathrm{Gal}(M/K)) \subset \mathrm{Fix}(\mathrm{Gal}(M/L)) = L$. Therefore $u \in L$. Let $u = x + y\sqrt{-d}$ where $x, y \in K$. Since $\tau(u) = u, y = 0$. Hence $u \in K$. □

Theorem 3.2.6. *Let M be the Hilbert class field of L. If π is a totally positive prime in $\mathcal{O}_K$ such that $\pi\mathcal{O}_K$ lies over an odd prime p where $p \nmid nd$, then*

$$\pi = x^2 + dy^2 \text{ for some } x, y \in \mathcal{O}_K \Longleftrightarrow \pi \text{ splits completely in } M.$$

Proof. Let π be a totally positive prime in $\mathcal{O}_K$ such that $\pi\mathcal{O}_K$ lies over an odd prime p where $p \nmid nd$. By Lemma 3.2.3, π is unramified in L. Next, claim that

$$\begin{aligned} \pi = x^2 + dy^2 &\Leftrightarrow \pi\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ and } \mathfrak{p} \text{ is principal in } \mathcal{O}_L \\ &\Leftrightarrow \pi\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ and } \mathfrak{p} \text{ splits completely in } M \\ &\Leftrightarrow \pi \text{ splits completely in } M. \end{aligned}$$

To prove the first equivalence, suppose that $\pi = x^2 + dy^2 = (x + \sqrt{-d}y) \cdot (x - \sqrt{-d}y)$. Setting $\mathfrak{p} = (x + \sqrt{-d}y)\mathcal{O}_L$, then $\bar{\mathfrak{p}} = (x - \sqrt{-d}y)\mathcal{O}_L$ and $\pi\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}$ must be the prime decomposition of $\pi\mathcal{O}_L$ in $\mathcal{O}_L$. Note that $\mathfrak{p} \neq \bar{\mathfrak{p}}$ since π is unramified in L. Conversely, suppose that $\pi\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $\mathfrak{p}$ is principal. We can write $\mathfrak{p} = (x_0 + \sqrt{-d}y_0)\mathcal{O}_L$. This implies that $\bar{\mathfrak{p}} = (x_0 - \sqrt{-d}y_0)\mathcal{O}_L$ and $\pi\mathcal{O}_L = (x_0^2 + dy_0^2)\mathcal{O}_L$, by Lemma 3.2.2, it follows that $\pi = u_0^l(x_0^2 + dy_0^2)$. Since π and $x_0^2 + dy_0^2$ are totally positive, u_0^l is totally positive. Thus $\bar{u}_0^l > 0$. Since $\mathrm{N}(u_0) = -1$, $\bar{u}_0 < 0$ and so l is even. Therefore $\pi = x^2 + dy^2$ where $x = x_0 u_0^{l/2}$ and $y = y_0 u_0^{l/2}$.

The second equivalence follows from (3.1) and the third one follows immediately from Lemma 3.2.5 and the fact that if $K \subset L \subset M$, where M and L are Galois over K, then a prime π of $\mathcal{O}_K$ splits completely in M if and only if it splits completely in L and some prime of $\mathcal{O}_L$ containing π splits completely in M. □

The next step is to give a more elementary way of saying that π splits completely in M. We have the following criterion:

Theorem 3.2.7. *Let M be the Hilbert class field of L. Then*
(i) there is a real algebraic integer α such that $M = L(\alpha)$, and
(ii) if $f(x) \in \mathcal{O}_K[x]$ is its monic minimal polynomial and π is as in Theorem 3.2.6 which does not divide the discriminant of $f(x)$, then

$$\pi \text{ splits completely in } M \iff \left(\begin{array}{c} (m/p) = (-d/p) = 1 \text{ or } (m/p) = -1 \text{ and} \\ f(x) \equiv 0 \bmod \pi \text{ has a solution in } \mathcal{O}_K \end{array} \right).$$

Proof. (i) Since $K \subset M \cap \mathbb{R}$ is finite separable extension, $M \cap \mathbb{R} = K(\alpha)$ for some $\alpha \in \mathcal{O}_M \cap \mathbb{R}$. Then $[M : K(\alpha)] = [M : M \cap \mathbb{R}] = [M\mathbb{R} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$. Since $K(\alpha) \subset L(\alpha) \subset M$, $L(\alpha) = K(\alpha)$ or $M = L(\alpha)$. Since α is real and K is a real quadratic field, $L(\alpha) \neq K(\alpha)$. Therefore $M = L(\alpha)$.

(ii) Let $f(x) \in \mathcal{O}_K[x]$ be the monic minimal polynomial of α over K. Since $[L(\alpha) : K(\alpha)] = [L : K] = 2$, $[L(\alpha) : L] = [K(\alpha) : K]$. Thus $f(x)$ is also the monic mimimal polynomial of α over L. Let π be a prime not dividing the discriminant of $f(x)$. This tells us that $f(x)$ is separable modulo π. By Lemma 3.2.3 we have

$$\pi\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \iff (m/p) = (-d/p) = 1 \text{ or } (m/p) = -1.$$

We may assume that π splits completely in L, so that $\mathcal{O}_K/\pi\mathcal{O}_K \simeq \mathcal{O}_L/\mathfrak{p}$. Since $f(x)$ is separable over $\mathcal{O}_K/\pi\mathcal{O}_K$, it is separable over $\mathcal{O}_L/\mathfrak{p}$, and then Proposition 3.2.4 shows that

$$\begin{aligned} \mathfrak{p} \text{ splits completely in } M &\iff f(x) \equiv 0 \bmod \mathfrak{p} \text{ is solvable in } \mathcal{O}_L \\ &\iff f(x) \equiv 0 \bmod \pi \text{ is solvable in } \mathcal{O}_K. \end{aligned}$$

The theorem now follows from the last equivalence in the proof of Theorem 3.2.6. □

In order to use Theorem 3.2.6, we need to compute the Hilbert class field M of L. We know from Theorem 2.6.8 that

$$[M : L] = |\mathrm{Gal}(M/L)| = |C(\mathcal{O}_L)| = h_L.$$

Thus the degree of M over L is the class number of L. Cohn [5] gives the formula to compute the class number of a biquadratic field. Thus we will use these facts to find the Hilbert class field in the following theorems.

Theorem 3.2.8. *Let π be a totally positive prime in $K = \mathbb{Q}(\sqrt{5})$ such that $\pi\mathcal{O}_K$ lies over a prime p in $\mathbb{Z}$.*
(i) If $p = 2$, then π can be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$.
(ii) If $p = 5$, then π cannot be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$.
(iii) If $p \neq 2, 5$, then π can be written in the form $x^2 + 2y^2$ where $x, y \in \mathcal{O}_K$ if and only if $(5/p) = (-2/p) = 1$ or $(5/p) = -1$.

Proof. (i) For $p = 2$, p is inert in K and so $\pi = (\frac{1+\sqrt{5}}{2})^l 2$ where $l \in \mathbb{Z}$. Since π is totally positive, l is even. Thus π can be written in the form $x^2 + 2y^2$ by setting $x = 0$ and $y = (\frac{1+\sqrt{5}}{2})^{l/2}$.
(ii) For $p = 5$, p is ramified in K and so $\pi = (\frac{1+\sqrt{5}}{2})^l\sqrt{5}$. Suppose for a contradiction that $\pi = x^2 + 2y^2$ for some $x, y \in \mathcal{O}_K$. Then $(\frac{1+\sqrt{5}}{2})^l\sqrt{5} = (\frac{a+b\sqrt{5}}{2})^2 + 2(\frac{c+d\sqrt{5}}{2})^2$ where $a \equiv b \bmod 2$ and $c \equiv d \bmod 2$. Since π is totally positive, l is odd. Thus $(\frac{1+\sqrt{5}}{2})\sqrt{5} = (\frac{A+B\sqrt{5}}{2})^2 + 2(\frac{C+D\sqrt{5}}{2})^2$ for some $A, B, C, D \in \mathbb{Z}$. Hence $A^2 + 5B^2 + 2C^2 + 10D^2 = 10$ and so $A = B = C = 0$ and $D = \pm 1$. This is a contradiction.
(iii) Let $p \neq 2, 5$. Since the class number of $L = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$ is 1. Then the Hilbert class field of L is the field L itself. By Theorem 3.2.6 and Theorem 3.2.7, we have $\pi = x^2 + 2y^2$ for some $x, y \in \mathcal{O}_K$ if and only if $(5/p) = (-2/p) = 1$ or $(5/p) = -1$. □

Theorem 3.2.9. *Let π be a totally positive prime in $K = \mathbb{Q}(\sqrt{17})$ such that $\pi\mathcal{O}_K$ lies over a prime p in $\mathbb{Z}$.*
(i) If $p = 2$, then π cannot be written in the form $x^2 + y^2$ where $x, y \in \mathcal{O}_K$.
(ii) If $p = 17$, then π can be written in the form $x^2 + y^2$ where $x, y \in \mathcal{O}_K$.
(iii) If $p \neq 2, 17$, then π can be written in the form $x^2 + y^2$ where $x, y \in \mathcal{O}_K$ if and only if $(17/p) = (-1/p) = 1$ or $(17/p) = -1$ and $X^2 \equiv \frac{1+\sqrt{17}}{2} \bmod \pi$ has a solution in $\mathcal{O}_K$.

Proof. (i) For $p = 2$, p splits completely in K and so $\pi = (4+\sqrt{17})^l(\frac{5\pm\sqrt{17}}{2})$ where $l \in \mathbb{Z}$. Suppose for a contradiction that $\pi = x^2 + y^2$ for some $x, y \in \mathcal{O}_K$. Then $\pi = (\frac{a+b\sqrt{17}}{2})^2 + (\frac{c+d\sqrt{17}}{2})^2$ where $a \equiv b \bmod 2$ and $c \equiv d \bmod 2$. Since π is totally positive, l is even and so $\frac{5\pm\sqrt{17}}{2} = (\frac{A+B\sqrt{17}}{2})^2 + (\frac{C+D\sqrt{17}}{2})^2$ for some $A, B, C, D \in \mathbb{Z}$. Hence $A^2 + 17B^2 + C^2 + 17D^2 = 10$ and so $B = D = 0$. This is a contradiction.
(ii) For $p = 17$, p is ramified in K and so $\pi = (4 + \sqrt{17})^l\sqrt{17}$ where $l \in \mathbb{Z}$. Since π is totally positive, l is odd. Then

$$\pi = \left((4 + \sqrt{17})^{(l-1)/2}(\frac{3 + \sqrt{17}}{2})\right)^2 + \left((4 + \sqrt{17})^{(l-1)/2}(\frac{5 + \sqrt{17}}{2})\right)^2.$$

(iii) Let $p \neq 2, 17$. We know that the class number of $L = \mathbb{Q}(\sqrt{17}, \sqrt{-1})$ is 2 and the Hilbert class field of $\mathbb{Q}(\sqrt{-17})$ is $\mathbb{Q}(\sqrt{-17}, \sqrt{\frac{1+\sqrt{17}}{2}})$ (see [6] p. 120). Since $\mathbb{Q}(\sqrt{-17}) \subset L \subset L(\frac{1+\sqrt{17}}{2}) = \mathbb{Q}(\sqrt{-17}, \sqrt{\frac{1+\sqrt{17}}{2}})$, $L(\sqrt{\frac{1+\sqrt{17}}{2}})$ is also a Hilbert class field of L. Note that the minimal polynomial of $\sqrt{\frac{1+\sqrt{17}}{2}}$ over K is $f(x) = X^2 - \frac{1+\sqrt{17}}{2}$. By Theorem 3.2.6 and Theorem 3.2.7, we have $\pi = x^2 + 2y^2$ if and only if $(17/p) = (-1/p) = 1$ or $(17/p) = -1$ and $X^2 \equiv \frac{1+\sqrt{17}}{2} \bmod \pi$ has a solution in $\mathcal{O}_K$. □

CHAPTER IV
THE NUMBERS OF REPRESENTATIONS OF INTEGERS OF THE FORM $x^2 + dy^2$ IN NUMBER FIELDS

4.1 Preliminaries

There are many papers [6], [14], [15] which give the criteria to determine whether an algebraic integer can be represented in the form x^2+dy^2 where x, y are algebraic integers and d is a positive rational integer. Another interesting problem about algebraic integers of the form $x^2 + dy^2$ where x, y are algebraic integers and d is positive rational integer is to study the number of these representations. T. Nagell [16] study the problem of the number of the representation of an integer which can be represented as the sums of two squares. We will generalize the result of T. Nagell to the representations of an algebraic integer in a number field of the form $x^2 + dy^2$ where x, y are algebraic integers and d is a positive rational integer.

Let ω be an integer in a number field K and d a positive rational integer. We say that ω *has a representation of the form* x^2+dy^2 if there are integers α and β in K such that $\omega = \alpha^2 + d\beta^2$. The representation $\omega = x^2 + y^2$ with $x = \pm\alpha, y = \pm\beta$ and $x = \pm\beta, y = \pm\alpha$ and the representation $\omega = x^2 + dy^2$ for $d > 1$ with $x = \pm\alpha$ and $y = \pm\beta$ are considered to be one and the same. The relation $1 = 1^2 + d \cdot 0^2$ is called the *trivial representation* of the number 1.

Let K be a number field of degree $n = r + 2s$ over $\mathbb{Q}$ where r is the number of real embeddings of K and s is the number of nonconjugate complex embeddings of K. Then $\mathcal{O}_K^\times \cong \mathcal{W}_K \times V$ where $\mathcal{W}_K$ is the cyclic group of even order of all roots of unity in K and V is a free abelian group of rank $t = r + s - 1$, i.e., there are units $u_1, \ldots, u_t$ such that for all $u \in \mathcal{O}_K^\times$, u can be written uniquely in the form

$u = wu_1^{a_1}, \ldots, u_t^{a_t}$ where $a_i \in \mathbb{Z}$ and $w \in \mathcal{W}_K$.

4.2 The Numbers of Representations of Integers of the Form $x^2 + dy^2$ in Number Fields

Theorem 4.2.1. *Let K be a number field. If 1 has more representations of the form $x^2 + dy^2$ than the trivial representation, then 1 has infinitely many representations.*

Proof. Assume that

$$1 = \gamma^2 + d\delta^2$$

where γ and δ are integers in K such that $\gamma \neq 1$ and $\delta \neq 0$.
For positive integer n, we define

$$\gamma_n + \delta_n\sqrt{-d} = (\gamma + \delta\sqrt{-d})^n,$$

where

$$\gamma_n = \gamma^n - \binom{n}{2}\gamma^{n-2}\delta^2 d + \binom{n}{4}\gamma^{n-4}\delta^4 d^2 - + \ldots \tag{4.1}$$

and

$$\delta_n = \binom{n}{1}\gamma^{n-1}\delta - \binom{n}{3}\gamma^{n-3}\delta^3 d + - \ldots. \tag{4.2}$$

Then

$$\gamma_n - \delta_n\sqrt{-d} = (\gamma - \delta\sqrt{-d})^n$$

and

$$(\gamma_n + \delta_n\sqrt{-d})(\gamma_n - \delta_n\sqrt{-d}) = (\gamma + \delta\sqrt{-d})^n(\gamma - \delta\sqrt{-d})^n = (\gamma^2 + d\delta^2)^n.$$

Therefore

$$\gamma_n^2 + d\delta_n^2 = 1.$$

Thus the Diophantine equation

$$x^2 + dy^2 = 1 \tag{4.3}$$

has the integral solutions

$$x = \gamma_n, y = \delta_n.$$

Next, we will prove that these solutions are all different.

Suppose for a contradiction that there are $m, n \in \mathbb{N}$ such that $m \neq n$ and

$$\gamma_m = \gamma_n, \delta_m = \delta_n.$$

Then

$$(\gamma + \delta\sqrt{-d})^m = (\gamma + \delta\sqrt{-d})^n,$$

and so $\gamma + \delta\sqrt{-d}$ is a root of unity. Suppose that

$$\gamma + \delta\sqrt{-d} = \zeta$$

is a primitive Nth root of unity. Since

$$\gamma - \delta\sqrt{-d} = \zeta^{-1},$$

we get

$$\gamma = \frac{1}{2}(\zeta + \zeta^{-1}), \delta = \frac{1}{2\sqrt{-d}}(\zeta - \zeta^{-1}).$$

Thus

$$\frac{1}{2}(\zeta^2 - 1) = \sqrt{-d}\zeta\delta$$

is an algebraic integer.

If N is a power of 2 and $N \geq 8$, then the number

$$\frac{1}{2}(\zeta^{N/4} - 1) = \frac{1}{2}(\pm i - 1)$$

must also be an algebraic integer. This is a contradiction.

If N is divisible by the odd prime p, then the number

$$\frac{1}{2}(\zeta^{2N/p} - 1)$$

must also be an algebraic integer but $\frac{1}{2}(\zeta^{2N/p} - 1)$ is the root of the irreducible polynomial

$$\frac{1}{2x}[(2x+1)^p - 1] = 2^{p-1}x^{p-1} + \ldots + p(p-1)x + p$$

which has integral coefficients. This is a contradiction.
Finally, if $N = 1, 2, 4$, then $\gamma = 0$ or δ is not algebraic integer. This is a contradiction. □

Theorem 4.2.2. *Let K be a number field.*
(i) Let π be a prime or a unit in K such that π has a representation of the form $x^2 + dy^2$. If 1 has only trivial representation, then π has exactly one representation. Otherwise π has infinitely many representations.
(ii) Let ω be an integer in K such that ω has a representation of the form x^2+dy^2. If 1 has only trivial representation, then ω has a finite number of the representations. Otherwise, ω has infinitely many representations.

Proof. (i) Assume that 1 has only trivial representation Let π be a prime in K such that π has two representations of the form $x^2 + dy^2$,

$$\pi = \alpha_1^2 + d\beta_1^2$$

and

$$\pi = \alpha_2^2 + d\beta_2^2$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are integers in K. Then

$$\pi(\beta_2^2 - \beta_1^2) = \alpha_1^2\beta_2^2 - \alpha_2^2\beta_1^2.$$

Since π is a prime, either $\alpha_1\beta_2 - \alpha_2\beta_1$ or $\alpha_1\beta_2 + \alpha_2\beta_1$ must be divisible by π. Without loss of generality, we may assume that

$$\alpha_1\beta_2 \equiv \alpha_2\beta_1 \bmod \pi.$$

Multiplying together the two representations of π, we get

$$\pi^2 = (\alpha_1\alpha_2 + d\beta_1\beta_2)^2 + d(\alpha_1\beta_2 - \alpha_2\beta_1)^2.$$

Since $\alpha_1\beta_2 - \alpha_2\beta_1$ is divisible by π, so is the number $\alpha_1\alpha_2 + d\beta_1\beta_2$. We put

$$\alpha_1\alpha_2 + d\beta_1\beta_2 = \pi\gamma \text{ and } \alpha_1\beta_2 - \alpha_2\beta_1 = \pi\delta,$$

where γ, δ are integers in K, we get

$$1 = \gamma^2 + d\delta^2.$$

Since 1 has only trivial representation, $\gamma = \pm 1$ and $\delta = 0$. Therefore

$$\alpha_1\alpha_2 + d\beta_1\beta_2 = \pm\pi \text{ and } \alpha_1\beta_2 - \alpha_2\beta_1 = 0.$$

Then

$$\alpha_2 = \frac{\beta_2}{\beta_1}\alpha_1 \text{ and } \frac{\beta_2}{\beta_1}\alpha_1^2 + d\beta_1\beta_2 = \pm\pi,$$

and so

$$\frac{\beta_2}{\beta_1}\pi = \frac{\beta_2}{\beta_1}(\alpha_1^2 + d\beta_1^2) = \frac{\beta_2}{\beta_1}\alpha_1^2 + d\beta_1\beta_2 = \pm\pi.$$

Hence $\beta_2 = \pm\beta_1$ and $\alpha_2 = \pm\alpha_1$ and so π has exactly one representation.

Suppose next that the equation (4.3) has an infinitely of solutions $x = \gamma_n, y = \delta_n$ given by (4.1) and (4.2). Let π be a prime in K such that

$$\pi = \alpha^2 + d\beta^2$$

where α and β are integers in K. For positive integer n, define

$$\alpha_n + \beta_n\sqrt{-d} = (\gamma_n + \delta_n\sqrt{-d})(\alpha + \beta\sqrt{-d})$$

where

$$\alpha_n = \alpha\gamma_n - d\beta\delta_n \text{ and } \beta_n = \alpha\delta_n + \beta\gamma_n.$$

Thus

$$\alpha_n - \beta_n\sqrt{-d} = (\gamma_n - \delta_n\sqrt{-d})(\alpha - \beta\sqrt{-d})$$

and

$$(\alpha_n + \beta_n\sqrt{-d})(\alpha_n - \beta_n\sqrt{-d}) = (\gamma^2 + d\delta^2)(\alpha^2 + d\beta^2) = \pi.$$

Hence

$$\pi = \alpha_n^2 + d\beta_n^2.$$

We will show that these are all different representations of π.

Suppose for a contradiction that there are $m, n \in \mathbb{N}$ such that $m \neq n$ and

$$\alpha_m = \alpha_n, \beta_m = \beta_n.$$

Then we get

$$\gamma_m = \gamma_n, \delta_m = \delta_n.$$

But in the proof of Theorem 4.2.1, $\gamma_m = \gamma_n, \delta_m = \delta_n.$ where $m \neq n$ leads to a contradiction. Therefore π has infinitely many representations.

(ii) Assume that 1 has only trivial representation. Let ω be an integer in K. Suppose for a contradiction that ω has infinitely many representations, i.e.,

$$\omega = \alpha_n^2 + d\beta_n^2, n \in \mathbb{N}$$

where α_n and β_n are integers in K and for $m \neq n$, $\alpha_n \neq \pm\alpha_m$ and $\beta_n \neq \pm\beta_m$. Since $\mathcal{O}_K/\omega\mathcal{O}_K$ is finite, there are $m, n \in \mathbb{N}$ such that $m \neq n$ and

$$\alpha_m \equiv \alpha_n \bmod \omega \text{ and } \beta_m \equiv \beta_n \bmod \omega. \tag{4.4}$$

Multiplying the two represeentations

$$\omega = \alpha_m^2 + d\beta_m^2 \text{ and } \omega = \alpha_n^2 + d\beta_n^2,$$

we get

$$\omega^2 = (\alpha_m\alpha_n + d\beta_m\beta_n)^2 + d(\alpha_m\beta_n - \alpha_n\beta_m)^2.$$

It follows from (4.4) that the two numbers

$$\alpha_m\alpha_n + d\beta_m\beta_n \text{ and } \alpha_m\beta_n - \alpha_n\beta_m$$

are divisible by ω. Hence we may put

$$\alpha_m\alpha_n + d\beta_m\beta_n = \omega\gamma \text{ and } \alpha_m\beta_n - \alpha_n\beta_m = \omega\delta$$

where γ and δ are integers in K. Then

$$1 = \gamma^2 + d\delta^2.$$

Since 1 has only trivial representation, $\gamma = \pm 1$ and $\delta = 0$. It follows that

$$\alpha_m\alpha_n + d\beta_m\beta_n = \pm\omega \text{ and } \alpha_m\beta_n - \alpha_n\beta_m = 0.$$

Then

$$\alpha_n = \frac{\beta_n}{\beta_m}\alpha_m \text{ and } \frac{\beta_n}{\beta_m}\alpha_m^2 + d\beta_m\beta_n = \pm\omega,$$

and so

$$\frac{\beta_n}{\beta_m}\omega = \frac{\beta_n}{\beta_m}(\alpha_m^2 + d\beta_m^2) = \frac{\beta_n}{\beta_m}\alpha_m^2 + d\beta_n\beta_m = \pm\omega.$$

Hence $\beta_n = \pm\beta_m$ and $\alpha_n = \pm\alpha_m$. This is a contradiction and so the number of representations must be finite. □

Theorem 4.2.3. *Let K be a number field and d a positive rational integer. The following statements are equivalent.*
(i) $K = \mathbb{Q}(\sqrt{-d})$ or K is totally real.
(ii) 1 has only trivial representation in K.

Proof. Let K be a number field of degree n over $\mathbb{Q}$, r the number of real embeddings of K, s the number of nonconjugate complex embeddings of K and $t = r + s - 1$ the rank of the unit group of K. Assume that $K = \mathbb{Q}(\sqrt{-d})$ or K is totally real.
Case 1: $K = \mathbb{Q}(\sqrt{-d})$: Let α and β be integers in K such that

$$\alpha^2 + d\beta^2 = 1.$$

Then

$$(\alpha + \beta\sqrt{-d})(\alpha - \beta\sqrt{-d}) = 1.$$

Thus $\alpha + \beta\sqrt{-d}$ and $\alpha - \beta\sqrt{-d}$ are units in K. For $d \neq 1, 3$, the units in K are ± 1 so we have the following system

$$\alpha + \beta\sqrt{-d} = 1 \text{ and } \alpha - \beta\sqrt{-d} = 1$$

or

$$\alpha + \beta\sqrt{-d} = -1 \text{ and } \alpha - \beta\sqrt{-d} = -1$$

For $d = 1, 3$, we have more cases to figure out. Nevertheless, in either cases we have $\alpha = \pm 1$ and $\beta = 0$. Hence 1 has only trivial representation.
Case 2: K is totally real: Let α and β be integers in K such that

$$\alpha^2 + d\beta^2 = 1.$$

Then the conjugate equations

$$1 = (\sigma_k(\alpha))^2 + d(\sigma_k(\beta))^2$$

where $k = 1, \ldots, n$ also hold. Since the conjugates are all real, we get

$$|\sigma_k(\beta)| \leq \frac{1}{\sqrt{d}} < 1$$

for $k = 1, \ldots, n$ and $d > 1$. Thus $|\mathrm{N}(\beta)| = |\sigma_1(\beta)| \ldots |\sigma_n(\beta)| < 1$. Therefore $N(\beta) = 0$ and so $\beta = 0$ and $\alpha = \pm 1$. Hence 1 has only trivial representation.
For the converse, assume that $K \neq \mathbb{Q}(\sqrt{-d})$ and K is not totally real. We will prove that 1 has a nontrivial representation.
Case 1: $\sqrt{-d} \in K$. Since $K \neq \mathbb{Q}(\sqrt{-d}), n \geq 4$ and so $t \geq 1$. Thus there is a unit ϵ in K such that ϵ is not a root of unity. Then the equation

$$1 = \alpha^2 + d\beta^2$$

is satisfied by the following numbers:

$$\alpha = \frac{1}{2}(\epsilon^m + \epsilon^{-m}) \text{ and } \beta = \frac{1}{2\sqrt{-d}}(\epsilon^m - \epsilon^{-m}),$$

where m is the order of the group $(\mathcal{O}_K/2\sqrt{-d}\mathcal{O}_K)^\times$. Note that β is an integer in K because

$$\epsilon^m \equiv 1 \bmod 2\sqrt{-d} \text{ and } \epsilon^{-m} \equiv 1 \bmod 2\sqrt{-d}$$

and α is an integer in K because $\alpha = \sqrt{-d}\beta + \epsilon^{-m}$. Since ϵ is not a root of unity, $\beta \neq 0$. Hence 1 has a nontrivial representation.
Case 2: $\sqrt{-d} \notin K$. Let $L = K(\sqrt{-d})$. Then the field L has degree $2n$ over $\mathbb{Q}$. Let R be the number of real embeddings of L, S the number of nonconjugate complex embeddings of L and $T = R + S - 1$ the rank of the unit group of L. Since $\sqrt{-d} \notin \mathbb{R}$, $R = 0$ and $S = r + 2s$ and so

$$T = R + S - 1 = r + 2s - 1 = t + s.$$

Since K is not totally real, $s \geq 1$ and so

$$T > t.$$

Let us consider the ring consisting of the numbers in L of the form $\lambda + \rho\sqrt{-d}$, where λ and ρ are integers in K. The unit group G of this ring has the rank

T. The subgroup G_1 consisting of the squares of the units in G clearly has the same rank T. The units in G_1 cannot all be equal to the product of a unit in K and a root of unity since $t < T$. Hence we conclude that there exists a unit $E = a + b\sqrt{-d}$ in the ring, a and b integers in K such that $a \neq 1$ and $b \neq 0$, and such that E^2 is not equal to the product of a unit in K and a root of unity. Then the number $E_1 = a - b\sqrt{-d}$ is also a unit in L. Hence $a^2 + db^2$ is a unit in K. Then the equation

$$1 = \alpha^2 + d\beta^2$$

is satisfied by the following numbers:

$$\alpha = \frac{E^{2m} + E_1^{2m}}{2(a^2 + db^2)^m} \text{ and } \beta = \frac{E^{2m} - E_1^{2m}}{2\sqrt{-d}(a^2 + db^2)^m}$$

where $m \in \mathbb{N}$. Since $a^2 + db^2$ is a unit in K, α and β are integers in K. If $\beta = 0$, then $E^{2m} = E_1^{2m}$. Hence EE_1^{-1} must be a root of unity and

$$E^2 = (a^2 + db^2)(EE_1^{-1})$$

is a product of units and a root of unity. This is a contradiction. Thus $\beta \neq 0$ and so 1 has a nontrivial representation.

□

REFERENCES

[1] Arno, S.: The imaginary quadratic field of class number 4, *Acta Arithmetica* **60**, 321-334 (1992).

[2] Brown, E., Parry, C.J.: The imaginary bicyclic biquadratic fields with class-number 1, *Journal fur die reine und angewandte Mathematik* **266**, 118-120 (1974).

[3] Buell, D.A., Williams, H.C., Williams, K.S.: On the imaginary bicyclic biquadratic fields with class-number 2, *Mathematics of Computation* **31** 1034-1042 (1977).

[4] Cho, B.: Primes of the form $x^2 + ny^2$ with conditions $x \equiv 1 \bmod N, y \equiv 0 \bmod N$, *Journal of Number Theory* **130** 852-861 (2010).

[5] Cohn, H.: *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York, 1978.

[6] Cox, D.A.: *Prime of the Form $x^2 + dy^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Son, INC., 1989.

[7] Elia, M., Monico, C.: On the Representation of Primes in $\mathbb{Q}(\sqrt{2})$ as Sums of Squares, *The JP Journal of Algebra, Number Theory and Applications* **8**, 121-133 (2007).

[8] Fine, B.: A note on the two-square-theorem *Canadian Mathematical Bulletin* **20**, 93-94 (1977).

[9] Hourong, Q.: The sum of two squares in a quadratic field, *Communications in Algebra* **25**, 177-184 (1997).

[10] Kern-Isberner, G., Rosenberger, G.: A note on numbers of the form $n = x^2 + Ny^2$, *Archiv der Mathematik* **43**, 148-156 (1984).

[11] Kim, H.K., Kim, Y.M.: A classification of certain biquadratic fields of class number 1, *Bulletin of the Korean Mathematical Society* **28**, 15-21 (1991).

[12] Marcus, D.A.: *Number Fields*, Springer-Verlag, New York, 1977.

[13] Mollin, R.: *Algebraic Number Theory*, Chapman & Hall CRC, New York, 1999.

[14] Nagell, T.: On the sum of two integral squares in certain quadratic fields, *Arkiv for Matematik* **4**, 267-286 (1961).

[15] Nagell, T.: On the A-numbers in the quadratic fields $K(\sqrt{\pm 37})$, *Arkiv for Matematik* **4**, 511 -521 (1961).

[16] Nagell, T.: On the number of representations of an A-number in an algebraic field, *Arkiv for Matematik* **4**, 467 -478 (1961).

[17] Niven, I.: Integers of quadratic fields as sums of squares, *Transactions of the American Mathematical Society* **48**, 405 - 417 (1940).

[18] Ozgur, N.Y.: On numbers of the form $n = x^2 + Ny^2$ and the Hecke groups $H(\sqrt{N})$, *Journal of Number Theory* **120**, 1274-1281 (2010).

[19] Ribenboim, P.: *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

VITA

Name Mr Sarat Sinlapavongsa

Education B.Sc. Mathematics (Second Class Honor)
Chulalongkorn University, 2002
Full Scholarship Granted by Chulalongkorn University
M.Sc. Mathematics Chulalongkorn University, 2006
Full Graduate Scholarship Granted by the Institute for the Promotion of Teaching Science and Technology

Reward Gold Medal from IMSO Thailand Camp 1997
Runner-up of Undergraduate Mathematical Competition (individual) by Mathematical Association of Thailand 1998
Honourable Mention in the Asian Pacific Mathematics Olympiad 1998