Number of classes of solutions of the equation

$$x^2 - Dy^2 = 4E$$

by

Mathieu Lemire, B.Sc. (Université de Montréal)

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfilment of
the requirements for the degree of
Master of Science

School of Mathematics and Statistics
Ottawa-Carleton Institute of Mathematics and Statistics

Carleton University

Ottawa, Ontario

April, 2003

© Copyright

2003, Mathieu Lemire

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 0-612-83502-2

Our file Notre référence

ISBN: 0-612-83502-2

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

Canada

The undersigned hereby recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis

Number of classes of solutions of the equation

$$x^2 - Dy^2 = 4E$$

submitted by

Mathieu Lemire, B.Sc. (Université de Montréal)

in partial fulfilment of the requirements

for the degree of Master of Science

Kenneth S. Williams

Dr Kenneth S. Williams, Thesis Supervisor

Cyril W. L. Garner

Dr. Cyril W. L. Garner, Director

School of Mathematics and Statistics

Carleton University

April, 2003

Abstract

In this thesis, we study the Diophantine equation

$$x^2 - Dy^2 = 4E, \tag{1}$$

where D is the discriminant of a real quadratic field K and E is a nonzero integer.

We address two main questions. The first is to determine necessary and sufficient conditions on D and E for the solvability of the equation (1) in integers x and y .

When solvable (1) has infinitely many solutions in integers x and y . We define an equivalence relation on the set of all solutions of (1) and call the set of equivalence classes the classes of solutions of (1). The number $N(D, E)$ of classes of solutions is always finite. Our second question asks if it is possible to determine the value of $N(D, E)$ for given D and E . We show that both questions can be answered in the affirmative in terms of the group structure of the strict ideal class group $H^+(K)$.

In Chapter 1 we give the definition of the equivalence relation on the set of all solutions of (1) and prove that the number $N(D, E)$ of classes is finite.

In Chapter 2 we state and prove a necessary and sufficient condition on D and E for the solvability of (1). Several examples of the use of this theorem are given.

In Chapter 3, we state and prove a theorem that gives the value of $N(D, E)$ for specified D and E .

In Chapter 4 we show that the solvability of (1) and the value of $N(D, E)$ are easier to determine for certain group structures of $H^+(K)$ and certain prime factorizations of E . We conclude our work by extending the definition of two equivalent solutions of (1) to equivalent solutions of the more general equation

$$x^2 - my^2 = n, \tag{2}$$

where m is a squarefree integer and n is a nonzero integer. We denote the number of equivalence classes by $N'(m, n)$. We show that the solvability of (2) and the value of $N'(m, n)$ can be related to the solvability of an equation of the same form as (1) for many classes of values of m and n .

The main new results in this thesis are Theorems 2.5 and 3.1.

Acknowledgements

I would like to thank my supervisor Dr. Kenneth S. Williams for his patience, support and guidance, as well as for many interesting mathematical and non-mathematical conversations. You are a model for me and working with you is a great honour. All my thanks to Dr. Cyril Garner for being the first person to believe in me at Carleton University and for being so kind to me. Many thanks to Dr. Brett Stevens for his help with the computer program. I would also like to thank the School of Mathematics and Statistics for giving me the chance to be a teaching assistant for many courses and for the financial support that really helped me. I would not be who I am now without the friendship of all my good friends. I would like to thank Lawrence Aoun, David Gains, Colette Haley, Sawsan Kobaisy, Victor Mak, Ariane Masuda, Surabhi Pandey, Rima Rahal, Katrina Rogers-Stewart, Sri Vidya Thuppall and Wei Wei. I feel lucky and special to know each and everyone of you. Finally I would like to thank every member of my family for their continuous support. Je vous aime tous.

Dedication

I dedicate this thesis to my three beloved cats Duchesse, Grisou and Ti-Blanc for all their love, for showing me how to marvel the world and all the wonderful memories.

Merci beaucoup les amis.

Contents

Abstract	i
Acknowledgements	iii
Dedication	iv
1 Basic properties of the Diophantine equation $x^2 - Dy^2 = 4E$	1
1.1 Introduction	1
1.2 Notation	9
1.3 Properties of the equation $x^2 - Dy^2 = 4E$	10
1.4 Two methods to determine the solvability of the Diophantine equation $x^2 - Dy^2 = 4E$	27
2 The strict ideal class group and the solvability of the equation $x^2 -$ $Dy^2 = 4E$	32
2.1 The group $H(K)$	32
2.2 The group $H^+(K)$	35

2.3	The solvability of $x^2 - Dy^2 = 4E$	41
2.4	Examples	56
3	Number of classes of solutions of $x^2 - Dy^2 = 4E$	76
3.1	Main theorem	76
3.2	Examples	85
4	Special cases of Theorems 2.5 and 3.1	89
4.1	Solvability of $x^2 - Fy^2 = G$ and $2x^2 - Fy^2 = G$	89
4.2	Special case when $H^+(K) \simeq \mathbb{Z}_2^s$	91
4.3	Special case when E is equal to a prime power	94
4.4	The equation $x^2 - Dy^2 = \pm 4p^r q^s$	104
4.5	Number of classes of solutions of more general equations	109
	Conclusion	113
	Appendix A	114
	Appendix B	126
	Bibliography	143

Chapter 1

Basic properties of the Diophantine equation $x^2 - Dy^2 = 4E$

1.1 Introduction

The Diophantine equation $x^2 - my^2 = n$, where m is a positive integer which is not a perfect square and n is a nonzero integer, has a long history. Euler attributed to the English mathematician John Pell a method of solving $x^2 - my^2 = 1$ in integers x and y . However this method had already been given by another English mathematician William Brouncker in a series of letters to the French mathematician Pierre Fermat. Nevertheless the equation has become known as Pell's equation. Lagrange was the first mathematician to prove that $x^2 - my^2 = 1$ has infinitely many solutions in integers x and y . Dickson's History of the Theory of Numbers gives a detailed account of the early work on the equation $x^2 - my^2 = n$. This equation continues to attract as much attention today as it did three hundred years ago. Many modern mathematicians have written papers on various aspects of this fascinating equation, see for example [7], [10], [11], [12], [15], [17], [22] and [27]. In particular R. A. Mollin

has written extensively in recent years on the equation $x^2 - my^2 = n$ from the point of view of continued fractions. A complete listing of his papers on the subject can be found at <http://www.math.ucalgary.ca/~ramollin/pubsonly.pdf>.

The equation $x^2 - my^2 = n$ arises in many situations. We just give one simple example where it occurs. Let I be the ideal generated by 2 and $1 + \sqrt{23}$ in the integral domain $\mathbb{Z} + \mathbb{Z}\sqrt{23}$, that is $I = \langle 2, 1 + \sqrt{23} \rangle$. We ask if the ideal I is principal in $\mathbb{Z} + \mathbb{Z}\sqrt{23}$. If I is principal then there exists $x + y\sqrt{23} \in \mathbb{Z} + \mathbb{Z}\sqrt{23}$ such that $\langle 2, 1 + \sqrt{23} \rangle = \langle x + y\sqrt{23} \rangle$. Taking norms of both sides, we obtain

$$|x^2 - 23y^2| = N(\langle x + y\sqrt{23} \rangle) = N(\langle 2, 1 + \sqrt{23} \rangle) = 2,$$

so that we are lead naturally to the equations

$$x^2 - 23y^2 = \pm 2.$$

With the plus sign an obvious solution is $x = 5, y = 1$ and indeed

$$\langle 2, 1 + \sqrt{23} \rangle = \langle 5 + \sqrt{23} \rangle$$

as

$$5 + \sqrt{23} = 2 \cdot 2 + 1 \cdot (1 + \sqrt{23}) \in I.$$

In this thesis we study the Diophantine equation

$$x^2 - Dy^2 = 4E, \tag{1}$$

where

D = discriminant of a real quadratic field K ,

E = a nonzero integer.

We have taken $m = D$ and $n = 4E$ as the theory is more elegant in this situation.

The connection to the more general equation $x^2 - my^2 = n$ is discussed in Sections 4.1 and 4.5.

Given D and E , one of the first questions that one can ask is if the equation (1) is solvable in integers x and y . As $E \neq 0$ any solution $(x, y) \in \mathbb{Z}^2$ of (1) is such that $(x, y) \neq (0, 0)$. In some cases, it is possible to answer this question either by finding a solution of (1) by trial or by showing that (1) is insolvable by means of congruences or the law of quadratic reciprocity. We illustrate this in the following three examples.

Example 1.1. *The equation $x^2 - 5y^2 = 4$ is solvable as by inspection we have*

$$(3)^2 - 5(1)^2 = 4.$$

Example 1.2. *The equation $x^2 - 41y^2 = 200$ is solvable. By taking $y = 1, 2, 3, \dots$ we find very quickly that $(35)^2 - 41(5)^2 = 200$.*

Example 1.3. *We show that the equation $x^2 - 13y^2 = 24$ is not solvable in integers x and y . Suppose on the contrary that there exist $u, v \in \mathbb{Z}$ such that $u^2 - 13v^2 = 24$. Taking this equation modulo 13, we obtain*

$$11 \equiv 24 \equiv u^2 - 13v^2 \equiv u^2 \pmod{13},$$

so that the Legendre symbol $\left(\frac{11}{13}\right) = +1$. However, by the law of quadratic reciprocity, we have

$$\left(\frac{11}{13}\right) \left(\frac{13}{11}\right) = (-1)^{\left(\frac{11-1}{2}\right)\left(\frac{13-1}{2}\right)} = (-1)^{(5)(6)} = 1,$$

and by the supplement to the law of quadratic reciprocity

$$\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

so that $\left(\frac{11}{13}\right) = -1$, which is a contradiction. Hence the equation is insolvable.

These simple methods will work in some cases but in general, they are either not applicable or take a lot of time. The following two examples illustrate this.

Example 1.4. The equation $u^2 - 28v^2 = 6018832$ is solvable. The solution for which v is the smallest is $u = 2512$ and $v = 102$. This solution takes some time to find by trial!

Example 1.5. In this example we show that the equation

$$x^2 - 1752y^2 = -8$$

is insolvable in integers x and y , and that it cannot be proved insolvable by means of congruences, that is

$$x^2 - 1752y^2 \equiv -8 \pmod{m}$$

is solvable for every positive integer $m > 1$. Note that $D = 1752$ is the discriminant of the real quadratic field $K = \mathbb{Q}(\sqrt{438})$ and $E = -2$.

Suppose that $x^2 - 1752y^2 = -8$ is solvable in integers x and y . Then, as $8 \mid 1752$, we must have $8 \mid x^2$ so that $4 \mid x$. Setting $x = 4z$ we obtain $2z^2 - 219y^2 = -1$. Conversely if y and z are integers such that $2z^2 - 219y^2 = -1$ then $x = 4z$ and y are integers satisfying $x^2 - 1752y^2 = -8$. Thus $x^2 - 1752y^2 = -8$ is insolvable if and only if $2x^2 - 219y^2 = -1$ is insolvable.

We now show that $2x^2 - 219y^2 = -1$ is insolvable in integers x and y . Suppose on the contrary that the equation is solvable. Clearly $x \neq 0$ and $y \neq 0$. Thus we may assume that $x > 0$ and $y > 0$. Further we choose the solution x, y so that y is least.

Let

$$x_1 = |293x - 3066y| \in \mathbb{Z}, \quad y_1 = -28x + 293y \in \mathbb{Z}.$$

A short calculation yields

$$2x_1^2 - 219y_1^2 = 2x^2 - 219y^2 = -1.$$

Clearly $x_1 \neq 0$ so $x_1 > 0$. Suppose $y_1 \leq 0$. Then $-28x + 293y \leq 0$ so that $x \geq \frac{293}{28}y$.

Thus $x^2 \geq \frac{85849}{784}y^2$ and so

$$-1 = 2x^2 - 219y^2 \geq \frac{y^2}{392} \geq \frac{1}{392},$$

a contradiction. Hence $y_1 > 0$. By the minimality of y we have $y \leq y_1$, so

$$-28x + 293y \geq y,$$

whence

$$x \leq \frac{292}{28}y = \frac{73}{7}y.$$

Therefore

$$x^2 \leq \frac{5329}{49}y^2$$

and

$$-1 = 2x^2 - 219y^2 \leq -\frac{73}{49}y^2 \leq -\frac{73}{49},$$

a contradiction. This completes the proof that $2x^2 - 219y^2 = -1$, and thus $x^2 - 1752y^2 = -8$, is insolvable in integers x and y .

We now prove that the congruence

$$x^2 - 1752y^2 \equiv -8 \pmod{m}$$

is solvable for every positive integer $m > 1$. We do this by showing that

$$x^2 - 1752y^2 \equiv -8 \pmod{p^\alpha}$$

is solvable for every prime p and every positive integer α .

case (i) : $p = 2$ If $\alpha = 1, 2$ or 3 we may take $x = 0$ and $y = 1$, as $x^2 - 1752y^2 = -1752 \equiv -8 \pmod{2^\alpha}$. Thus we may suppose that $\alpha \geq 4$. As $217 \equiv 1 \pmod{8}$ there exists an odd integer t such that

$$t^2 \equiv 217 \pmod{2^{\alpha-3}},$$

by [5, Theorem 17, p. 13]. Let u be the inverse of t modulo $2^{\alpha-3}$. Then

$$217u^2 \equiv (tu)^2 \equiv 1 \pmod{2^{\alpha-3}}.$$

Set $x = 4u$, $y = u$. Then

$$x^2 - 1752y^2 = 16u^2 - 1752u^2 = -1736u^2 = -8 \cdot 217u^2 \equiv -8 \pmod{2^\alpha}.$$

case (ii) : $p = 3$ As $\left(\frac{-2}{3}\right) = \left(\frac{1}{3}\right) = 1$ there exists an integer t such that

$$t^2 \equiv -2 \pmod{3^\alpha},$$

by [5, Theorem 17, p. 13]. Set $x = 2t$, $y = 0$. Then

$$x^2 - 1752y^2 = 4t^2 \equiv -8 \pmod{3^\alpha}.$$

case (iii) : $p = 73$ As $\left(\frac{-2}{73}\right) = \left(\frac{144}{73}\right) = 1$ there exists an integer t such that $t^2 \equiv -2 \pmod{3^\alpha}$. Set $x = 2t$, $y = 0$. Then

$$x^2 - 1752y^2 = 4t^2 \equiv -8 \pmod{73^\alpha}.$$

case (iv) : $p \neq 2, 3, 73$ The number of $y \in \{0, 1, 2, \dots, p-1\}$ such that $438y^2 - 2$ is a quadratic residue $\pmod{p}$ is

$$\begin{aligned} & \frac{1}{2} \sum_{\substack{y=0 \\ p \nmid 438y^2-2}}^{p-1} \left(1 + \left(\frac{438y^2 - 2}{p} \right) \right) \\ &= \frac{1}{2} \left(p - 1 - \left(\frac{219}{p} \right) \right) + \frac{1}{2} \sum_{y=0}^{p-1} \left(\frac{438y^2 - 2}{p} \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2} \left(p - 1 - \left(\frac{219}{p} \right) \right) - \frac{1}{2} \left(\frac{438}{p} \right) \\
&= \frac{1}{2} \left(p - 1 - \left(\frac{219}{p} \right) - \left(\frac{438}{p} \right) \right) \\
&\geq \frac{1}{2} (p - 1 - 1 - 1) \\
&= \frac{p-3}{2} \geq 1.
\end{aligned}$$

Thus there exists y_1 such that

$$\left(\frac{438y_1^2 - 2}{p} \right) = 1.$$

Hence there exists x_1 such that

$$x_1^2 \equiv 438y_1^2 - 2 \pmod{p^\alpha}.$$

Set $x = 2x_1$, $y = y_1$. Then

$$x^2 - 1752y^2 = 4x_1^2 - 1752y_1^2 = 4(x_1^2 - 438y_1^2) \equiv -8 \pmod{p^\alpha}.$$

In the course of this proof we made use of the result: if p is an odd prime and a, b, c are integers with $p \nmid a$ and $p \nmid b^2 - 4ac$ then

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = - \left(\frac{a}{p} \right),$$

see [9, p. 82].

In this thesis we use ideas from algebraic number theory to discuss the solvability or insolvability of the equation (1), and when solvable we discuss classes of solutions.

1.2 Notation

In this section we introduce the notation that will be used throughout the thesis. As mentioned in Section 1.1, D is the discriminant of a real quadratic field K so that

$$K = \mathbb{Q}(\sqrt{D}).$$

Hence $\alpha \in K$ if and only if $\alpha = r + s\sqrt{D}$, where $r, s \in \mathbb{Q}$. For $\alpha = r + s\sqrt{D} \in K$ we let $\alpha' = r - s\sqrt{D}$ and we call α' the conjugate of α . The trace $\text{tr}(\alpha)$ of α and the norm $N(\alpha)$ of α are defined by

$$\text{tr}(\alpha) = \alpha + \alpha' = (r + s\sqrt{D}) + (r - s\sqrt{D}) = 2r \in \mathbb{Q}$$

and

$$N(\alpha) = \alpha\alpha' = r^2 - Ds^2 \in \mathbb{Q}.$$

As usual $\mathcal{O}_K$ = the ring of algebraic integers of K . We note that for $\alpha \in K$,

$$\alpha \in \mathcal{O}_K \iff \text{tr}(\alpha), N(\alpha) \in \mathbb{Z}.$$

We also set

$$\mathcal{U}(\mathcal{O}_K) = \text{group of units of } \mathcal{O}_K$$

and

$$\mathcal{U}^+(\mathcal{O}_K) = \text{subgroup of } \mathcal{U}(\mathcal{O}_K) \text{ of units of norm } +1.$$

We recall that

$$\mathcal{U}(\mathcal{O}_K) = \{\pm \varepsilon^n \mid \varepsilon \text{ is the fundamental unit } > 1 \text{ of } \mathcal{O}_K, n \in \mathbb{Z}\}.$$

$$\mathcal{U}^+(\mathcal{O}_K) = \{\pm \eta^n \mid \eta \text{ is the fundamental unit } > 1 \text{ of } \mathcal{O}_K \text{ of norm } 1, n \in \mathbb{Z}\}.$$

$$\eta = \begin{cases} \varepsilon, & \text{if } N(\varepsilon) = 1, \\ \varepsilon^2, & \text{if } N(\varepsilon) = -1. \end{cases}$$

$$[\mathcal{U}(\mathcal{O}_K) : \mathcal{U}^+(\mathcal{O}_K)] = 1 \text{ or } 2.$$

1.3 Properties of the equation $x^2 - Dy^2 = 4E$

We now begin our study of the equation (1).

Theorem 1.1. *Let D be the discriminant of a real quadratic field K and let E be a nonzero integer. If $(x, y) \in \mathbb{Z}^2$ is a solution of the equation $x^2 - Dy^2 = 4E$ then*

$$\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K, \quad N\left(\frac{x + y\sqrt{D}}{2}\right) = E.$$

Proof: Suppose that $(x, y) \in \mathbb{Z}^2$ is a solution of the equation $x^2 - Dy^2 = 4E$, where D is the discriminant of a real quadratic field K and E is a nonzero integer.

As $x, y \in \mathbb{Z}$, we have $\frac{x}{2}, \frac{y}{2} \in \mathbb{Q}$ so that $\frac{x + y\sqrt{D}}{2} \in K$. Since $\frac{x + y\sqrt{D}}{2}$ is the root of the polynomial $t^2 - xt + E \in \mathbb{Z}[x]$, we deduce that $\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K$. Further

$$N\left(\frac{x + y\sqrt{D}}{2}\right) = \left(\frac{x + y\sqrt{D}}{2}\right) \left(\frac{x - y\sqrt{D}}{2}\right) = \frac{x^2 - Dy^2}{4} = E. \quad \square$$

The next theorem shows that the converse of Theorem 1.1 is also true.

Theorem 1.2. *Let D be the discriminant of a real quadratic field K and let E be a nonzero integer. If*

$$\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K, \quad N\left(\frac{x + y\sqrt{D}}{2}\right) = E$$

then $(x, y) \in \mathbb{Z}^2$ is a solution of the equation $x^2 - Dy^2 = 4E$.

Proof: We have

$$\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K \implies \frac{x + y\sqrt{D}}{2} \in K \implies \frac{x}{2}, \frac{y}{2} \in \mathbb{Q} \implies x, y \in \mathbb{Q}$$

and

$$\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K \implies \frac{x - y\sqrt{D}}{2} \in \mathcal{O}_K.$$

Thus we have

$$x = \frac{x + y\sqrt{D}}{2} + \frac{x - y\sqrt{D}}{2} \in \mathcal{O}_K.$$

Hence

$$x \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

Next

$$E = N\left(\frac{x + y\sqrt{D}}{2}\right) = \left(\frac{x + y\sqrt{D}}{2}\right)\left(\frac{x - y\sqrt{D}}{2}\right) = \frac{x^2 - Dy^2}{4}$$

so that

$$x^2 - Dy^2 = 4E.$$

It only remains to show that $y \in \mathbb{Z}$. Clearly $Dy^2 = x^2 - 4E \in \mathbb{Z}$. Let m be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Thus

$$D = \begin{cases} m, & \text{if } m \equiv 1 \pmod{4}, \\ 4m, & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases}$$

If $D = m$ then $my^2 \in \mathbb{Z}$. As m is squarefree this implies that $y \in \mathbb{Z}$.

If $D = 4m$ then $4my^2 \in \mathbb{Z}$. As m is squarefree this implies that $4y^2 \in \mathbb{Z}$, which implies that $2y \in \mathbb{Z}$. Suppose that $y = \frac{z}{2}$, where z is an odd integer. Then

$$mz^2 = 4my^2 = Dy^2 = x^2 - 4E$$

so that as z is odd

$$m \equiv mz^2 \equiv x^2 \equiv 0 \text{ or } 1 \pmod{4},$$

contradicting $m \equiv 2, 3 \pmod{4}$. Hence $y \in \mathbb{Z}$. □

Theorems 1.1 and 1.2 tell us that there is a one-to-one correspondence between the solutions (x, y) of (1) and the algebraic integers $\frac{x + y\sqrt{D}}{2}$ of K of norm E , that is

$$\{(x, y) \in \mathbb{Z}^2 \mid x^2 - Dy^2 = 4E\} \xleftrightarrow{1-1} \left\{ \frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K \mid N\left(\frac{x + y\sqrt{D}}{2}\right) = E \right\}.$$

Solutions of (1) give us, if they exist, all the elements of $\mathcal{O}_K$ of a given norm E . We write $S(D, E)$ to denote the set of all solutions of (1), that is

$$S(D, E) = \{(x, y) \in \mathbb{Z}^2 \mid x^2 - Dy^2 = 4E\}.$$

If $(x, y) \in S(D, E)$ we often refer to $\frac{x + y\sqrt{D}}{2}$ as a “solution” of $x^2 - Dy^2 = 4E$.

We now prove a theorem about the solutions of (1).

Theorem 1.3. *Let D be a discriminant of a real quadratic field K and let E be a nonzero integer. If $\frac{x + y\sqrt{D}}{2}$ is a solution of $x^2 - Dy^2 = 4E$ and $\theta \in \mathcal{U}^+(\mathcal{O}_K)$ then $\theta \left(\frac{x + y\sqrt{D}}{2} \right)$ is also a solution of $x^2 - Dy^2 = 4E$.*

Proof: As $(x, y) \in \mathbb{Z}^2$ is a solution of (1), by Theorem 1.1 we have

$$\frac{x + y\sqrt{D}}{2} \in \mathcal{O}_K, \quad N \left(\frac{x + y\sqrt{D}}{2} \right) = E.$$

Further, as $\theta \in \mathcal{U}^+(K)$, we have $\theta \in \mathcal{O}_K$ and $N(\theta) = 1$. Hence

$$\theta \left(\frac{x + y\sqrt{D}}{2} \right) \in \mathcal{O}_K, \quad N \left(\theta \left(\frac{x + y\sqrt{D}}{2} \right) \right) = E.$$

Thus, by Theorem 1.2, $\theta \left(\frac{x + y\sqrt{D}}{2} \right)$ is a solution of (1). □

We can now prove a theorem about the size of the set $S(D, E)$.

Theorem 1.4. *If $S(D, E) \neq \emptyset$ then $S(D, E)$ is an infinite set.*

Proof: As $S(D, E) \neq \emptyset$ the equation $x^2 - Dy^2 = 4E$ is solvable. Let $\frac{x + y\sqrt{D}}{2}$ be a solution. Let η be the fundamental unit (> 1) of norm $+1$ in $\mathcal{O}_K$. For each $n \in \mathbb{N}$

$$\eta^n \left(\frac{x + y\sqrt{D}}{2} \right)$$

is a solution of (1) by Theorem 1.3. Therefore $S(D, E)$ is an infinite set. $\square$

Theorem 1.3 enables us to introduce an equivalence relation on the set $S(D, E)$.

Definition 1.1. Let D be the discriminant of a real quadratic field K and let E be a nonzero integer. Suppose that $S(D, E) \neq \emptyset$. Let $(x_1, y_1) \in \mathbb{Z}^2$ and $(x_2, y_2) \in \mathbb{Z}^2$ be solutions of $x^2 - Dy^2 = 4E$. We say that (x_1, y_1) and (x_2, y_2) are strictly associated solutions of $x^2 - Dy^2 = 4E$, written $(x_1, y_1) \sim (x_2, y_2)$, if and only if there exists $\eta \in \mathcal{U}^+(\mathcal{O}_K)$ such that

$$\frac{x_1 + y_1\sqrt{D}}{2} = \eta \left(\frac{x_2 + y_2\sqrt{D}}{2} \right).$$

We show that $\sim$ is an equivalence relation on $S(D, E)$.

Theorem 1.5. $\sim$ is an equivalence relation on $S(D, E)$.

Proof: Let $\frac{u + v\sqrt{D}}{2}$ be a solution of (1). As $1 \in \mathcal{U}^+(\mathcal{O}_K)$ and $\frac{u + v\sqrt{D}}{2} = 1 \left(\frac{u + v\sqrt{D}}{2} \right)$, we see that $\frac{u + v\sqrt{D}}{2} \sim \frac{u + v\sqrt{D}}{2}$, so that $\sim$ is reflexive.

Now let $\frac{u + v\sqrt{D}}{2}$ and $\frac{u_1 + v_1\sqrt{D}}{2}$ be solutions of (1) with $\frac{u + v\sqrt{D}}{2} \sim \frac{u_1 + v_1\sqrt{D}}{2}$.

Then there exists $\theta \in \mathcal{U}^+(\mathcal{O}_K)$ such that

$$\frac{u + v\sqrt{D}}{2} = \theta \left(\frac{u_1 + v_1\sqrt{D}}{2} \right).$$

Hence $\frac{u_1 + v_1\sqrt{D}}{2} = \frac{1}{\theta} \left(\frac{u + v\sqrt{D}}{2} \right)$, where $\frac{1}{\theta} \in U^+(\mathcal{O}_K)$. Thus $\frac{u_1 + v_1\sqrt{D}}{2} \sim \frac{u + v\sqrt{D}}{2}$, so that $\sim$ is symmetric.

Finally let $\frac{u + v\sqrt{D}}{2}$, $\frac{u_1 + v_1\sqrt{D}}{2}$ and $\frac{u_2 + v_2\sqrt{D}}{2}$ be solutions of (1) such that

$$\frac{u + v\sqrt{D}}{2} \sim \frac{u_1 + v_1\sqrt{D}}{2}, \quad \frac{u_1 + v_1\sqrt{D}}{2} \sim \frac{u_2 + v_2\sqrt{D}}{2}.$$

Then there exist $\theta, \phi \in \mathcal{U}^+(\mathcal{O}_K)$ such that

$$\frac{u + v\sqrt{D}}{2} = \theta \left(\frac{u_1 + v_1\sqrt{D}}{2} \right), \quad \frac{u_1 + v_1\sqrt{D}}{2} = \phi \left(\frac{u_2 + v_2\sqrt{D}}{2} \right).$$

Hence

$$\frac{u + v\sqrt{D}}{2} = \theta\phi \left(\frac{u_2 + v_2\sqrt{D}}{2} \right), \quad \text{where } \theta\phi \in \mathcal{U}^+(\mathcal{O}_K).$$

Thus $\frac{u + v\sqrt{D}}{2} \sim \frac{u_2 + v_2\sqrt{D}}{2}$ and so $\sim$ is transitive.

This proves that $\sim$ is an equivalence relation on $S(D, E)$. □

Definition 1.2. *The equivalence classes under $\sim$ are called classes of solutions. The class of solutions containing the solution (x, y) is denoted by $[(x, y)]$. The set of all equivalence classes of the equation $x^2 - Dy^2 = 4E$ is denoted by $Q(D, E)$.*

If the solutions (x, y) and (x', y') of (1) belong to the same class we often write $(x, y) \sim (x', y')$ as $\frac{x + y\sqrt{D}}{2} \sim \frac{x' + y'\sqrt{D}}{2}$. We next prove a theorem that determines if two elements of $S(D, E)$ are in the same class of solutions.

Theorem 1.6. *Let D be the discriminant of a real quadratic field K and E a nonzero integer. Let $(x, y), (x', y') \in S(D, E)$. Then*

$$\frac{x + y\sqrt{D}}{2} \sim \frac{x' + y'\sqrt{D}}{2} \text{ if and only if } \frac{xx' - Dyy'}{2E} \in \mathbb{Z} \text{ and } \frac{xy' - x'y}{2E} \in \mathbb{Z}.$$

Proof: ($\implies$;) Suppose that

$$\frac{x + y\sqrt{D}}{2} \sim \frac{x' + y'\sqrt{D}}{2}.$$

Then there exists a unit $\frac{a + b\sqrt{D}}{2} \in \mathcal{U}^+(\mathcal{O}_K)$ such that

$$\frac{x + y\sqrt{D}}{2} = \left(\frac{a + b\sqrt{D}}{2} \right) \left(\frac{x' + y'\sqrt{D}}{2} \right).$$

As $N\left(\frac{a + b\sqrt{D}}{2}\right) = 1$ we have

$$a^2 - Db^2 = 4.$$

Thus

$$\frac{x + y\sqrt{D}}{2} = \frac{(ax' + by'D) + (bx' + ay')\sqrt{D}}{4}.$$

Therefore

$$x = \frac{ax' + by'D}{2} \text{ and } y = \frac{bx' + ay'}{2}.$$

Hence

$$1) \frac{xx' - Dyy'}{2E} = \frac{\left(\frac{ax' + by'D}{2}\right)x' - D\left(\frac{bx' + ay'}{2}\right)y'}{2E}$$

$$\begin{aligned}
&= \frac{\left(\frac{ax'^2 + bx'y'D}{2}\right) - D\left(\frac{bx'y' + ay'^2}{2}\right)}{2E} \\
&= \frac{ax'^2 - ay'^2 D}{4E} = \frac{a(x'^2 - y'^2 D)}{4E} = a \in \mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
2) \frac{xy' - x'y}{2E} &= \frac{\left(\frac{ax' + by'D}{2}\right)y' - x'\left(\frac{bx' + ay'}{2}\right)}{2E} \\
&= \frac{ax'y' + by'^2 D - bx'^2 - ax'y'}{4E} \\
&= \frac{-b(x'^2 - Dy'^2)}{4E} = -b \in \mathbb{Z}.
\end{aligned}$$

($\Leftarrow$):) Suppose that

$$\frac{xx' - Dyy'}{2E} = a \in \mathbb{Z} \quad , \quad \frac{xy' - x'y}{2E} = -b \in \mathbb{Z}.$$

Then

$$a^2 - b^2 D = \frac{1}{4E^2} ((xx' - Dyy')^2 - D(xy' - x'y)^2) = \frac{1}{4E^2} ((x^2 - Dy^2)(x'^2 - Dy'^2)) = 4,$$

and so

$$\frac{a + b\sqrt{D}}{2} \text{ is a solution of } x^2 - Dy^2 = 4 \text{ and } \frac{a + b\sqrt{D}}{2} \in \mathcal{O}_K.$$

Also

$$\frac{ax' + by'D}{4} = \frac{\left(\frac{xx' - Dyy'}{2E}\right)x' - D\left(\frac{xy' - x'y}{2E}\right)y'}{4} = x\left(\frac{x'^2 - Dy'^2}{8E}\right) = \frac{x}{2}$$

and

$$\frac{ay' + bx'}{4} = \frac{\left(\frac{xx' - Dyy'}{2E}\right)y' - \left(\frac{xy' - x'y}{2E}\right)x'}{4} = \frac{y}{2}.$$

Hence

$$\frac{x + y\sqrt{D}}{2} = \left(\frac{ax' + by'D}{4} \right) + \left(\frac{ay' + bx'}{4} \right) \sqrt{D} = \left(\frac{a + b\sqrt{D}}{2} \right) \left(\frac{x' + y'\sqrt{D}}{2} \right),$$

where

$$\frac{a + b\sqrt{D}}{2} \text{ is a unit of norm } +1 \text{ in } \mathcal{O}_K.$$

Therefore $\frac{x + y\sqrt{D}}{2} \sim \frac{x' + y'\sqrt{D}}{2}$. □

We now introduce the notion of a fundamental solution of a class of solutions.

Among all the solutions $\frac{x + y\sqrt{D}}{2}$ in a given class C we choose a unique solution $\frac{x^* + y^*\sqrt{D}}{2}$ in the following way. Let y^* be the least value of $y \geq 0$ which occurs

in C . Let x' be such that $\frac{x' + y^*\sqrt{D}}{2} \in C$.

If $\frac{-x' + y^*\sqrt{D}}{2} \in C$ we set $x^* = |x'|$.

If $\frac{-x' + y^*\sqrt{D}}{2} \notin C$ we set $x^* = x'$.

Clearly x^* is uniquely determined.

Definition 1.3. Let C be a class of solutions of $S(D, E)$. The solution $(x^*, y^*) \in C$ is called the fundamental solution of C .

In the fundamental solution the integer $|x^*|$ has the least possible value for $|x|$ when $\frac{x + y\sqrt{D}}{2}$ belongs to C .

We remark that if $\frac{x + y\sqrt{D}}{2}$ is a solution of (1) then $\frac{x - y\sqrt{D}}{2}$ is also a solution

of (1). The two solutions are in general in two different classes of solutions. We define a relationship between these two classes of solutions as follows.

Definition 1.4. Let C be a class of solutions of $S(D, E)$. Suppose $C = [(x, y)]$. Then $(x, -y)$ is a solution of (1). We define $\bar{C} = [(x, -y)]$. The classes C and $\bar{C}$ are said to be conjugates of one another.

We show that this definition is a valid one. Suppose that $C = [(x, y)] = [(x', y')]$.

We must show that

$$[(x, -y)] = [(x', -y')].$$

As $[(x, y)] = [(x', y')]$ we have $\frac{x + y\sqrt{D}}{2} \sim \frac{x' + y'\sqrt{D}}{2}$. Thus, by Theorem 1.6, we have

$$\frac{xx' - Dyy'}{2E} \in \mathbb{Z}, \quad \frac{xy' - x'y}{2E} \in \mathbb{Z}.$$

Hence

$$\frac{xx' - D(-y)(-y')}{2E} \in \mathbb{Z}, \quad \frac{x(-y') - x'(-y)}{2E} \in \mathbb{Z}.$$

Then, by Theorem 1.6, we deduce that

$$\frac{x - y\sqrt{D}}{2} \sim \frac{x' - y'\sqrt{D}}{2}$$

so that

$$[(x, -y)] = [(x', -y')].$$

We remark that conjugates classes are in general distinct, but that sometimes they may coincide. We give a special name to C in the latter case.

Definition 1.5. *If $C = \overline{C}$ the class C is said to be ambiguous.*

It is clear from Definition 1.4 that $\overline{\overline{C}} = C$. Hence the class C is ambiguous if and only if the class $\overline{C}$ is ambiguous. The next theorem shows that if $C = [(x, y)]$ is not ambiguous then $\frac{x + y\sqrt{D}}{2}$ and $\frac{-x + y\sqrt{D}}{2}$ are in different classes.

Theorem 1.7. *Let $C = [(x, y)]$ be a class of $S(D, E)$.*

If C is ambiguous then $C = [(\pm x, \pm y)]$.

If C is not ambiguous then $[(x, y)] = [(-x, -y)] = C \neq \overline{C} = [(x, -y)] = [(-x, y)]$.

Proof : As $C = [(x, y)]$ we have $\frac{x + y\sqrt{D}}{2} \in C$. As $-1 \in \mathcal{U}^+(\mathbb{O}_K)$ and

$$(-1) \left(\frac{-x - y\sqrt{D}}{2} \right) = \frac{x + y\sqrt{D}}{2},$$

we have $\frac{x + y\sqrt{D}}{2} \sim \frac{-x - y\sqrt{D}}{2}$, which implies that

$$[(x, y)] = [(-x, -y)] = C.$$

In the same way we find that $\frac{x - y\sqrt{D}}{2} \sim \frac{-x + y\sqrt{D}}{2}$, which implies that

$$[(x, -y)] = [(-x, y)] = \overline{C}.$$

If C is ambiguous we have

$$[(x, y)] = [(-x, -y)] = C = \overline{C} = [(x, -y)] = [(-x, y)],$$

which implies $C = [(\pm x, \pm y)]$.

If C is not ambiguous we have $C \neq \overline{C}$. Therefore

$$[(x, y)] = [(-x, -y)] = C \neq \overline{C} = [(x, -y)] = [(-x, y)]. \quad \square$$

We give one example of an ambiguous class and one of a non-ambiguous class.

Example 1.6. Consider the equation $x^2 - 5y^2 = 20$. A solution of this equation is $x = 5, y = 1$. Let $C = [(5, 1)]$. $\frac{5 + \sqrt{5}}{2}$ is a fundamental solution of C . Now $\overline{C} = [(5, -1)]$ by Definition 1.4. As

$$\frac{5 \cdot 5 - 5 \cdot 1 \cdot (-1)}{10} = 3 \in \mathbb{Z} \quad \text{and} \quad \frac{5 \cdot (-1) - 5 \cdot 1}{10} = -1 \in \mathbb{Z},$$

Theorem 1.6 implies that $(5, 1) \sim (5, -1)$, that is $C = \overline{C}$. Therefore C is an ambiguous class.

Example 1.7. Consider the equation $x^2 - 41y^2 = 32$. A solution of this equation is $x = 14, y = 2$. Let $C = [(14, 2)]$. $\frac{14 + 2\sqrt{41}}{2}$ is a fundamental solution of C . Let $\overline{C} = [(14, -2)]$ by Definition 1.4. As

$$\frac{14 \cdot (-2) - 14 \cdot 2}{16} = -\frac{7}{2} \notin \mathbb{Z},$$

Theorem 1.6 implies that $(14, 2) \not\sim (14, -2)$, so that $C \neq \overline{C}$. Therefore $C = [(14, 2)]$ is a non-ambiguous class.

We remark that the equation $x^2 - Dy^2 = 4E$ has a solution with $y = 0$ if and only if E is a perfect square. If $E = F^2$ then $(x, y) = (2F, 0)$ is a solution of $x^2 - Dy^2 = 4E$.

Set $C = [(2F, 0)]$. By Definition 1.4 we see that $\overline{C} = [(2F, 0)]$. Hence $C = \overline{C}$ and C is an ambiguous class. Thus by Theorem 1.7 $C = [(\pm 2F, 0)]$.

The equation $x^2 - Dy^2 = 4E$ has a solution with $x = 0$ if and only if $-\frac{4E}{D}$ is a perfect square. If $-\frac{4E}{D} = G^2$ then $(x, y) = (0, G)$ is a solution of $x^2 - Dy^2 = 4E$. Set $C = [(0, G)]$. Then $\overline{C} = [(0, -G)]$. Now

$$\frac{(0)(0) - D(G)(-G)}{2E} = \frac{DG^2}{2E} = \frac{-4E}{2E} = -2 \in \mathbb{Z}$$

and

$$\frac{(0)(-G) - (0)(G)}{2E} = 0 \in \mathbb{Z},$$

so by Theorem 1.6 we have

$$\frac{0 + G\sqrt{D}}{2} \sim \frac{0 - G\sqrt{D}}{2}.$$

Hence $C = \overline{C}$ and C is ambiguous.

We now state and prove an important result that allows us to find a fundamental solution for each class of $S(D, E)$.

Theorem 1.8. *Let D be the discriminant of a real quadratic field K and E a nonzero integer.*

(1) *If $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class C of the equation*

$$x^2 - Dy^2 = 4E, \text{ where } E > 0, \quad (2)$$

and if $\frac{x_1 + y_1\sqrt{D}}{2}$ is the fundamental unit of $\mathcal{O}_K$ of norm $+1$, then we have the inequalities

$$0 \leq v \leq \frac{y_1\sqrt{E}}{\sqrt{x_1+2}}, \quad (3)$$

$$0 < |u| \leq \sqrt{(x_1+2)E}. \quad (4)$$

(2) If $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class C of the equation

$$x^2 - Dy^2 = 4E, \text{ where } E < 0, \quad (5)$$

and if $\frac{x_1 + y_1\sqrt{D}}{2}$ is the fundamental unit of $\mathcal{O}_K$ of norm $+1$, then we have the inequalities

$$0 < v \leq \frac{y_1\sqrt{|E|}}{\sqrt{x_1-2}}. \quad (6)$$

$$0 \leq |u| \leq \sqrt{(x_1-2)|E|}. \quad (7)$$

Proof:

case (1) : $u^2 - Dv^2 = 4E$, where $E > 0$. We note that $u \neq 0$ and $x_1 > 2$. We can assume that $u > 0$ since if the inequalities (3) and (4) are true for a class C they are also true for the conjugate class $\overline{C}$. We can easily deduce the following inequality under these conditions

$$ux_1 - Dvy_1 = ux_1 - \sqrt{(u^2 - 4E)(x_1^2 - 4)} > 0. \quad (8)$$

Consider the solution

$$\left(\frac{u + v\sqrt{D}}{2}\right) \left(\frac{x_1 - y_1\sqrt{D}}{2}\right) = \left(\frac{ux_1 - Dvy_1}{4}\right) + \left(\frac{x_1v - y_1u}{4}\right) \sqrt{D},$$

of $x^2 - Dy^2 = 4E$. As $N\left(\frac{x_1 - y_1\sqrt{D}}{2}\right) = 1$ it belongs to the class C . Since $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class C , by the remark following Definition 1.3 we have $\left|\frac{ux_1 - Dvy_1}{2}\right| \geq |u|$. As $ux_1 - Dvy_1 > 0$ and $u > 0$ we have

$$\frac{ux_1 - Dvy_1}{2} \geq u.$$

From this inequality it follows that

$$u^2(x_1 - 2)^2 \geq D^2v^2y_1^2 = (u^2 - 4E)(x_1^2 - 4)$$

or

$$\frac{x_1 - 2}{x_1 + 2} \geq 1 - \frac{4E}{u^2},$$

and finally

$$u^2 \leq (x_1 + 2)E.$$

Taking the square root on each side we obtain (4). It is easily seen that (3) follows from (4).

case (2): $u^2 - Dv^2 = 4E$, where $E < 0$. We note that $v \neq 0$, so that $v > 0$, and $x_1 > 2$. We can assume that $u \geq 0$ since if the inequalities (6) and (7) are true for

a class C they are also true for the conjugate class $\overline{C}$. We can easily deduce the following inequality under these conditions

$$(x_1v)^2 = \left(y_1^2 + \frac{4}{D}\right)(u^2 - 4E) > y_1^2 u^2.$$

As $x_1 > 0$, $y_1 > 0$, $u \geq 0$ and $v > 0$ we deduce that

$$x_1v - y_1u > 0. \quad (9)$$

Consider now the solution

$$\left(\frac{u + v\sqrt{D}}{2}\right) \left(\frac{x_1 - y_1\sqrt{D}}{2}\right) = \left(\frac{ux_1 - Dvy_1}{4}\right) + \left(\frac{x_1v - y_1u}{4}\right) \sqrt{D}$$

of $x^2 - Dy^2 = 4E$. As $N\left(\frac{x_1 - y_1\sqrt{D}}{2}\right) = 1$ it belongs to the class C . Since $\frac{u + v\sqrt{D}}{2}$ is the fundamental solution of the class C , we have

$$\left|\frac{x_1v - y_1u}{4}\right| \geq v.$$

As $x_1v - y_1u > 0$ we have $\frac{x_1v - y_1u}{2} \geq v$. It thus follows that

$$(u^2 - 4E)(x_1 - 2)^2 = Dv^2(x_1 - 2)^2 \geq Dy_1^2 u^2 = (x_1^2 - 4)u^2,$$

or

$$1 + \frac{4|E|}{u^2} \geq \frac{x_1 + 2}{x_1 - 2},$$

and finally

$$u^2 \leq (x_1 - 2)|E|.$$

By taking the square root on both sides we obtain (7). The inequality (6) follows from (7). $\square$

We now introduce a notation for the number of classes of solutions of the equation $x^2 - Dy^2 = 4E$.

Definition 1.6. Let D be the discriminant of a real quadratic field and E a nonzero integer. Then we set $N(D, E) =$ the number of classes of solutions of the equation $x^2 - Dy^2 = 4E$, equivalently $N(D, E) = \text{card } Q(D, E)$.

The following theorem is an immediate consequence of Theorem 1.8.

Theorem 1.9. $N(D, E)$ is always finite.

Indeed if $E > 0$ we have

$$\begin{aligned} N(D, E) &\leq \left(\left\lceil \frac{y_1 \sqrt{E}}{\sqrt{x_1 + 2}} \right\rceil + 1 \right) \left(2 \left\lceil \sqrt{(x_1 + 2)E} \right\rceil \right) \\ &\leq 2 \left(\frac{y_1 \sqrt{E}}{\sqrt{x_1 + 2}} + 1 \right) \sqrt{(x_1 + 2)E} \\ &= 2Ey_1 + 2\sqrt{(x_1 + 2)E} \end{aligned}$$

and for $E < 0$

$$\begin{aligned} N(D, E) &\leq \left\lceil \frac{y_1 \sqrt{|E|}}{\sqrt{x_1 - 2}} \right\rceil \left(2 \left\lceil \sqrt{(x_1 - 2)|E|} \right\rceil + 1 \right) \\ &\leq \frac{y_1 \sqrt{|E|}}{\sqrt{x_1 - 2}} \left(2\sqrt{(x_1 - 2)|E|} + 1 \right) \\ &\leq 2|E|y_1 + y_1 \sqrt{|E|}. \end{aligned}$$

We give an example to illustrate the use of Theorem 1.8.

Example 1.8. Consider the equation $x^2 - 13y^2 = 12 = 4 \cdot 3$. Here $D = 13$ and $E = 3$.

We use Theorem 1.8 to show that $N(13, 3) = 2$. We note first that the fundamental unit of $\mathcal{O}_K$ of norm $+1$, where $K = \mathbb{Q}(\sqrt{13})$, is $\frac{11 + 3\sqrt{13}}{2}$, so that $x_1 = 11$, $y_1 = 3$.

By Theorem 1.8 we have

$$0 \leq v \leq \frac{3\sqrt{3}}{\sqrt{13}} < \frac{3}{2},$$

so that $v = 0$ or $v = 1$. The only value of v such that $12 + 13v^2$ is a perfect square is $v = 1$. Therefore the only possible fundamental solutions of $x^2 - 13y^2 = 12$ are $(5, 1)$ and $(-5, 1)$. As

$$\frac{5 \cdot (-5) - 13 \cdot 1 \cdot 1}{6} = -\frac{19}{3} \notin \mathbb{Z},$$

Theorem 1.6 implies that $(5, 1) \not\sim (-5, 1)$. Thus $[(5, 1)] \neq [(-5, 1)]$. Therefore $N(13, 3) = 2$.

1.4 Two methods to determine the solvability of the Diophantine equation $x^2 - Dy^2 = 4E$

We complete this chapter by discussing briefly two methods in the elementary theory of numbers which are available to discuss the solvability of the equation $x^2 - Dy^2 = 4E$ in integers x and y for certain D and E . The first is the method of descent which has been exploited by Chowla [3] and others [16, Lemma 17, p. 60], [23, p. 195] to prove the insolvability of $x^2 - Dy^2 = 4E$ for certain classes of D and E . This was the method used in Example 1.5. The second is the method of continued fractions.

When $4|E| < \sqrt{D}$ the continued fraction expansion of $\sqrt{D}$ can be used to determine whether the equation $x^2 - Dy^2 = 4E$ is solvable or insolvable, and when solvable it determines a solution. We illustrate these two methods in the next two theorems.

Theorem 1.10. *Let D be the discriminant of a real quadratic field and let E be a nonzero integer. Suppose that D is of the form $D = k^2 - 4$, where k is an integer with*

$$k > 2. \tag{10}$$

$$E \neq \text{a square} \in \mathbb{Z}, \tag{11}$$

$$-(k - 2) < E < k + 2. \tag{12}$$

Then the equation

$$x^2 - Dy^2 = 4E \tag{13}$$

has no solution in integers x and y .

Proof: Clearly (13) does not have a solution with $y = 0$ as E is not a perfect square. Suppose it has a solution with $x = 0$. Then by (12) we have

$$k^2 - 4 = D \leq Dy^2 = -4E < 4k - 8$$

so that

$$(k - 2)^2 < 0,$$

a contradiction. Hence it is enough to show that (13) does not have a solution in positive integers. Suppose that x and y are positive integers satisfying (13). Let (x_1, y_1) be the solution in positive integers to (13) for which y_1 is least. From $x_1^2 - (k^2 - 4)y_1^2 = 4E$ we deduce that $x_1^2 - k^2y_1^2 \equiv 0 \pmod{4}$ so that $x_1 - ky_1 \equiv 0 \pmod{2}$.

Further

$$kx_1 - (k^2 - 4)y_1 = k(x_1 - ky_1) + 4y_1 \equiv 0 \pmod{2}.$$

Thus

$$\frac{x_1 - ky_1}{2}, \quad \frac{kx_1 - (k^2 - 4)y_1}{2}$$

are integers. We set

$$x_2 = \frac{|kx_1 - (k^2 - 4)y_1|}{2}, \quad y_2 = \frac{|x_1 - ky_1|}{2}$$

so that x_2 and y_2 are nonnegative integers. Next

$$\begin{aligned} x_2^2 - (k^2 - 4)y_2^2 &= \left(\frac{kx_1 - (k^2 - 4)y_1}{2} \right)^2 - (k^2 - 4) \left(\frac{x_1 - ky_1}{2} \right)^2 \\ &= x_1^2 - (k^2 - 4)y_1^2 = 4E \end{aligned}$$

so that (x_2, y_2) is a solution of (13). If $y_2 = 0$ then $x_1 = ky_1$ so $E = y_1^2$ contradicting (11). Hence $y_2 \neq 0$. Thus $y_2 \geq 1$. If $x_2 = 0$ then as $k > 2$ and $y_2 \geq 1$

$$4E = (4 - k^2)y_2^2 \leq 4 - k^2 \leq 8 - 4k$$

so that $E \leq 2 - k$, contradicting (12). Thus $x_2 \geq 1$. Hence by the minimality of y_1 we have $y_2 \geq y_1$. Thus either $\frac{x_1 - ky_1}{2} \geq y_1$ or $\frac{ky_1 - x_1}{2} \geq y_1$. In the former case $x_1 \geq (k + 2)y_1$ so

$$4E = x_1^2 - (k^2 - 4)y_1^2 \geq (k + 2)^2 y_1^2 - (k^2 - 4)y_1^2 = (4k + 8)y_1^2 \geq 4k + 8$$

that is $E \geq k + 2$, contradicting (12). In the latter case $(k - 2)y_1 \geq x_1$ so

$$4E = x_1^2 - (k^2 - 4)y_1^2 \leq (k - 2)^2 y_1^2 - (k^2 - 4)y_1^2 = (8 - 4k)y_1^2 \leq 8 - 4k$$

so $E \leq 2 - k$, contradicting (12). □

Example 1.9. Consider the equation $x^2 - 12y^2 = 20$. We use Theorem 1.10 to show that this equation is insolvable in integers x and y . We note first that 12 is the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{3})$. Also $12 = k^2 - 4$ with $k = 4$. Moreover we have

$$-2 < E = 5 < 6.$$

Thus $x^2 - 12y^2 = 20$ is insolvable in integers x and y by Theorem 1.10.

Theorem 1.11. Let D be the discriminant of a real quadratic field and E a nonzero integer. Suppose that D is of the form $D = 4k^2 + 4k$, where k is a positive integer, and that $|E| < \frac{\sqrt{k^2 + k}}{2}$. Then the equation $x^2 - Dy^2 = 4E$ has no solution in coprime integers x and y .

Proof: The proof requires some knowledge of continued fractions. The necessary results can be found in [19, Chapter 7] or [1, Chapter 11]. The continued fraction expansion of $\sqrt{D}$ is

$$\sqrt{D} = [2k, \overline{1, 4k}]$$

so that the period length is 2. The convergents to $\sqrt{D}$ are

$$\frac{h_0}{k_0} = \frac{2k}{1}, \frac{h_1}{k_1} = \frac{2k+1}{1}, \frac{h_2}{k_2} = \frac{8k^2+6k}{4k+1}, \dots$$

A simple induction argument shows that

$$h_n^2 - Dk_n^2 = \begin{cases} -4k, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \text{ is odd.} \end{cases}$$

Thus, by [19, Theorem 7.24, p. 352], the equation $x^2 - Dy^2 = 4E$ is insolvable in coprime integers x and y as $|4E| < \sqrt{4k^2 + 4k}$. $\square$

Example 1.10. Consider the equation $x^2 - 120y^2 = -8$. We use Theorem 1.11 to show that this equation is insolvable in coprime integers x and y . We note first that 120 is the discriminant of the real quadratic field $K = \mathbb{Q}(\sqrt{30})$. Also $120 = 4k^2 + 4k$ with $k = 5$. Moreover we have

$$|E| = 2 < \frac{\sqrt{30}}{2}.$$

Thus $x^2 - 120y^2 = -8$ is insolvable in coprime integers x and y by Theorem 1.11.

Chapter 2

The strict ideal class group and the solvability of the equation $x^2 - Dy^2 = 4E$

In this chapter we recall the definition of the ideal class group $H(K)$ of a real quadratic field K as well as that of the strict ideal class group $H^+(K)$. We then prove a theorem which links the solvability of the equation $x^2 - Dy^2 = 4E$, where D is the discriminant of K and E is a nonzero integer, to the structure of the group $H^+(K)$ and to the solvability of certain congruences involving the orders of the classes of the prime ideals dividing E in $H^+(K)$.

2.1 The group $H(K)$

In this section we define the ideal class group $H(K)$ of a real quadratic field K . We state some theorems without proofs. Proofs of these theorems can be found for example in [1], [4], [21] and [24].

Let K be an algebraic number field. Let $\mathcal{O}_K$ be the ring of integers of K . Let $I(K)$ be the group of nonzero (fractional or integral) ideals of $\mathcal{O}_K$. Let $P(K)$ be the

subgroup of $I(K)$ consisting of principal ideals. As $I(K)$ is an abelian group, $P(K)$ is a normal subgroup of $I(K)$, and the factor group $I(K)/P(K)$ is called the ideal class group of K and is denoted by $H(K)$. The elements of $H(K)$ are the cosets $AP(K)$, where A is a nonzero ideal of $\mathcal{O}_K$. It is known that $H(K)$ is a finite abelian group. The order of the ideal class group $H(K)$ is called the class number of the field K and is denoted by $h(K)$.

Definition 2.1. Two nonzero (fractional or integral) ideals A and B of $\mathcal{O}_K$ are said to be equivalent if there exist $\alpha \in K \setminus \{0\}$ and $\beta \in K \setminus \{0\}$ such that $\langle \alpha \rangle A = \langle \beta \rangle B$. If A and B are equivalent we write $A \sim B$.

Clearly $A \sim B \iff A = \langle \delta \rangle B$ for some $\delta \in K \setminus \{0\} \iff AB^{-1} \in P(K) \iff AP(K) = BP(K)$. The equivalence class containing the ideal A is $[A] = AP(K)$. The product of equivalence classes is given by $[A][B] = (AP(K))(BP(K)) = ABP(K) = [AB]$.

Now let K be a real quadratic field. Let D denote the discriminant $d(K)$ of K . Define $\left(\frac{D}{p}\right)$ to be the Legendre symbol for an odd prime p and the Kronecker symbol for $p = 2$. The next theorem gives the factorization of the principal ideal $\langle p \rangle$ into prime ideals in $\mathcal{O}_K$. The norm of the prime ideal P is denoted by $N(P)$.

Theorem 2.1. Let K be a real quadratic field. Let $D = d(K)$. Let p be a prime. Then

$$(1) \langle p \rangle = P_1 P_2, N(P_1) = N(P_2) = p, P_1 \neq P_2 \iff \left(\frac{D}{p}\right) = 1,$$

$$(2) \langle p \rangle = P^2, N(P) = p \iff \left(\frac{D}{p}\right) = 0,$$

$$(3) \langle p \rangle = P, N(P) = p^2 \iff \left(\frac{D}{p}\right) = -1,$$

where P_1, P_2, P denote prime ideals of $\mathcal{O}_K$.

In Case (1) we say that p splits in K , in Case (2) that p ramifies and in Case (3) that p is inert.

The following algorithm determines the ideal class group of a real quadratic field K . It can be found in [1] and [4].

Input : Quadratic field $K = \mathbb{Q}(\sqrt{m})$, where m is a positive squarefree integer.

Step 1 : Determine the discriminant $d(K)$.

Step 2 : Compute the Minkowski bound $M_K = \sqrt{d(K)}$.

Step 3 : Determine all rational primes $p \leq M_K$.

Step 4 : Determine the prime ideal factorization of each principal ideal $\langle p \rangle$ in $\mathcal{O}_K$

with p as in Step 3.

Step 5 : Determine all products of these primes ideals having norm $\leq M_K$.

Step 6 : Determine the generators of $H(K)$ from classes of these products.

Output : $H(K)$.

We will see that the ideal class group $H(K)$ of a real quadratic field K of discriminant

D plays an important role in determining whether or not the equation $x^2 - Dy^2 = 4E$ is solvable in integers x and y . But first we define another group, namely the strict ideal class group $H^+(K)$ of K .

2.2 The group $H^+(K)$

Definition 2.2. Let K be an algebraic number field. Let $\mathcal{O}_K$ be the ring of integers of K . Two nonzero ideals (fractional or integral) A and B of $\mathcal{O}_K$ are said to be strictly equivalent if there exist $\alpha \in K \setminus \{0\}$ and $\beta \in K \setminus \{0\}$ such that $\langle \alpha \rangle A = \langle \beta \rangle B$, where $N(\alpha\beta) > 0$.

If A and B are strictly equivalent we write $A \approx B$. Clearly $\approx$ is an equivalence relation on the set of nonzero fractional and integral ideals of $\mathcal{O}_K$, and $A \approx B \implies A \sim B$. The strict equivalence class containing the ideal A is denoted by $[A]_+$.

Let $B \in [A]_+$. Then $B \approx A$. Hence $B \sim A$. Thus $B \in [A]$. We have shown that

$$[A]_+ \subseteq [A].$$

The product of strict equivalence classes is given by $[A]_+[B]_+ = [AB]_+$. With respect to multiplication, the set $H^+(K)$ of strict equivalence classes of nonzero fractional or integral ideals of $\mathcal{O}_K$ is a group called the strict ideal class group. It is known that $H^+(K)$ is a finite abelian group. The order of this group is the strict class number $h^+(K)$. By the fundamental theorem of finite abelian groups there exist

$h_1, \dots, h_m \in \mathbb{N}$ such that

$$H^+(K) \simeq \mathbb{Z}_{h_1} \times \cdots \times \mathbb{Z}_{h_m}, \quad (1)$$

where $h_1 \cdots h_m = h^+(K)$ and $1 < h_1 \mid h_2 \mid \cdots \mid h_m$. The positive integers $h_1, \dots, h_m$ are called the invariants of $H^+(K)$. Moreover there exist $H_1, \dots, H_m \in H^+(K)$ such that $\text{ord}(H_i) = h_i$ ($i = 1, \dots, m$) and for each strict ideal class C in $H^+(K)$ there exist unique integers $k_1, \dots, k_m$ such that the class is given by

$$C = H_1^{k_1} \cdots H_m^{k_m}, \quad \text{where } 0 \leq k_i < h_i, \quad i = 1, \dots, m.$$

We set

$$V_{H_i}(C) = k_i, \quad i = 1, 2, \dots, m,$$

so that

$$C = \prod_{i=1}^m H_i^{V_{H_i}(C)}.$$

We now give a theorem that will allow us to find $H^+(K)$ given $H(K)$. We first state a lemma.

Lemma 2.1. *Let $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer. Let A and B be two nonzero fractional or integral ideals of $\mathcal{O}_K$ such that $A \sim B$, so that there exist $\alpha, \beta \in K \setminus \{0\}$ such that $\langle \alpha \rangle A = \langle \beta \rangle B$. When $m > 0$ let η_1 denote the fundamental unit > 1 of $\mathcal{O}_K$.*

(a) If $m < 0$ we have $A \approx B$.

(b) If $m > 0$ and $N(\eta_1) < 0$, we have $A \approx B$.

(c) If $m > 0$ and $N(\eta_1) > 0$ we have either $A \approx B$ or $A \approx \sqrt{D}B$ but not both.

Proof:

case (a) : $m < 0$.

Since $m < 0$ we have $N(\alpha) > 0$ and $N(\beta) > 0$. Therefore $N(\alpha\beta) = N(\alpha)N(\beta) > 0$.

Hence $\langle \alpha \rangle A = \langle \beta \rangle B$ with $N(\alpha\beta) > 0$ so $A \approx B$.

case (b) : $m > 0$, $N(\eta_1) < 0$.

We have $\langle \alpha \rangle A = \langle \beta \rangle B$. If $N(\alpha\beta) > 0$ then $A \approx B$. If $N(\alpha\beta) < 0$ we note that

$\alpha\eta_1 \in K$,

$$\langle \alpha\eta_1 \rangle A = \langle \alpha \rangle A = \langle \beta \rangle B,$$

and $N(\alpha\eta_1\beta) = N(\alpha\beta)N(\eta_1) > 0$ so $A \approx B$.

case (c) : $m > 0$, $N(\eta_1) > 0$.

We have $\langle \alpha \rangle A = \langle \beta \rangle B$. If $A \sim B$ and $A \not\approx B$ we must have $N(\alpha\beta) < 0$.

Now $\langle \alpha\sqrt{D} \rangle A = \langle \beta \rangle \sqrt{D}B$ and as $N(\alpha\sqrt{D}\beta) = -DN(\alpha\beta) > 0$ so $A \approx \sqrt{D}B$.

Next we show that we cannot have both $A \approx B$ and $A \approx \sqrt{D}B$. Suppose on the

contrary that $A \approx B$ and $A \approx \sqrt{D}B$. Then $B \approx \sqrt{D}B$. Hence there exist $\alpha \in K \setminus \{0\}$

and $\beta \in K \setminus \{0\}$ such that $\langle \alpha \rangle B = \langle \beta \rangle \sqrt{D}B$ and $N(\alpha\beta) > 0$. Thus, as $B \neq 0$,

$\langle \alpha \rangle = \langle \beta \rangle \sqrt{D}$ so that $\langle \sqrt{D} \rangle = \langle \delta \rangle$, where $\delta = \alpha\beta^{-1} \in K$ satisfies

$N(\delta) = N(\alpha)/N(\beta) = N(\alpha\beta)/N(\beta)^2 > 0$. Hence $\sqrt{D} = \varepsilon\delta$ for some unit $\varepsilon \in \mathcal{O}_K$. As $N(\eta_1) > 0$ we have $N(\varepsilon) > 0$. Thus $-D = N(\sqrt{D}) = N(\varepsilon\delta) = N(\varepsilon)N(\delta) > 0$, a contradiction. $\square$

We now use this lemma to relate the structure of the group $H^+(K)$ to that of $H(K)$.

Theorem 2.2. *Let $K = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer. Let $h = h(K)$.*

Let $A_1, \dots, A_h$ be ideals of $\mathcal{O}_K$ such that $H(K) = \{[A_1], \dots, [A_h]\}$. When $m > 0$ let η_1 denote the fundamental unit > 1 of $\mathcal{O}_K$.

(1) *If $m < 0$ or if $m > 0$ and $N(\eta_1) < 0$ we have $[A] = [A]_+$ for all ideals A so that $H(K) = H^+(K)$.*

(2) *If $m > 0$ and $N(\eta_1) > 0$ we have*

$$H^+(K) = \{ [A_1]_+, [\sqrt{D}A_1]_+, \dots, [A_h]_+, [\sqrt{D}A_h]_+ \}.$$

Proof:

case (1) : $m < 0$ or $m > 0$ and $N(\eta_1) < 0$.

If $A \sim B$ then by Lemma 2.1 we have $A \approx B$. Therefore $[A] = [A]_+$ for all ideals A and so $H(K) = H^+(K)$.

case (2) : $m > 0$ and $N(\eta_1) > 0$.

It is clear from Lemma 2.1(c) that when $m > 0$ and $N(\eta_1) > 0$ then

$$[A]_+ \cap [\sqrt{D}A]_+ = \emptyset$$

and

$$\begin{aligned} [A] &= \{B \mid B \sim A\} = \{B \mid B \approx A \text{ or } B \approx \sqrt{D}A\} \\ &= \{B \mid B \approx A\} \cup \{B \mid B \approx \sqrt{D}A\} = [A]_+ \cup [\sqrt{D}A]_+. \end{aligned}$$

First we show that

$$[A_i]_+ \neq [A_j]_+ \text{ for } i, j \in \{1, 2, \dots, h\}, i \neq j.$$

Suppose that $[A_i]_+ = [A_j]_+$. Then $A_i \approx A_j$. Hence $A_i \sim A_j$. Thus $[A_i] = [A_j]$, and so $i = j$, a contradiction.

Next we show that

$$[A_i]_+ \neq [\sqrt{D}A_j]_+ \text{ for } i, j \in \{1, 2, \dots, h\}.$$

Suppose $[A_i]_+ = [\sqrt{D}A_j]_+$. Then $A_i \approx \sqrt{D}A_j$. Hence $A_i \sim \sqrt{D}A_j \sim A_j$ so $i = j$. Thus $A_i \approx \sqrt{D}A_i$, contradicting Lemma 2.1(c).

We have now shown that $[A_1]_+, [\sqrt{D}A_1]_+, \dots, [A_h]_+, [\sqrt{D}A_h]_+$ are $2h$ distinct elements of $H^+(K)$.

Now consider $[B]_+ \in H^+(K)$. Then $[B] \in H(K)$. Hence $B \sim A_i$ for some $i \in \{1, 2, \dots, h\}$. By Lemma 2.1(c) either $B \approx A_i$ or $B \approx \sqrt{D}A_i$. Therefore $[B]_+ = [A_i]_+$ or $[\sqrt{D}A_i]_+$.

This completes the proof that

$$H^+(K) = \{[A_1]_+, [\sqrt{D}A_1]_+, \dots, [A_h]_+, [\sqrt{D}A_h]_+\}.$$

□

As consequence of Theorem 2.2 we have

$$h^+(K) = \begin{cases} h(K), & \text{if } m < 0 \text{ or if } m > 0 \text{ and } N(\eta_1) < 0, \\ 2h(K), & \text{if } m > 0 \text{ and } N(\eta_1) > 0. \end{cases}$$

We finish this section with two useful lemmas.

Lemma 2.2. *Let K be a real quadratic field. Let $H^+(K)$ be the strict ideal class group and let $\alpha \in K \setminus \{0\}$.*

- (1) *If $N(\alpha) > 0$, we have $[\langle \alpha \rangle]_+ = [\langle 1 \rangle]_+$.*
- (2) *If $N(\alpha) < 0$, we have $[\langle \alpha \rangle]_+ = [\langle \sqrt{D} \rangle]_+$.*

Proof:

case (1) :

$1 \langle \alpha \rangle = \langle 1\alpha \rangle = \alpha \langle 1 \rangle$ and $N(1\alpha) = N(\alpha) > 0$. Thus we have $\langle \alpha \rangle \approx \langle 1 \rangle$, that is, $[\langle \alpha \rangle]_+ = [\langle 1 \rangle]_+$.

case (2) :

$\sqrt{D} \langle \alpha \rangle = \langle \sqrt{D}\alpha \rangle = \alpha \langle \sqrt{D} \rangle$ and $N(\sqrt{D}\alpha) = N(\sqrt{D})N(\alpha) > 0$ as $N(\sqrt{D}) < 0$ and $N(\alpha) < 0$. Thus we have $\langle \alpha \rangle \approx \langle \sqrt{D} \rangle$, that is, $[\langle \alpha \rangle]_+ = [\langle \sqrt{D} \rangle]_+$. $\square$

Lemma 2.3. *Let K be a real quadratic field. Then*

$$H^+(K) = H(K) \iff [A]_+ = [A] \text{ for all nonzero ideals } A \text{ of } \mathcal{O}_K.$$

Proof: If $[A]_+ = [A]$ for all nonzero ideals A of $\mathcal{O}_K$ then clearly $H^+(K) = H(K)$.

Now suppose that $H^+(K) = H(K)$. We wish to prove that $[A]_+ = [A]$ for all

nonzero ideals A of $\mathcal{O}_K$. Suppose this is not the case. Then there exists an ideal A of $\mathcal{O}_K$ such that $[A]_+ \neq [A]$. But $[A]_+ \subseteq [A]$ so we have $[A]_+ \subset [A]$. Hence there exists $B \in [A]$ with $B \notin [A]_+$. Thus $B \sim A$ but $B \not\approx A$. By Lemma 2.1 we are not in cases (a) or (b). Thus case (c) holds. But in this case by Theorem 2.2 $H^+(K) \simeq \mathbb{Z}_2 \times H(K)$ so $|H^+(K)| = 2|H(K)|$, contradicting $|H^+(K)| = |H(K)|$. $\square$

2.3 The solvability of $x^2 - Dy^2 = 4E$.

In this section we give a necessary and sufficient condition for the solvability of the equation $x^2 - Dy^2 = 4E$ in integers x and y , where D is the discriminant of a real quadratic field K and E is a nonzero integer. We will see that this depends on the structure of the strict ideal class group $H^+(K)$, where $K = \mathbb{Q}(\sqrt{D})$, as well as the classes of some prime ideals in the same group.

We begin with a theorem that gives a sufficient condition for the insolubility of the equation $x^2 - Dy^2 = 4E$ in integers x and y .

Theorem 2.3. *Let D be the discriminant of a real quadratic field. Let E be a nonzero integer. Let r be a prime which is inert in $\mathbb{Q}(\sqrt{D})$, so that $\left(\frac{D}{r}\right) = -1$. If $r^{2k+1} \parallel E$ then the equation $x^2 - Dy^2 = 4E$ is not solvable in integers x and y .*

Proof: We suppose that x and y are integers such that $x^2 - Dy^2 = 4E$ and obtain a contradiction. As r is a prime, which is inert in $\mathbb{Q}(\sqrt{D})$, we have $\left(\frac{D}{r}\right) = -1$. Hence $r \nmid D$. We first show that $y \neq 0$. If $y = 0$ then $x^2 = 4E$ and so $r^{2k+1} \parallel x^2$ if

$r > 2$ and $r^{2k+3} \parallel x^2$ if $r = 2$. In both cases we have a contradiction. Next we show that $x \neq 0$. If $x = 0$ then $-Dy^2 = 4E$. As D is the discriminant of a real quadratic field, we have $D > 0$. As $E \neq 0$ we have $y \neq 0$ and $Dy^2 = 4|E|$. As $r^{2k+1} \parallel E$ we have $r^{2k+1} \parallel Dy^2$ if $r > 2$ and $r^{2k+3} \parallel Dy^2$ if $r = 2$, a contradiction as $r \nmid D$. Hence $x \neq 0$ and $y \neq 0$. Thus we can define nonnegative integers α and β by

$$r^\alpha \parallel x, \quad r^\beta \parallel y.$$

If $\alpha > \beta$ then $r^{2\beta} \parallel x^2 - Dy^2 = 4E$, contradicting $r^{2k+1} \parallel E$. If $\alpha < \beta$ then $r^{2\alpha} \parallel x^2 - Dy^2 = 4E$, contradicting $r^{2k+1} \parallel E$. Hence $\alpha = \beta$. Define $x_1 = \frac{x}{r^\alpha} \in \mathbb{Z}$ and $y_1 = \frac{y}{r^\alpha} \in \mathbb{Z}$. Then $r \nmid x_1$, $r \nmid y_1$ and

$$4E = x^2 - Dy^2 = r^{2\alpha}(x_1^2 - Dy_1^2),$$

so that $r^{2\alpha} \mid 4E$. Define $E_1 = \frac{4E}{r^{2\alpha}} \in \mathbb{Z}$. Hence

$$x_1^2 - Dy_1^2 = E_1.$$

As $r^{2k+1} \parallel E$ we have $r \mid E_1$. Thus as $r \nmid y_1$ we have

$$-1 = \left(\frac{D}{r}\right) = \left(\frac{Dy_1^2}{r}\right) = \left(\frac{x_1^2 - E_1}{r}\right) = \left(\frac{x_1^2}{r}\right) = 1,$$

a contradiction. This completes the proof that $x^2 - Dy^2 = 4E$ has no solutions in integers x and y . □

The representation of the ideal class $[< \sqrt{D} >]_+$ will be important for our theorem on the solvability of the equation $x^2 - Dy^2 = 4E$.

Theorem 2.4. Let K be a real quadratic field of discriminant D so that $K = \mathbb{Q}(\sqrt{D})$.

Let $H_1, \dots, H_m$ be the generators of $H^+(K)$ as specified in (1). Let $[\langle \sqrt{D} \rangle]_+$ be the strict ideal class of the ideal $\langle \sqrt{D} \rangle$. Then

$$(1) [\langle \sqrt{D} \rangle]_+ = [\langle 1 \rangle]_+ \iff H(K) = H^+(K).$$

(2) If $H^+(K) \neq H(K)$ then there exist unique integers $c_1, \dots, c_m$ with $0 \leq c_i < h_i$,

$i = 1, \dots, m$ such that

$$(a) [\langle \sqrt{D} \rangle]_+ = H_1^{c_1} \dots H_m^{c_m}.$$

(b) The c_i are not all 0.

(c) Each $c_i = 0$ or $\frac{h_i}{2}$, $i = 1, 2, \dots, m$.

Proof:

Proof of (1): If $[\langle \sqrt{D} \rangle]_+ = [\langle 1 \rangle]_+$ then $\langle \sqrt{D} \rangle = \alpha \langle 1 \rangle = \langle \alpha \rangle$, for some $\alpha \in K \setminus \{0\}$ with $N(\alpha) > 0$. Hence $\sqrt{D} = \varepsilon \alpha$, where ε is a unit. This implies that $N(\varepsilon) = \frac{N(\sqrt{D})}{N(\alpha)} < 0$. Thus $N(\varepsilon) = -1$. Therefore $H(K) = H^+(K)$ by Theorem 2.2. Conversely suppose that $H(K) = H^+(K)$. By Lemma 2.3 we have $[\langle 1 \rangle] = [\langle 1 \rangle]_+$ and $[\sqrt{D}] = [\sqrt{D}]_+$. As $\langle \sqrt{D} \rangle \sim \langle 1 \rangle$, we have $[\langle \sqrt{D} \rangle] = [\langle 1 \rangle]$. This implies that $[\langle \sqrt{D} \rangle]_+ = [\langle 1 \rangle]_+$.

Proof of (2): Suppose that $H(K) \neq H^+(K)$. As $H^+(K)$ is a finite abelian group with generators $H_1, \dots, H_m$ of orders $h_1, \dots, h_m$ respectively, we know that there exist unique integers $c_1, \dots, c_m$ with $0 \leq c_i \leq h_i$, $i = 1, \dots, m$, such that $[\langle \sqrt{D} \rangle]_+ = H_1^{c_1} \dots H_m^{c_m}$. Hence $H_1^{2c_1} \dots H_m^{2c_m} = [\langle \sqrt{D} \rangle]_+^2 = [\langle \sqrt{D} \rangle^2]_+ = [\langle D \rangle]_+ = [\langle 1 \rangle]_+$.

Therefore $2c_i \equiv 0 \pmod{h_i}$ for all $i \in \{1, \dots, m\}$. If h_i is odd, then $c_i \equiv 0 \pmod{h_i}$ so, as $0 \leq c_i < h_i$, we have $c_i = 0$. If h_i is even, then $c_i \equiv 0 \pmod{\frac{h_i}{2}}$ so, as $0 \leq c_i < h_i$, we have $c_i = 0$ or $c_i = \frac{h_i}{2}$.

Without loss of generality we may suppose that $h_1, \dots, h_k$ are odd and $h_{k+1}, \dots, h_m$ are even, where $0 \leq k \leq m$. As $H(K) \neq H^+(K)$ we have $[\langle \sqrt{D} \rangle]_+ \neq [\langle 1 \rangle]_+$, by (1) of this theorem. Therefore, since each $c_i = 0$ or $\frac{h_i}{2}$, there is at least one c_i such that $c_i = \frac{h_i}{2}$. $\square$

We are now ready to state and prove a theorem giving necessary and sufficient conditions for the solvability of the equation $x^2 - Dy^2 = 4E$.

Theorem 2.5. *Let K be a real quadratic field of discriminant D so that $K = \mathbb{Q}(\sqrt{D})$.*

Let E be a nonzero integer.

Let $p_1, \dots, p_r$ be the primes dividing E such that $\left(\frac{D}{p_i}\right) = +1$.

Let $q_1, \dots, q_s$ be the primes dividing E such that $\left(\frac{D}{q_j}\right) = 0$.

Let $r_1, \dots, r_t$ be the primes dividing E such that $\left(\frac{D}{r_k}\right) = -1$.

(If there are no primes $p_i \mid E$ with $\left(\frac{D}{p_i}\right) = +1$, we take $r = 0$ and understand the product $p_1^{a_1} \cdots p_r^{a_r}$ to be the empty product $= 1$, similarly for s and t .) We assume that each prime r_i divides E to an even power (otherwise the equation is not solvable

by Theorem 2.3). We have

$$E = (\text{sgn } E) p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t},$$

where $a_1, \dots, a_r, b_1, \dots, b_s, c_1, \dots, c_t$ are positive integers. In $\mathcal{O}_K$ we have

$\langle p_i \rangle = P_i P'_i$, $i = 1, 2, \dots, r$, where P_i and P'_i are distinct conjugate prime ideals

with $N(P_i) = N(P'_i) = p_i$,

$\langle q_j \rangle = Q_j^2$, $j = 1, \dots, s$, where Q_j is a self-conjugate prime ideal with $N(Q_j) = q_j$,

and

$\langle r_k \rangle = R_k$, $k = 1, \dots, t$, where R_k is a self-conjugate prime ideal with $N(R_k) = r_k^2$.

Let $\{H_1, \dots, H_m\}$ be a fixed set of generators of $H^+(K)$ with $\text{ord}(H_i) = h_i$, where

$i = 1, 2, \dots, m$, and

$$1 < h_1 \mid \cdots \mid h_m, \quad h_1 \cdots h_m = h^+(K).$$

(1) There is at least one prime p_i dividing E such that $\left(\frac{D}{p_i}\right) = +1$ (that is $r \geq 1$).

(a) If $E > 0$ or $E < 0$ and $H^+(K) = H(K)$ then the equation $x^2 - Dy^2 = 4E$

is solvable in integers x and y if and only if there exists $(k_1, \dots, k_r) \in \mathbb{Z}^r$, where

$k_i \in \{0, 1, \dots, a_i\}$, $i = 1, \dots, r$, such that

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w}$$

for all $w \in \{1, 2, \dots, m\}$.

(b) If $E < 0$ and $H^+(K) \neq H(K)$ then the equation $x^2 - Dy^2 = 4E$ is solvable in integers x and y if and only if there exists $(k_1, \dots, k_r) \in \mathbb{Z}^r$, where $k_i \in \{0, 1, \dots, a_i\}$, $i = 1, \dots, r$, such that

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w}$$

for all $w \in \{1, 2, \dots, m\}$, where $c_1, \dots, c_w$ are the unique integers in the representation of $[< \sqrt{D} >]_+$ in Theorem 2.4.

(2) There is no prime p_i dividing E such that $\left(\frac{D}{p_i}\right) = +1$ (so that $r = 0$).

(a) If $E > 0$ or $E < 0$ and $H^+(K) = H(K)$ then the equation $x^2 - Dy^2 = 4E$ is solvable in integers x and y if and only if

$$\sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w}$$

for all $w \in \{1, 2, \dots, m\}$.

(b) If $E < 0$ and $H^+(K) \neq H(K)$ then the equation $x^2 - Dy^2 = 4E$ is solvable in integers x and y if and only if

$$\sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w}$$

for all $w \in \{1, 2, \dots, m\}$, where $c_1, \dots, c_w$ are the unique integers in the representation of $[< \sqrt{D} >]_+$ in Theorem 2.4.

We remark that cases (1) and (2) can be combined by interpreting the sum

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) \text{ as the empty sum} = 0 \text{ when } r = 0.$$

Proof:

case (1)(a) : $E > 0$ or $E < 0$, $H(K) = H^+(K)$.

There is at least one prime p dividing E such that $\left(\frac{D}{p}\right) = +1$, so that $r \geq 1$.

Moreover $E > 0$ or $E < 0$ and $H^+(K) = H(K)$. Theorem 2.4 tells us that

$[< \sqrt{D} >]_+ = [< 1 >]_+$ if $H^+(K) = H(K)$. Let

$\mathcal{K}$ = the set of $\underline{k} = (k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $k_i \in \{0, 1, \dots, a_i\}$ ($i = 1, \dots, r$) and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for all $w \in \{1, \dots, m\}$.

($\Leftarrow$;) Suppose $\mathcal{K} \neq \emptyset$. Then there exists $\underline{k} = (k_1, \dots, k_r) \in \mathcal{K}$. In $H^+(K)$ we have

$$[P_i]_+[P'_i]_+ = [P_i P'_i]_+ = [< p_i >]_+ = [< 1 >]_+, \quad i = 1, 2, \dots, r,$$

so that

$$[P'_i]_+ = [P_i]_+^{-1}, \quad i = 1, 2, \dots, r,$$

and

$$[R_k]_+ = [< r_k >]_+ = [< 1 >]_+, \quad k = 1, 2, \dots, t.$$

Then

$$\left[\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} \right]_+$$

$$\begin{aligned}
&= \prod_{i=1}^r [P_i]_+^{k_i} [P_i']_+^{a_i - k_i} \prod_{j=1}^s [Q_j]_+^{b_j} \prod_{k=1}^t [R_k]_+^{c_k} \\
&= \prod_{i=1}^r [P_i]_+^{2k_i - a_i} \prod_{j=1}^s [Q_j]_+^{b_j} \\
&= \prod_{i=1}^r \left(\prod_{w=1}^m H_w^{V_{H_w}([P_i]_+)} \right)^{2k_i - a_i} \prod_{j=1}^s \left(\prod_{w=1}^m H_w^{V_{H_w}([Q_j]_+)} \right)^{b_j} \\
&= \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)} \\
&= [\langle 1 \rangle]_+.
\end{aligned}$$

Hence for each $\underline{k} \in \mathcal{K}$ there exists $\delta(\underline{k}) \in \mathcal{O}_K$ such that

$$\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \langle \delta(\underline{k}) \rangle, \quad N(\delta(\underline{k})) > 0. \quad (2)$$

As $\delta(\underline{k}) \in \mathcal{O}_K$ there exist $x(\underline{k}) \in \mathbb{Z}$ and $y(\underline{k}) \in \mathbb{Z}$ such that $\delta(\underline{k}) = \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2}$, so that $N(\delta(\underline{k})) = \frac{x(\underline{k})^2 - Dy(\underline{k})^2}{4}$. Taking norms of both sides of the equation in (2), we obtain

$$\begin{aligned}
N(\delta(\underline{k})) &= |N(\delta(\underline{k}))| = N(\langle \delta(\underline{k}) \rangle) \\
&= N \left(\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} \right) \\
&= \prod_{i=1}^r N(P_i)^{a_i} \prod_{j=1}^s N(Q_j)^{b_j} \prod_{k=1}^t N(R_k)^{c_k} \\
&= \prod_{i=1}^r p_i^{a_i} \prod_{j=1}^s q_j^{b_j} \prod_{k=1}^t r_k^{2c_k} = |E|.
\end{aligned}$$

If $E > 0$ we have $(x(\underline{k}))^2 - D(y(\underline{k}))^2 = 4E$. Therefore $x^2 - Dy^2 = 4E$ is solvable.

If $E < 0$ and $H^+(K) = H(K)$ then by Lemma 2.3 and Theorem 2.2 we have $N(\eta_1) =$

-1 , where η_1 is the fundamental unit of $\mathcal{O}_K$, then $\eta_1\delta(\underline{k}) \in \mathcal{O}_K$ and $N(\eta_1\delta(\underline{k})) < 0$.

Therefore

$$-N(\eta_1\delta(\underline{k})) = |N(\eta_1\delta(\underline{k}))| = N(\langle \eta_1\delta(\underline{k}) \rangle) = N(\langle \delta(\underline{k}) \rangle) = |E| = -E,$$

so $N(\eta_1\delta(\underline{k})) = E$. Set $\eta_1\delta(\underline{k}) = \frac{x_1(\underline{k}) + y_1(\underline{k})\sqrt{D}}{2} \in \mathcal{O}_K$. Then we have

$$(x_1(\underline{k}))^2 - D(y_1(\underline{k}))^2 = 4E. \text{ Therefore } x^2 - Dy^2 = 4E \text{ is solvable.}$$

($\implies$.) Suppose the equation $x^2 - Dy^2 = 4E$, where $E = (\text{sgn } E) p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t}$

is solvable. Let $(x, y) \in \mathbb{Z}^2$ be a solution. Then

$$\begin{aligned} \left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \left\langle \frac{x - y\sqrt{D}}{2} \right\rangle &= \langle p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t} \rangle \\ &= \langle p_1 \rangle^{a_1} \cdots \langle p_r \rangle^{a_r} \langle q_1 \rangle^{b_1} \cdots \langle q_s \rangle^{b_s} \langle r_1 \rangle^{2c_1} \cdots \langle r_t \rangle^{2c_t} \\ &= P_1^{a_1} P_1'^{a_1} \cdots P_r^{a_r} P_r'^{a_r} Q_1^{2b_1} \cdots Q_s^{2b_s} R_1^{2c_1} \cdots R_t^{2c_t}. \end{aligned}$$

Hence

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = P_1^{k_1} P_1'^{k_1'} \cdots P_r^{k_r} P_r'^{k_r'} Q_1^{r_1} \cdots Q_s^{r_s} R_1^{s_1} \cdots R_t^{s_t}, \quad (3)$$

and

$$\left\langle \frac{x - y\sqrt{D}}{2} \right\rangle = P_1^{a_1 - k_1} P_1'^{a_1 - k_1'} \cdots P_r^{a_r - k_r} P_r'^{a_r - k_r'} Q_1^{2b_1 - r_1} \cdots Q_s^{2b_s - r_s} R_1^{2c_1 - s_1} \cdots R_t^{2c_t - s_t}$$

for some integers $k_1, \dots, k_r, k_1', \dots, k_r', r_1, \dots, r_s, s_1, \dots, s_t$ such that

$$k_i, k_i' \in \{0, \dots, a_i\}, \quad i \in \{1, \dots, r\},$$

$$r_j \in \{0, \dots, 2b_j\}, \quad j \in \{1, \dots, s\},$$

$$s_k \in \{0, \dots, 2c_k\}, \quad k \in \{1, \dots, t\}.$$

As $x^2 - Dy^2 = 4E$ we have

$$N \left(\left\langle \frac{x + \sqrt{D}y}{2} \right\rangle \right) = |E| = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t}$$

and by (3)

$$N \left(\left\langle \frac{x + \sqrt{D}y}{2} \right\rangle \right) = p_1^{k_1+k'_1} \cdots p_r^{k_r+k'_r} q_1^{r_1} \cdots q_s^{r_s} r_1^{2s_1} \cdots r_t^{2s_t}.$$

This implies that

$$k_i + k'_i = a_i, \quad i \in \{1, \dots, r\},$$

$$r_j = b_j, \quad j \in \{1, \dots, s\},$$

$$c_k = s_k, \quad k \in \{1, \dots, t\}.$$

Thus

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = P_1^{k_1} P_1'^{a_1-k_1} \cdots P_r^{k_r} P_r'^{a_r-k_r} Q_1^{b_1} \cdots Q_s^{b_s} R_1^{c_1} \cdots R_t^{c_t}.$$

Since $[P'_i]_+ = [P_i]_+^{-1}$ ($i = 1, 2, \dots, r$) and $[R_k]_+ = [\langle 1 \rangle]_+$ ($k = 1, \dots, t$) in $H^+(K)$,

we have

$$\left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = \prod_{i=1}^r [P_i]_+^{2k_i-a_i} \prod_{j=1}^s [Q_j]_+^{b_j} = \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i-a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}.$$

If $E > 0$ then $N \left(\frac{x + y\sqrt{D}}{2} \right) > 0$ so that $\left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = [\langle 1 \rangle]_+$ by Theorem 2.2(1).

If $E < 0$ and $H(K) = H^+(K)$ then by Lemma 2.3 and Theorem 2.2 we have $N(\eta_1) < 0$

$$\text{and } \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right] = [\langle 1 \rangle] = [\langle 1 \rangle]_+.$$

Hence

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for all $w \in \{1, 2, \dots, m\}$. Therefore, there is a $\underline{k} = (k_1, \dots, k_r) \in \mathcal{K}$, proving $\mathcal{K} \neq \emptyset$.

case (1)(b) : $E < 0$ and $H^+(K) \neq H(K)$.

As $H^+(K) \neq H(K)$ Theorem 2.4 tells us that $[\langle \sqrt{D} \rangle]_+ \neq [\langle 1 \rangle]_+$. Let

$\mathcal{K}$ = the set of $\underline{k} = (k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $k_i \in \{0, 1, \dots, a_i\}$ ($i = 1, \dots, r$) and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w},$$

for all $w \in \{1, \dots, m\}$.

($\Leftarrow$): Suppose $\mathcal{K} \neq \emptyset$. Then there exists $\underline{k} = (k_1, \dots, k_r) \in \mathcal{K}$. In $H^+(K)$ we have

$$[P_i]_+[P'_i]_+ = [P_i P'_i]_+ = [\langle p_i \rangle]_+ = [\langle 1 \rangle]_+, \quad i = 1, 2, \dots, r,$$

so that

$$[P'_i]_+ = [P_i]_+^{-1}, \quad i = 1, 2, \dots, r,$$

and

$$[R_k]_+ = [\langle r_k \rangle]_+ = [\langle 1 \rangle]_+, \quad k = 1, 2, \dots, t.$$

Then

$$\begin{aligned}
& \left[\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} \right]_+ \\
&= \prod_{i=1}^r [P_i]_+^{k_i} [P_i']_+^{a_i - k_i} \prod_{j=1}^s [Q_j]_+^{b_j} \prod_{k=1}^t [R_k]_+^{c_k} \\
&= \prod_{i=1}^r [P_i]_+^{2k_i - a_i} \prod_{j=1}^s [Q_j]_+^{b_j} \\
&= \prod_{i=1}^r \left(\prod_{w=1}^m H_w^{V_{H_w}([P_i]_+)} \right)^{2k_i - a_i} \prod_{j=1}^s \left(\prod_{w=1}^m H_w^{V_{H_w}([Q_j]_+)} \right)^{b_j} \\
&= \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)} \\
&= \prod_{w=1}^m H_w^{c_w} \\
&= [\langle \sqrt{D} \rangle]_+.
\end{aligned}$$

Hence by Lemma 2.2(2) for each $\underline{k} \in \mathcal{K}$ there exists $\delta(\underline{k}) \in \mathcal{O}_K$ such that

$$\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \langle \delta(\underline{k}) \rangle, \quad N(\delta(\underline{k})) < 0. \quad (4)$$

As $\delta(\underline{k}) \in \mathcal{O}_K$ there exist $x(\underline{k}) \in \mathbb{Z}$ and $y(\underline{k}) \in \mathbb{Z}$ such that $\delta(\underline{k}) = \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2}$, so that $N(\delta(\underline{k})) = \frac{x(\underline{k})^2 - Dy(\underline{k})^2}{4}$. Taking norms of both sides of the equation in

(4), we obtain

$$\begin{aligned}
-N(\delta(\underline{k})) &= |N(\delta(\underline{k}))| = N(\langle \delta(\underline{k}) \rangle) \\
&= N \left(\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} \right) \\
&= \prod_{i=1}^r N(P_i)^{a_i} \prod_{j=1}^s N(Q_j)^{b_j} \prod_{k=1}^t N(R_k)^{c_k}
\end{aligned}$$

$$= \prod_{i=1}^r p_i^{a_i} \prod_{j=1}^s q_j^{b_j} \prod_{k=1}^t r_k^{2c_k} = |E| = -E.$$

so that $N(\delta(\underline{k})) = E$. By Theorem 1.3 we have that $(x(\underline{k}))^2 - D(y(\underline{k}))^2 = 4E$.

Therefore $x^2 - Dy^2 = 4E$ is solvable.

($\Rightarrow$): Let $(x, y) \in \mathbb{Z}^2$ be a solution of $x^2 - Dy^2 = 4E$. Then

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \left\langle \frac{x - y\sqrt{D}}{2} \right\rangle = \langle p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t} \rangle.$$

Since $E < 0$ we have by an argument similar to case (1)(a)

$$\begin{aligned} [\langle \sqrt{D} \rangle]_+ &= \left[\left\langle \frac{x + \sqrt{D}y}{2} \right\rangle \right]_+ \\ &= \prod_{i=1}^r [P_i]_+^{2k_i - a_i} \prod_{j=1}^s [Q_j]_+^{b_j} \\ &= \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}, \end{aligned}$$

for some $k_i \in \{0, 1, \dots, a_i\}$. Hence

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w},$$

for all $w = 1, \dots, m$. Therefore there exists $\underline{k} = (k_1, \dots, k_r) \in \mathcal{K}$, so $\mathcal{K} \neq \emptyset$.

case (2)(a) :

There is no prime p dividing E such that $\left(\frac{D}{p}\right) = +1$. Therefore we have $E = (\text{sgn} E) q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t}$. Moreover $E > 0$ or $E < 0$ and $H^+(K) = H(K)$.

($\Leftarrow$): In $H^+(K)$ we have

$$\prod_{w=1}^m H_w^{\sum_{j=1}^s b_j V_{H_w}([Q_j]_+)} = [\langle 1 \rangle]_+.$$

Hence there exists $\delta(\underline{k}) \in \mathcal{O}_K$ for each $\underline{k} \in \mathcal{K}$, where $N(\delta(\underline{k})) > 0$, such that

$$\prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \langle \delta(\underline{k}) \rangle.$$

As $\delta(\underline{k}) \in \mathcal{O}_K$ there exist $x(\underline{k}) \in \mathbb{Z}$ and $y(\underline{k}) \in \mathbb{Z}$ such that $\delta(\underline{k}) = \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2}$.

If $E > 0$ taking norms we obtain

$$\begin{aligned} E &= \prod_{j=1}^s q_j^{b_j} \prod_{k=1}^t r_k^{2c_k} = N \left(\prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} \right) = N(\langle \delta(\underline{k}) \rangle) \\ &= |N(\delta(\underline{k}))| = N(\delta(\underline{k})) = \frac{x(\underline{k})^2 - Dy(\underline{k})^2}{4}. \end{aligned}$$

Therefore $x^2 - Dy^2 = 4E$ is solvable.

If $E < 0$ and $H(K) = H^+(K)$ then $N(\eta_1) = -1$ and $\eta_1 \delta(\underline{k}) \in \mathcal{O}_K$, $N(\eta_1 \delta(\underline{k})) < 0$ and $N(\eta_1 \delta(\underline{k})) = E$. Thus by Theorem 1.3 $x^2 - Dy^2 = 4E$ is solvable.

($\Rightarrow$): Let $(x, y) \in \mathbb{Z}^2$ be a solution of $x^2 - Dy^2 = 4E$. Then

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \left\langle \frac{x - y\sqrt{D}}{2} \right\rangle = \langle q_1^{b_1} \dots q_s^{b_s} r_1^{2c_1} \dots r_t^{2c_t} \rangle.$$

By an argument similar to case (1)(a) we obtain

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = Q_1^{r_1} \dots Q_s^{r_s} R_1^{2s_1} \dots R_t^{2s_t}$$

and

$$[\langle 1 \rangle]_+ = [Q_1]_+^{b_1} \dots [Q_s]_+^{b_s} = \prod_{w=1}^m H_w^{\sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}.$$

Hence

$$\sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for all $w = 1, \dots, m$.

case (2)(b): $E < 0$ and $H(K) \neq H^+(K)$.

Let $c_1, \dots, c_m$ be the unique integers in the representation of $[< \sqrt{D} >]_+$ in Theorem 2.4.

($\Leftarrow$): In $H^+(K)$ we have

$$\prod_{w=1}^m H_w^{\sum_{j=1}^s b_j V_{H_w}([Q_j]_+)} = [< \sqrt{D} >]_+.$$

Hence there exists $\delta(\underline{k}) \in \mathcal{O}_K$ for each $\underline{k} \in \mathcal{K}$, where $N(\delta(\underline{k})) < 0$, such that

$$\prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = < \delta(\underline{k}) >.$$

As $\delta(\underline{k}) \in \mathcal{O}_K$ there exist $x(\underline{k}) \in \mathbb{Z}$ and $y(\underline{k}) \in \mathbb{Z}$ such that $\delta(\underline{k}) = \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2}$.

Taking norms we obtain $N(\delta(\underline{k})) = E$ and by Theorem 1.3 we have that $(x(\underline{k}))^2 - D(y(\underline{k}))^2 = 4E$. Therefore $x^2 - Dy^2 = 4E$ is solvable.

($\Rightarrow$): Let $(x, y) \in \mathbb{Z}^2$ be a solution of $x^2 - Dy^2 = 4E$. Then

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \left\langle \frac{x - y\sqrt{D}}{2} \right\rangle = < q_1^{b_1} \dots q_s^{b_s} r_1^{2c_1} \dots r_t^{2c_t} >.$$

By an argument similar to case (1)(b) we have

$$[< \sqrt{D} >]_+ = \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = [Q_1]_+^{b_1} \dots [Q_s]_+^{b_s} = \prod_{w=1}^m H_w^{\sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}.$$

Hence

$$\sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w},$$

for all $w \in \{1, 2, \dots, m\}$. □

2.4 Examples

In this section we use Theorem 2.5 to determine the solvability of some equations of the form $x^2 - Dy^2 = 4E$, where D is a positive discriminant and E is a nonzero integer.

Example 2.1. *We show that the equation $x^2 - 5y^2 = 1100 = 4 \cdot 275$ is solvable. Here $D = 5$ and $E = 275$. To apply Theorem 2.5 we first find the group structure of $H^+(K)$, where $K = \mathbb{Q}(\sqrt{5})$.*

(1) *We show that $H(K)$ is the trivial group. In this case we have $K = \mathbb{Q}(\sqrt{5})$, $d(K) = 5$ and the Minkowski bound $M_K = \sqrt{5}$.*

2 is the only rational prime $\leq M_K$.

As $\left(\frac{5}{2}\right) = -1$, we have that $\langle 2 \rangle$ is a principal ideal. Thus $H(K) = \{\langle 1 \rangle\}$.

(2) *We show that $H^+(K)$ is also trivial. This follows from Theorem 2.2 as $h(K) = 1$ and the fundamental unit $\frac{1+\sqrt{5}}{2}$ of $\mathcal{O}_K$ has norm -1 . Thus, by Theorem 2.2, we have $H^+(K) = \{\langle 1 \rangle_+\}$.*

(3) *Since $H^+(K)$ is the trivial group the congruence of Theorem 2.5 (case (1)(a)) is trivially solvable and thus the equation $x^2 - 5y^2 = 1100$ is solvable. One solution is*

$x = 40$ and $y = 10$.

Example 2.2. We show that the equation $x^2 - 33y^2 = -744 = -4 \cdot 186$ is solvable.

Here $D = 33$ and $E = -186$. To apply Theorem 2.5 we first find the group structure of $H^+(K)$, where $K = \mathbb{Q}(\sqrt{33})$.

(1) We show that $H(K)$ is trivial. Here $d(K) = 33$ and the Minkowski bound $M_K = \sqrt{33}$. The rational primes $p \leq M_K$ are 2, 3 and 5. As

$$\left(\frac{33}{2}\right) = +1, \quad \left(\frac{33}{3}\right) = 0, \quad \left(\frac{33}{5}\right) = -1,$$

we have

$$\langle 2 \rangle = P_1 P_2, \quad \langle 3 \rangle = Q^2 \text{ and } \langle 5 \rangle \text{ is prime,}$$

where

$$P_1 = \left\langle 2, \frac{1 + \sqrt{33}}{2} \right\rangle, \quad P_2 = \left\langle 2, \frac{1 - \sqrt{33}}{2} \right\rangle, \quad N(P_1) = N(P_2) = 2,$$

$$Q = \langle 3, \sqrt{33} \rangle, \quad N(Q) = 3,$$

are distinct prime ideals. The ideal P_1 is principal as

$$\begin{aligned} \left\langle 2, \frac{1 + \sqrt{33}}{2} \right\rangle &= \left\langle 2, \frac{5 + \sqrt{33}}{2} \right\rangle \left(\text{as } \frac{5 + \sqrt{33}}{2} = 2 + \frac{1 + \sqrt{33}}{2} \right) \\ &= \left\langle \left(\frac{5 + \sqrt{33}}{2} \right) \left(\frac{5 - \sqrt{33}}{2} \right), \frac{5 + \sqrt{33}}{2} \right\rangle \\ &= \left\langle \frac{5 + \sqrt{33}}{2} \right\rangle \left\langle \frac{5 - \sqrt{33}}{2}, 1 \right\rangle = \left\langle \frac{5 + \sqrt{33}}{2} \right\rangle \langle 1 \rangle \\ &= \left\langle \frac{5 + \sqrt{33}}{2} \right\rangle. \end{aligned}$$

The ideal Q is also principal as

$$\begin{aligned} Q &= \langle 3, \sqrt{33} \rangle = \langle 3, 6 + \sqrt{33} \rangle \quad (\text{as } 6 + \sqrt{33} = 2 \cdot 3 + \sqrt{33}) \\ &= \langle (6 + \sqrt{33})(6 - \sqrt{33}), 6 + \sqrt{33} \rangle = \langle 6 + \sqrt{33} \rangle \langle 6 - \sqrt{33}, 1 \rangle \\ &= \langle 6 + \sqrt{33} \rangle \langle 1 \rangle = \langle 6 + \sqrt{33} \rangle. \end{aligned}$$

Thus $[Q] = [\langle 1 \rangle]$ and $[P_1] = [P_2] = [\langle 1 \rangle]$ since $[P_1][P_2] = [\langle 1 \rangle]$.

Therefore $H(K) = \{[\langle 1 \rangle]\}$.

(2) We show that $H^+(K) \simeq \mathbb{Z}_2$ and find a generator. The fundamental unit of $\mathcal{O}_K$ is $23 + 4\sqrt{33}$ where $N(23 + 4\sqrt{33}) = 1 > 0$. Therefore, by Theorem 2.2, we have $h^+(K) = 2$, $H^+(K) \simeq \mathbb{Z}_2$ and $H^+(K) = \{[\langle 1 \rangle]_+, [\langle \sqrt{33} \rangle]_+\}$. The generator of $H^+(K)$ is $H_1 = [\langle \sqrt{33} \rangle]_+$.

(3) We use Theorem 2.5 to show that $x^2 - 33y^2 = -744$ is solvable. Clearly $|E| = 186 = 2 \cdot 3 \cdot 31$. As $\left(\frac{33}{2}\right) = +1$, $\left(\frac{33}{3}\right) = 0$ and $\left(\frac{33}{31}\right) = +1$, we have $\langle 2 \rangle = PP'$, $\langle 3 \rangle = Q^2$ and $\langle 31 \rangle = RR'$, where the prime ideals P, P', Q, R and R' are given by

$$\begin{aligned} P &= \left\langle 2, \frac{1 + \sqrt{33}}{2} \right\rangle, \quad P' = \left\langle 2, \frac{1 - \sqrt{33}}{2} \right\rangle, \quad Q = \langle 3, \sqrt{33} \rangle, \\ R &= \left\langle 31, \frac{8 + \sqrt{33}}{2} \right\rangle \quad \text{and} \quad R' = \left\langle 31, \frac{8 - \sqrt{33}}{2} \right\rangle. \end{aligned}$$

The norms of these ideals are $N(P) = N(P') = 2$, $N(Q) = N(Q') = 3$ and $N(R) = N(R') = 31$. As $H(K)$ is trivial we know that P, Q and R are principal ideals. We

determine generators of these ideals. From part (2) we have

$$P = \left\langle \frac{5 + \sqrt{33}}{2} \right\rangle \text{ and } Q = \langle 6 + \sqrt{33} \rangle .$$

We observe that

$$8 + \sqrt{33} \in R \left(\text{as } 8 + \sqrt{33} = (1)(31) + \left(\frac{7 - 3\sqrt{33}}{2} \right) \left(\frac{1 + \sqrt{33}}{2} \right) \right) .$$

Therefore there exists an integral ideal B of $\mathcal{O}_K$ such that

$$\langle 8 + \sqrt{33} \rangle = \left\langle 31, \frac{1 + \sqrt{33}}{2} \right\rangle B .$$

Taking norms we deduce

$$31 = N(\langle 8 + \sqrt{33} \rangle) = N\left(\left\langle 31, \frac{1 + \sqrt{33}}{2} \right\rangle\right) N(B) = 31N(B) .$$

$$\text{Thus } N(B) = 1 \text{ and } \langle 8 + \sqrt{33} \rangle = \left\langle 31, \frac{1 + \sqrt{33}}{2} \right\rangle .$$

The norms of these generators are

$$N\left(\frac{5 + \sqrt{33}}{2}\right) = -2 , \quad N(6 + \sqrt{33}) = 3 \text{ and } N(8 + \sqrt{33}) = 31 .$$

Therefore we have $P \approx \langle \sqrt{33} \rangle$, $Q \approx \langle 1 \rangle$ and $R \approx \langle 1 \rangle$. Thus

$$[\langle P \rangle]_+ = H_1^1 , \quad [\langle Q \rangle]_+ = H_1^0 \text{ and } [\langle R \rangle]_+ = H_1^0 .$$

Since $H(K) \neq H^+(K)$ the congruence of Theorem 2.5 (case (1)(b)) is

$$2k_1 + 2k_2 + 1 \equiv 1 \pmod{2} , \quad k_1, k_2 \in \{0, 1\} .$$

This congruence has the solution $k_1 = k_2 = 0$. Therefore the equation $x^2 - 33y^2 = -744$ is solvable. With the help of a computer we find that $x = 9$ and $y = 5$ is a solution.

Example 2.3. We show that the equation $x^2 - 105y^2 = 31096 = 4 \cdot 7774$ is solvable.

Here $D = 105$ and $E = 7774$. To apply Theorem 2.5 we first find the group structure of $H^+(K)$, where $K = \mathbb{Q}(\sqrt{105})$.

(1) We show that $H(K) \simeq \mathbb{Z}_2$.

In this case we have $d(K) = 105$ and $M_K = \sqrt{105}$. The rational primes $p \leq M_K$ are 2, 3, 5 and 7. As $\left(\frac{105}{2}\right) = +1$, $\left(\frac{105}{3}\right) = 0$, $\left(\frac{105}{5}\right) = 0$ and $\left(\frac{105}{7}\right) = 0$, we have the prime ideal factorizations

$$\langle 2 \rangle = P_1 P_2, \quad \langle 3 \rangle = Q^2, \quad \langle 5 \rangle = R^2 \quad \text{and} \quad \langle 7 \rangle = S^2,$$

where

$$\begin{aligned} P_1 &= \left\langle 2, \frac{1 + \sqrt{105}}{2} \right\rangle, \quad P_2 = \left\langle 2, \frac{1 - \sqrt{105}}{2} \right\rangle, \\ Q &= \langle 3, \sqrt{105} \rangle, \quad R = \langle 5, \sqrt{105} \rangle, \\ S &= \langle 7, \sqrt{105} \rangle, \end{aligned}$$

are distinct prime ideals. The norms of these ideals are $N(P_1) = N(P_2) = 2$, $N(Q) = 3$, $N(R) = 5$, $N(S) = 7$. The prime ideal R is principal as

$$\begin{aligned} \langle 5, \sqrt{105} \rangle &= \langle 5, 10 - \sqrt{105} \rangle \quad \left(\text{as } 10 - \sqrt{105} = 2 \cdot 5 - \sqrt{105} \right) \\ &= \langle 10 - \sqrt{105} \rangle \quad \left(\text{as } 10 - \sqrt{105} \mid 5 \right). \end{aligned}$$

Thus $[R] = [1]$.

Moreover we have

$$\frac{9 + \sqrt{105}}{2} \in P_1 \quad \left(\text{as } \frac{9 + \sqrt{105}}{2} = 2 \cdot 2 + \left(\frac{1 + \sqrt{105}}{2} \right) \right),$$

$$\begin{aligned}
\frac{9 + \sqrt{105}}{2} &\in Q \left(as \frac{9 + \sqrt{105}}{2} = 3 \left(\frac{-67 + \sqrt{105}}{2} \right) + \sqrt{105} (-1 + \sqrt{105}) \right), \\
\frac{9 - \sqrt{105}}{2} &\in P_2 \left(as \frac{9 - \sqrt{105}}{2} = 2 \cdot 2 + \left(\frac{1 - \sqrt{105}}{2} \right) \right), \\
\frac{9 - \sqrt{105}}{2} &\in Q \left(as \frac{9 + \sqrt{105}}{2} = 3 \left(\frac{-67 + \sqrt{105}}{2} \right) + \sqrt{105} (-2 + \sqrt{105}) \right), \\
21 + 2\sqrt{105} &\in Q \left(as \ 21 + 2\sqrt{105} = 7 \cdot 3 + 2\sqrt{105} \right), \\
21 + 2\sqrt{105} &\in S \left(as \ 21 + 2\sqrt{105} = 3 \cdot 7 + 2\sqrt{105} \right).
\end{aligned}$$

Since P_1, P_2, Q and S are distinct prime ideals there exist integral ideals B_1, B_2 and B_3

of $\mathcal{O}_K$ such that

$$\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle = P_1 Q B_1, \quad \left\langle \frac{9 - \sqrt{105}}{2} \right\rangle = P_2 Q B_2 \text{ and } \langle 21 + 2\sqrt{105} \rangle = Q S B_3.$$

Taking norms we obtain

$$\begin{aligned}
6 &= N \left(\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle \right) = N(P_1) N(Q) N(B_1) = 6 \cdot N(B_1), \\
6 &= N \left(\left\langle \frac{9 - \sqrt{105}}{2} \right\rangle \right) = N(P_2) N(Q) N(B_2) = 6 \cdot N(B_2), \\
21 &= N \left(\langle 21 + 2\sqrt{105} \rangle \right) = N(Q) N(S) N(B_3) = 21 \cdot N(B_3),
\end{aligned}$$

so that $N(B_1) = N(B_2) = N(B_3) = 1$. Hence $B_1 = B_2 = B_3 = \langle 1 \rangle$ and

$$P_1 Q = \left\langle \frac{9 + \sqrt{105}}{2} \right\rangle, \quad P_2 Q = \left\langle \frac{9 - \sqrt{105}}{2} \right\rangle \text{ and } QS = \langle 21 + 2\sqrt{105} \rangle.$$

Thus

$$[P_1][P_2] = [P_1 P_2] = [\langle 2 \rangle] = [\langle 1 \rangle].$$

$$[Q]^2 = [Q^2] = [< 3 >] = [< 1 >].$$

$$[S]^2 = [S^2] = [< 7 >] = [< 1 >].$$

$$[P_1][Q] = [P_1Q] = \left[\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle \right] = [< 1 >].$$

$$[P_2][Q] = [P_2Q] = \left[\left\langle \frac{9 - \sqrt{105}}{2} \right\rangle \right] = [< 1 >].$$

$$[Q][S] = [QS] = \left[\left\langle 21 + \sqrt{105} \right\rangle \right] = [< 1 >].$$

We deduce that $[P_1] = [P_2] = [Q] = [S]$. Thus there are at most two elements in $H(K)$. We now show that $[< Q >] \neq [< 1 >]$. Suppose that $Q = < 3, \sqrt{105} >$ is principal, say $Q = \left\langle \frac{x + y\sqrt{105}}{2} \right\rangle$, where $x, y \in \mathbb{Z}$ and $x \equiv y \pmod{2}$. Then

$$3 = N(< 3, \sqrt{105} >) = N \left(\left\langle \frac{x + y\sqrt{105}}{2} \right\rangle \right) = \left| \frac{x^2 - 105y^2}{4} \right|,$$

so that $x^2 - 105y^2 = \pm 12$. Taking this equation modulo 5 we obtain $x^2 \equiv 2$ or $3 \pmod{5}$, which is a contradiction. Therefore we have $H(K) = \{ [< 1 >], [< P_1 >] \}$ so $H(K) \simeq \mathbb{Z}_2$.

(2) We show that $H^+(K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and find generators of $H^+(K)$. The fundamental unit of $\mathcal{O}_K$ is $41 + 4\sqrt{105}$ and $N(41 + 4\sqrt{105}) = +1$. Therefore, by Theorem 2.2, we have that

$$H^+(K) = \{ [< 1 >]_+, [< \sqrt{105} >]_+, [P_1]_+, [< \sqrt{105} > P_1]_+ \}.$$

As $P_1^2 = \left\langle \frac{11 + \sqrt{105}}{2} \right\rangle \in [1]_+$, $[P_1]_+^2 = [1]_+$ and $H(K)^+ \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. We fix once and for all $H_1 = [< \sqrt{105} >]_+$ and $H_2 = [P_1]_+$.

(3) We apply Theorem 2.5 to show that the equation is solvable.

$7774 = 2 \cdot 13^2 \cdot 23$. As $\left(\frac{105}{2}\right) = \left(\frac{105}{13}\right) = \left(\frac{105}{23}\right) = +1$, we have

$\langle 2 \rangle = A_1 A'_1$, $\langle 3 \rangle = A_2 A'_2$ and $\langle 23 \rangle = A_3 A'_3$, where the prime ideals

$A_1, A'_1, A_2, A'_2, A_3$ and A'_3 are given by

$$A_1 = \left\langle 2, \frac{1 + \sqrt{105}}{2} \right\rangle, A'_1 = \left\langle \frac{1 - \sqrt{105}}{2} \right\rangle, A_2 = \left\langle 13, \frac{1 + \sqrt{105}}{2} \right\rangle, A'_2 = \left\langle 13, \frac{1 - \sqrt{105}}{2} \right\rangle$$

$$A_3 = \left\langle 23, \frac{1 + \sqrt{105}}{2} \right\rangle \text{ and } A'_3 = \left\langle 23, \frac{1 - \sqrt{105}}{2} \right\rangle.$$

The norms of these ideals are

$$N(A_1) = N(A'_1) = 2, N(A_2) = N(A'_2) = 13, N(A_3) = N(A'_3) = 23.$$

Since $A_1 = P_1$ we have $A_1 \approx P_1$. Thus $[\langle A_1 \rangle]_+ = H_1^0 H_2^1$. We have

$$\frac{1 + \sqrt{105}}{2} \in A_2, \left(as \frac{1 + \sqrt{105}}{2} = 13 \cdot 0 + 1 \cdot \left(\frac{1 + \sqrt{105}}{2} \right) \right)$$

$$\frac{1 + \sqrt{105}}{2} \in P_1, \left(as \frac{1 + \sqrt{105}}{2} = 2 \cdot 0 + 1 \cdot \left(\frac{1 + \sqrt{105}}{2} \right) \right)$$

$$\frac{17 + \sqrt{105}}{2} \in A_3, \left(as = 23 \cdot \left(\frac{-145 - \sqrt{105}}{2} \right) + \left(\frac{1 + \sqrt{105}}{2} \right) \cdot \left(\frac{-16 + 64\sqrt{105}}{2} \right) \right)$$

$$\frac{17 + \sqrt{105}}{2} \in P_1, \left(as \frac{17 + \sqrt{105}}{2} = 2 \cdot 4 + \frac{1 + \sqrt{105}}{2} \right).$$

Since P_1, A_2, A_3 are distinct primes then there exist integral ideals C_1, C_2 of $\mathcal{O}_K$ such

that

$$\left\langle \frac{1 + \sqrt{105}}{2} \right\rangle = P_1 A_2 C_1 \text{ and } \left\langle \frac{17 + \sqrt{105}}{2} \right\rangle = P_1 A_3 C_2.$$

Taking norms we obtain

$$26 = N \left(\left\langle \frac{1 + \sqrt{105}}{2} \right\rangle \right) = N(P_1)N(A_2)N(C_1) = 26N(C_1)$$

and

$$46 = N \left(\left\langle \frac{17 + \sqrt{105}}{2} \right\rangle \right) = N(P_1)N(A_3)N(C_2) = 46N(C_2)$$

so that $N(C_1) = N(C_2) = 1$. Hence $C_1 = C_2 = \langle 1 \rangle$. Thus

$$\begin{aligned} \left\langle \frac{1 + \sqrt{105}}{2} \right\rangle &= P_1 A_2 \text{ and } \left\langle \frac{17 + \sqrt{105}}{2} \right\rangle = P_1 A_3, \\ N \left(\frac{1 + \sqrt{105}}{2} \right) &= -26 \text{ and } N \left(\frac{17 + \sqrt{105}}{2} \right) = 46. \end{aligned}$$

Therefore

$$\left\langle \frac{1 + \sqrt{105}}{2} \right\rangle \approx \langle \sqrt{105} \rangle \text{ and } \left\langle \frac{17 + \sqrt{105}}{2} \right\rangle \approx \langle 1 \rangle.$$

Hence

$$[P_1]_+ [A_2]_+ = [P_1 A_2]_+ = \left[\left\langle \frac{1 + \sqrt{105}}{2} \right\rangle \right]_+ = [\langle \sqrt{105} \rangle]_+$$

and

$$[P_1]_+ [A_3]_+ = [P_1 A_3]_+ = \left[\left\langle \frac{17 + \sqrt{105}}{2} \right\rangle \right]_+ = [\langle 1 \rangle]_+,$$

which imply that

$$[A_2]_+ = [P_1]_+^{-1} [\langle \sqrt{105} \rangle]_+ = [P_1] [\langle \sqrt{105} \rangle]_+ = H_1^1 H_2^1$$

and

$$[A_3]_+ = [P_1]_+^{-1} = [P_1]_+ = H_1^0 H_2^1.$$

By applying Theorem 2.5 (case (1)(a)) we obtain the following two congruences

$$2k_2 - 2 \equiv 0 \pmod{2},$$

$$2k_1 + 2k_2 + 2k_3 - 4 \equiv 0 \pmod{2}.$$

A solution is $(k_1, k_2, k_3) = (0, 0, 0)$. Therefore Theorem 2.5 shows that the equation $x^2 - 105y^2 = 31096$ is solvable. For example $x = 179$ and $y = 3$ is a solution.

Example 2.4. We show that the equation $x^2 - 145y^2 = -480 = -4 \cdot 120$ is solvable.

Here $D = 145$ and $E = -120$. In this case we have $d(K) = 145$ and $M_K = \sqrt{145}$.

(1) We find a generator of $H(K)$.

The rational primes $p \leq M_K$ are 2, 3, 5, 7 and 11. As $\left(\frac{145}{2}\right) = +1$, $\left(\frac{145}{3}\right) = +1$, $\left(\frac{145}{5}\right) = 0$, $\left(\frac{145}{7}\right) = -1$ and $\left(\frac{145}{11}\right) = -1$, we have

$\langle 2 \rangle = P_1 P_2$, $\langle 3 \rangle = Q_1 Q_2$, $\langle 5 \rangle = R^2$, $\langle 7 \rangle$ and $\langle 11 \rangle$ are principal,

where

$$\begin{aligned} P_1 &= \left\langle 2, \frac{1 + \sqrt{145}}{2} \right\rangle, \quad P_2 = \left\langle 2, \frac{1 - \sqrt{145}}{2} \right\rangle, \\ Q_1 &= \left\langle 3, \frac{1 + \sqrt{145}}{2} \right\rangle, \quad Q_2 = \left\langle 3, \frac{1 - \sqrt{145}}{2} \right\rangle, \\ R &= \langle 5, \sqrt{145} \rangle, \end{aligned}$$

are distinct prime ideals. The norms of these ideals are $N(P_1) = N(P_2) = 2$, $N(Q_1) = N(Q_2) = 3$ and $N(R) = 5$. Moreover we have

$$\begin{aligned} \frac{11 + \sqrt{145}}{2} &\in P_2 \left(as \frac{11 + \sqrt{145}}{2} = 2 \cdot 3 - \left(\frac{1 - \sqrt{145}}{2} \right) \right), \\ \frac{11 + \sqrt{145}}{2} &\in Q_2 \left(as \frac{11 + \sqrt{145}}{2} = 3 \cdot 2 - \left(\frac{1 - \sqrt{145}}{2} \right) \right), \\ \frac{11 - \sqrt{145}}{2} &\in P_1 \left(as \frac{11 - \sqrt{145}}{2} = 3 \cdot 2 - \left(\frac{1 + \sqrt{145}}{2} \right) \right), \\ \frac{11 - \sqrt{145}}{2} &\in Q_1 \left(as \frac{11 - \sqrt{145}}{2} = 2 \cdot 3 - \left(\frac{1 + \sqrt{145}}{2} \right) \right), \\ \frac{15 + \sqrt{145}}{2} &\in P_2 \left(as \frac{15 + \sqrt{145}}{2} = 4 \cdot 2 - \left(\frac{1 - \sqrt{145}}{2} \right) \right), \\ \frac{15 + \sqrt{145}}{2} &\in R \left(as \frac{15 + \sqrt{145}}{2} = \left(\frac{3 + \sqrt{145}}{2} \right) \cdot 5 - 2 \left(\sqrt{145} \right) \right). \end{aligned}$$

Since P_1, P_2, Q_1, Q_2 and R are distinct prime ideals there exist integral ideals B_1, B_2 and B_3 of $\mathcal{O}_K$ such that

$$\left\langle \frac{11 - \sqrt{145}}{2} \right\rangle = P_1 Q_1 B_1, \quad \left\langle \frac{11 + \sqrt{145}}{2} \right\rangle = P_2 Q_2 B_2, \quad \left\langle \frac{15 + \sqrt{145}}{2} \right\rangle = P_2 R B_3.$$

Taking norms we obtain

$$\begin{aligned} 6 &= N \left(\left\langle \frac{11 - \sqrt{145}}{2} \right\rangle \right) = N(P_1) N(Q_1) N(B_1) = 6 \cdot N(B_1), \\ 6 &= N \left(\left\langle \frac{11 + \sqrt{145}}{2} \right\rangle \right) = N(P_2) N(Q_2) N(B_2) = 6 \cdot N(B_2), \\ 20 &= N \left(\left\langle \frac{15 + \sqrt{145}}{2} \right\rangle \right) = N(P_2) N(R) N(B_3) = 10 \cdot N(B_3), \end{aligned}$$

so that $N(B_1) = N(B_2) = 1$ and $N(B_3) = 2$. Hence $B_1 = B_2 = \langle 1 \rangle$ and $B_3 = P_1$ or P_2 .

If $B_3 = P_1$ then $\left\langle \frac{15 + \sqrt{145}}{2} \right\rangle = P_1 P_2 R = \langle 2 \rangle R$. This implies that $\langle 2 \rangle \mid \left\langle \frac{15 + \sqrt{145}}{2} \right\rangle$, which is impossible. Hence $B_3 = P_2$ and $\left\langle \frac{15 + \sqrt{145}}{2} \right\rangle = P_2^2 R$. Thus

$$[P_1][Q_1] = [\langle 1 \rangle], [P_2][Q_2] = [\langle 1 \rangle], [P_2]^2[R] = [\langle 1 \rangle].$$

Since $[P_1][P_2] = [\langle 1 \rangle]$, $[P_2][Q_2] = [\langle 1 \rangle]$ and $[R]^2 = [\langle 1 \rangle]$, we deduce that $[P_1] = [Q_2]$, $[P_2] = [Q_1]$ and $[P_2]^2 = [R]$. Moreover $[P_2]^4 = [R]^2 = [\langle 1 \rangle] = [P_1][P_2]$, which implies that $[P_1] = [P_2]^3$. Thus $[\langle 1 \rangle], [P_2], [P_2]^2, [P_2]^3$ comprise all the ideal classes. From the tables of [20] we have that $h(K) = 4$. Hence we have $H(K) = \{[\langle 1 \rangle], [P_2], [P_2]^2, [P_2]^3\}$.

(2) We show that $H^+(K) \simeq \mathbb{Z}_4$ and find a generator of $H^+(K)$. The fundamental unit of $\mathcal{O}_K$ is $578 + 48\sqrt{145}$ and $N(578 + 48\sqrt{145}) = -1$. Therefore, by Theorem 2.2, we have $H^+(K) = \{[\langle 1 \rangle]_+, [P_2]_+, [P_2]_+^2, [P_2]_+^3\}$ and $H^+(K) \simeq \mathbb{Z}_4$. We choose the generator H_1 of $H^+(K)$ to be $H_1 = [P_2]$.

(3) We apply Theorem 2.5 to show that the equation $x^2 - 145y^2 = -480$ is solvable.

Here $|E| = 120 = 2^3 \cdot 3 \cdot 5$. As $\left(\frac{145}{2}\right) = \left(\frac{145}{3}\right) = +1$ and $\left(\frac{145}{5}\right) = 0$, we have

$\langle 2 \rangle = PP'$, $\langle 3 \rangle = QQ'$ and $\langle 5 \rangle = R'^2$, where the prime ideals P, P', Q, Q' and R' are given by

$$P = \left\langle 2, \frac{1 + \sqrt{145}}{2} \right\rangle, P' = \left\langle 2, \frac{1 - \sqrt{145}}{2} \right\rangle,$$

$$Q = \left\langle 3, \frac{1 + \sqrt{145}}{2} \right\rangle, Q' = \left\langle 3, \frac{1 - \sqrt{145}}{2} \right\rangle.$$

$$R' = \langle 5, \sqrt{145} \rangle.$$

The norms of these ideals are

$$N(P) = N(P') = 2, \quad N(Q) = N(Q') = 3 \text{ and } N(R') = 5.$$

We have

$$\begin{aligned} [P]_+ &= \left[\left\langle 2, \frac{1 + \sqrt{145}}{2} \right\rangle \right]_+ = [P_2]_+^3, \\ [Q]_+ &= \left[\left\langle 3, \frac{1 + \sqrt{145}}{2} \right\rangle \right]_+ = [Q_1]_+ = [P_2]_+, \\ [R']_+ &= [\langle 5, \sqrt{145} \rangle]_+ = [R]_+ = [P_2]_+^2. \end{aligned}$$

By Theorem 2.5 (case (1)(a)) the equation is solvable if and only if the congruence

$$(2k_1 - 3)(3) + (2k_2 - 1)(1) + 2 \equiv 0 \pmod{4},$$

is solvable for $k_1 \in \{0, 1, 2, 3\}$ and $k_2 \in \{0, 1\}$. Clearly $(k_1, k_2) = (0, 0)$ is a solution of this congruence. Therefore the equation $x^2 - 145y^2 = -480$ is solvable. For example $x = 10$ and $y = 2$ is a solution.

Example 2.5. We show that the equation $x^2 - 105y^2 = -864 = -4 \cdot 216$ is solvable.

Here $D = 105$, $E = -216$ and $K = \mathbb{Q}(\sqrt{105})$.

(1) We know that $H(K) \simeq \mathbb{Z}_2$. (from Example 2.3)

(2) $H^+(K) = \{[\langle 1 \rangle]_+, [\langle \sqrt{105} \rangle]_+, [P_1]_+, [\sqrt{105}P_1]_+\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

We pick generators $H_1 = [\langle \sqrt{105} \rangle]_+$ and $H_2 = [P_1]_+$.

(3) We apply Theorem 2.5 to show that $x^2 - 105y^2 = -864$ is solvable.

Clearly $|E| = 216 = 2^3 \cdot 3^3$. As $\left(\frac{105}{2}\right) = +1$ and $\left(\frac{105}{3}\right) = 0$, we have

$\langle 2 \rangle = A_1 A'_1$ and $\langle 3 \rangle = A_2^2$, where the distinct prime ideals A_1, A'_1

and A_2 are given by

$$A_1 = \left\langle 2, \frac{1 + \sqrt{105}}{2} \right\rangle, A'_1 = \left\langle 2, \frac{1 - \sqrt{105}}{2} \right\rangle, A_2 = \langle 3, \sqrt{105} \rangle.$$

The norms of these ideals are

$$N(A_1) = N(A'_1) = 2, N(A_2) = 3.$$

Since $A_1 = P_1$ we have $A_1 \approx P_1$ and $[A_1]_+ = H_1^0 H_2^1$. Further

$$\begin{aligned} \frac{9 + \sqrt{105}}{2} &\in Q \left(\text{as } \frac{9 + \sqrt{105}}{2} = 3 \left(\frac{3 + \sqrt{105}}{2} \right) - 1(\sqrt{105}) \right), \\ \frac{9 + \sqrt{105}}{2} &\in P_1 \left(\text{as } \frac{9 + \sqrt{105}}{2} = 2 \cdot 2 + \frac{1 + \sqrt{105}}{2} \right). \end{aligned}$$

Therefore there exists an integral ideal B of $\mathcal{O}_K$ such that $\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle = P_1 Q B$.

Taking norms we obtain

$$6 = N \left(\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle \right) = N(P_1) N(Q) N(B) = 6N(B).$$

Hence $N(B) = 1$ and $B = \mathcal{O}_K$. Therefore $\left\langle \frac{9 + \sqrt{105}}{2} \right\rangle = P_1 Q$. As $N \left(\frac{9 + \sqrt{105}}{2} \right) = -6$ thus $[P_1]_+ [Q]_+ = [\langle \sqrt{105} \rangle]_+$. Hence $[Q]_+ = [P_1]_+^{-1} [\langle \sqrt{105} \rangle]_+ = [P_1]_+ [\langle \sqrt{105} \rangle]_+ =$

H_1H_2 . In this case the two congruences of Theorem 2.5 (case (1)(b)) are

$$(2k_1 - 3)(0) + 3(1) \equiv 1 \pmod{2},$$

$$(2k_1 - 3)(1) + 3(1) \equiv 0 \pmod{2},$$

which always hold. Therefore, by Theorem 2.5, the equation $x^2 - 105y^2 = -864$ is solvable. One solution is $x = 9$ and $y = 3$.

Example 2.6. We show that the equation $2x^2 - 219y^2 = -1$ is insolvable. Clearly this equation is solvable if and only if the equation $x^2 - 1752y^2 = -8$ is solvable. In Example 1.5 we have shown that the congruence equation $2x^2 - 219y^2 \equiv -1 \pmod{m}$ is solvable for all positive integers $m > 1$. Thus we cannot use congruences to deduce that $2x^2 - 219y^2 = -1$ is insolvable.

We use Theorem 2.5 on the equation $x^2 - 1752y^2 = -8$ to deduce that $2x^2 - 219y^2 = -1$ is insolvable. Here $D = 1752$, $E = -2$, $K = \mathbb{Q}(\sqrt{438})$ and $M_K = \sqrt{1752} \approx 41.86$. By [20] we have $h(K) = 4$. The rational primes $p \leq M_K$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 and 41. As

$$\begin{aligned} \left(\frac{1752}{2}\right) &= 0, \left(\frac{1752}{3}\right) = 0, \left(\frac{1752}{5}\right) = -1, \left(\frac{1752}{7}\right) = 1 \\ \left(\frac{1752}{11}\right) &= 1, \left(\frac{1752}{13}\right) = 1, \left(\frac{1752}{17}\right) = 1, \left(\frac{1752}{19}\right) = 1 \\ \left(\frac{1752}{23}\right) &= 1, \left(\frac{1752}{29}\right) = -1, \left(\frac{1752}{31}\right) = 1, \left(\frac{1752}{37}\right) = -1 \\ \left(\frac{1752}{41}\right) &= -1, \end{aligned}$$

we have

$$\langle 2 \rangle = P_2^2, \langle 3 \rangle = P_3^2, \langle 5 \rangle \text{ is prime}, \langle 7 \rangle = P_7 P_7',$$

$$\langle 11 \rangle = P_{11} P_{11}', \langle 13 \rangle = P_{13} P_{13}', \langle 17 \rangle = P_{17} P_{17}', \langle 19 \rangle = P_{19} P_{19}',$$

$$\langle 23 \rangle = P_{23} P_{23}', \langle 29 \rangle \text{ is prime}, \langle 31 \rangle = P_{31} P_{31}', \langle 37 \rangle \text{ is prime},$$

$$\text{and } \langle 41 \rangle \text{ is prime},$$

where

$$P_2 = \langle 2, \sqrt{438} \rangle, P_3 = \langle 3, \sqrt{438} \rangle, P_7 = \langle 7, 2 + \sqrt{438} \rangle,$$

$$P_7' = \langle 7, 2 - \sqrt{438} \rangle, P_{11} = \langle 11, 3 + \sqrt{438} \rangle, P_{11}' = \langle 11, 3 - \sqrt{438} \rangle,$$

$$P_{13} = \langle 13, 3 + \sqrt{438} \rangle, P_{13}' = \langle 13, 3 - \sqrt{438} \rangle, P_{17} = \langle 17, 8 + \sqrt{438} \rangle,$$

$$P_{17}' = \langle 17, 8 - \sqrt{438} \rangle, P_{19} = \langle 19, 1 + \sqrt{438} \rangle, P_{19}' = \langle 19, 1 - \sqrt{438} \rangle,$$

$$P_{23} = \langle 23, 1 + \sqrt{438} \rangle, P_{23}' = \langle 23, 1 - \sqrt{438} \rangle, P_{31} = \langle 31, 2 + \sqrt{438} \rangle$$

$$\text{and } P_{31}' = \langle 31, 2 - \sqrt{438} \rangle.$$

We have

$$83 + 4\sqrt{438} \in P_7' \left(\text{as } 83 + 4\sqrt{438} = 7 \cdot 13 + (-4) \cdot (2 - \sqrt{438}) \right),$$

$$83 + 4\sqrt{438} \in P_{17} \left(\text{as } 83 + 4\sqrt{438} = 3 \cdot 17 + (4) \cdot (8 + \sqrt{438}) \right),$$

$$19 - \sqrt{438} \in P_7 \left(\text{as } 19 - \sqrt{438} = 3 \cdot 7 + (-1) \cdot (2 + \sqrt{438}) \right),$$

$$19 - \sqrt{438} \in P_{11} \left(\text{as } 19 - \sqrt{438} = 2 \cdot 11 + (-1) \cdot (3 + \sqrt{438}) \right),$$

$$\begin{aligned}
125 - 6\sqrt{438} &\in P_{11} \left(\text{as } 125 - 6\sqrt{438} = 11 \cdot 13 + (-6) \cdot (3 + \sqrt{438}) \right), \\
125 - 6\sqrt{438} &\in P_{13} \left(\text{as } 125 - 6\sqrt{438} = 13 \cdot 11 + (-6) \cdot (3 + \sqrt{438}) \right), \\
103 + 5\sqrt{438} &\in P_{11} \left(\text{as } 103 + 5\sqrt{438} = 11 \cdot 8 + 5 \cdot (3 + \sqrt{438}) \right), \\
103 + 5\sqrt{438} &\in P_{31} \left(\text{as } 103 + 5\sqrt{438} = 31 \cdot 3 + 5 \cdot (2 + \sqrt{438}) \right).
\end{aligned}$$

Since P'_7 , P_{17} , P_7 , P_{11} , P_{13} and P_{31} are all distinct ideals there exist integral ideals A_1 , A_2 , A_3 and A_4 of $\mathcal{O}_K$ such that

$$\begin{aligned}
\langle 83 + 4\sqrt{438} \rangle &= P'_7 P_{17} A_1, \quad \langle 19 - \sqrt{438} \rangle = P_7 P_{11} A_2, \\
\langle 125 - 6\sqrt{438} \rangle &= P_{11} P_{13} A_3, \quad \langle 103 + 5\sqrt{438} \rangle = P_{11} P_{31} A_4.
\end{aligned}$$

Taking norms we obtain $N(A_1) = N(A_2) = N(A_3) = N(A_4) = 1$. Thus we have $[P'_7][P_{17}] = [\langle 1 \rangle]$, $[P_7][P_{11}] = [\langle 1 \rangle]$, $[P_{11}][P_{13}] = [\langle 1 \rangle]$ and $[P_{11}][P_{31}] = [\langle 1 \rangle]$. This implies that $[P_7] = [P_{17}]$, $[P_7] = [P_{11}]^{-1}$, $[P_{11}]^{-1} = [P_{13}]$ and $[P_{11}]^{-1} = [P_{31}]$. Therefore we have $[P_7] = [P_{13}] = [P_{17}] = [P_{31}]$. Moreover we have

$$\begin{aligned}
20 + \sqrt{438} &\in P_2 \left(\text{as } 20 + \sqrt{438} = 2 \cdot 10 + 1 \cdot \sqrt{438} \right), \\
20 + \sqrt{438} &\in P_{19} \left(\text{as } 20 + \sqrt{438} = 19 \cdot 1 + 1 \cdot (1 + \sqrt{438}) \right), \\
22 + \sqrt{438} &\in P_2 \left(\text{as } 22 + \sqrt{438} = 2 \cdot 11 + 1 \cdot \sqrt{438} \right), \\
22 + \sqrt{438} &\in P'_{23} \left(\text{as } 22 + \sqrt{438} = 23 \cdot 1 + (-1) \cdot (1 - \sqrt{438}) \right).
\end{aligned}$$

Since P_2 , P_{19} and P'_{23} are distinct ideals there exist integral ideals B_1 and B_2 of $\mathcal{O}_K$

such that

$$\langle 20 + \sqrt{438} \rangle = P_2 P_{19} B_1 \text{ and } \langle 22 + \sqrt{438} \rangle = P_2 P'_{23} B_2.$$

Taking norms we obtain $N(B_1) = N(B_2) = 1$. Thus $[P_2][P_{19}] = [\langle 1 \rangle]$ and $[P_2][P'_{23}] = [\langle 1 \rangle]$. Hence $[P_2] = [P_{19}]^{-1}$ and $[P_2] = [P_{23}]$. As $[P_2] = [P_2]^{-1}$ we have $[P_2] = [P_{19}] = [P_{23}]$.

We have shown that the ideal class of any prime ideal P of $\mathcal{O}_K$ dividing a rational prime $p \leq M_K$ is equal to one of $[\langle 1 \rangle]$, $[P_2]$, $[P_7]$ and $[P_{11}]$. As $h(K) = 4$ we must have that they are all distinct, otherwise $1 \leq h(K) < 4$, a contradiction. Thus $[P_2] \neq [\langle 1 \rangle]$. This implies that $[P_2]_+ \neq [\sqrt{1752}]_+$.

By Theorem 2.5 (case (2)(b)) we have that $x^2 - 1752y^2 = -8$ is insolvable.

Example 2.7. We show that the equation $x^2 - 60y^2 = 37044 = 4 \cdot 9261$ is solvable.

Here $D = 60$ and $E = 9261$. Thus $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{60}) = \mathbb{Q}(\sqrt{15})$.

(1) We show that $H(\mathbb{Q}(\sqrt{15})) \simeq \mathbb{Z}_2$.

Here we have $K = \mathbb{Q}(\sqrt{15})$, $d(K) = 60$ and $M_K = \sqrt{60}$.

The rational primes $p \leq M_K$ are 2, 3, 5 and 7.

As $\left(\frac{60}{2}\right) = 0$, $\left(\frac{60}{3}\right) = 0$, $\left(\frac{60}{5}\right) = 0$, and $\left(\frac{60}{7}\right) = +1$, we have the prime ideal factorizations

$$\langle 2 \rangle = P^2, \langle 3 \rangle = Q^2, \langle 5 \rangle = R^2, \langle 7 \rangle = \langle 7, 1 + \sqrt{15} \rangle \langle 7, 1 - \sqrt{15} \rangle = SS'.$$

The norms of these ideals are $N(P) = 2$, $N(Q) = 3$, $N(R) = 5$ and $N(S) = N(S') =$

7. Moreover we have

$$5 + \sqrt{15} \in P \left(\text{as } 5 + \sqrt{15} = 2 \cdot 2 + 1 \cdot (1 + \sqrt{15}) \right),$$

$$5 + \sqrt{15} \in R \left(\text{as } 5 + \sqrt{15} = 2 \cdot 0 + 1 \cdot (5 + \sqrt{15}) \right),$$

$$6 + \sqrt{15} \in Q \left(\text{as } 6 + \sqrt{15} = 2 \cdot 3 + 1 \cdot (\sqrt{15}) \right),$$

$$6 + \sqrt{15} \in S' \left(\text{as } 6 + \sqrt{15} = 7 \cdot 1 - 1 \cdot (1 - \sqrt{15}) \right),$$

$$1 + \sqrt{15} \in P \left(\text{as } 1 + \sqrt{15} = 2 \cdot 0 + 1 \cdot (1 + \sqrt{15}) \right),$$

$$1 + \sqrt{15} \in S \left(\text{as } 1 + \sqrt{15} = 7 \cdot 0 + 1 \cdot (1 + \sqrt{15}) \right),$$

$$3 + \sqrt{15} \in P \left(\text{as } 3 + \sqrt{15} = 2 \cdot 1 + 1 \cdot (1 + \sqrt{15}) \right),$$

$$3 + \sqrt{15} \in Q \left(\text{as } 3 + \sqrt{15} = 3 \cdot 1 + 1 \cdot (\sqrt{15}) \right).$$

Therefore we have

$$[P][R] = [\langle 1 \rangle], [Q][S'] = [\langle 1 \rangle],$$

$$[P][S] = [\langle 1 \rangle], [P][Q] = [\langle 1 \rangle].$$

Hence we have $[P] = [Q] = [R] = [S]$. Suppose that P is principal. Then there exists $x + y\sqrt{15} \in \mathcal{O}_K$ such that $P = \langle x + y\sqrt{15} \rangle$. Hence $2 = N(P) = N(\langle x + y\sqrt{15} \rangle) = |x^2 - 15y^2|$ so that $x^2 - 15y^2 = \pm 2$. If the $+$ sign holds then $x^2 \equiv 2 \pmod{3}$ a contradiction. If the $-$ sign holds then $x^2 \equiv -2 \pmod{5}$, a contradiction. Hence P is not principal. Thus $H(K) = \{[\langle 1 \rangle], [\langle 2, 1 + \sqrt{15} \rangle]\} \simeq \mathbb{Z}_2$.

(2) We show that $H^+(K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and find its generators. The fundamental unit

of $\mathcal{O}_K$ is $4 + \sqrt{15}$ and $N(4 + \sqrt{15}) = +1$. Therefore, by Theorem 2.2, we have that $H^+(K) = \{[< 1 >]_+, [\langle \sqrt{15} \rangle]_+, [P]_+, [\sqrt{15}P]_+\}$. As $[P]_+^2 = [P^2]_+ = [\langle 2 \rangle]_+ = [1]_+$ we have $H^+(K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. We fix once and for all the generators $H_1 = [\langle \sqrt{15} \rangle]_+$ and $H_2 = [P]_+$ of $H^+(K)$.

(3) We apply Theorem 2.5 to show that the equation is solvable. We have $9261 = 3^3 \cdot 7^3$. As $\left(\frac{60}{3}\right) = 0$ and $\left(\frac{60}{7}\right) = +1$, we have $< 3 > = \langle 3, \sqrt{15} \rangle^2 = Q^2$ and $< 7 > = \langle 7, 1 + \sqrt{15} \rangle \langle 7, 1 - \sqrt{15} \rangle = SS'$. Thus

$$[Q]_+ = H_1^0 H_2^1 \text{ and } [S]_+ = H_1^0 H_2^1.$$

The two congruences of Theorem 2.5 (case (1)(a)) are

$$(2k_1 - 3)(0) + 3(0) \equiv 0 \pmod{2},$$

$$(2k_1 - 3)(1) + 3(1) \equiv 0 \pmod{2},$$

where $k_1 \in \{0, 1, 2, 3\}$. These congruences are trivially true. Therefore Theorem 2.5 shows that the equation is solvable. One solution is $x = 198$ and $y = 6$.

Chapter 3

Number of classes of solutions of $x^2 - Dy^2 = 4E$

In this section we state and prove using algebraic number theory the main theorem of this thesis (Theorem 3.1). Given D a positive discriminant and E a nonzero integer, Theorem 3.1 gives us the value of $N(D, E)$. We recall that $N(D, E)$ is equal to the number of classes of solutions of the equation $x^2 - Dy^2 = 4E$. Bounds for $N(D, E)$ have been given by Stolt [25], [26] using elementary methods.

3.1 Main theorem

Theorem 3.1. *Let D be a positive discriminant of a real quadratic field K . Let E be a nonzero integer. We suppose that the equation $x^2 - Dy^2 = 4E$ is solvable.*

Let $p_1, \dots, p_r$ be the primes dividing E such that $\left(\frac{D}{p_i}\right) = +1$.

Let $q_1, \dots, q_s$ be the primes dividing E such that $\left(\frac{D}{q_j}\right) = 0$.

Let $r_1, \dots, r_k$ be the primes dividing E such that $\left(\frac{D}{r_i}\right) = -1$.

Each prime r_i divides E to an even power, otherwise the equation is insolvable.

We have

$$E = (\text{sgn } E) p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t},$$

where $a_1, \dots, a_r, b_1, \dots, b_s, c_1, \dots, c_t$ are positive integers.

In $\mathcal{O}_K$ we have

$\langle p_i \rangle = P_i P'_i$, $i = 1, 2, \dots, r$, where P_i and P'_i are distinct conjugate prime ideals with $N(P_i) = N(P'_i) = p_i$,

$\langle q_j \rangle = Q_j^2$, $j = 1, \dots, s$, where Q_j is a self-conjugate prime ideal with $N(Q_j) = q_j$,

and

$\langle r_k \rangle = R_k$, $k = 1, \dots, t$, where R_k is a self-conjugate prime ideal with $N(R_k) = r_k^2$.

Let $H_1, \dots, H_m$ be a fixed set of generators of $H^+(K)$ with $\text{ord}(H_i) = h_i$, where $i = 1, 2, \dots, m$, and

$$1 < h_1 \mid \cdots \mid h_m, \quad h_1 \cdots h_m = h^+(K).$$

(1) If there is at least one prime p_i dividing E such that $\left(\frac{D}{p_i}\right) = +1$, $E > 0$ or $E < 0$ and $H^+(K) = H(K)$, then $N(D, E)$ is the number of $(k_1, \dots, k_r) \in \mathbb{Z}^r$, where $k_i = \{0, 1, \dots, a_i\}$, $i = 1, \dots, r$, such that

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w}$$

for all $w = 1, \dots, m$.

(2) If there is at least one prime p_i dividing E such that $\left(\frac{D}{p_i}\right) = +1$, $E < 0$ and

$H^+(K) \neq H(K)$, then $N(D, E)$ is equal to the number of $(k_1, \dots, k_r) \in \mathbb{Z}^r$, where $k_i \in \{0, 1, \dots, a_i\}$, $i = 1, \dots, r$, such that

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w}$$

for all $w = 1, \dots, m$, where $c_1, \dots, c_w$ are the unique integers in the representation of $[\langle \sqrt{D} \rangle]_+$ in Theorem 2.4.

(3) If there is no prime p_i dividing E such that $\left(\frac{D}{p_i}\right) = +1$, then

$$N(D, E) = 1.$$

Proof:

case (1): Here $r \geq 1$. Let $\mathcal{K} =$ the set of $\underline{k} = (k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $k_i \in \{0, 1, \dots, a_i\}$ ($i = 1, \dots, r$) and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for all $w \in \{1, \dots, m\}$. From the proof of Theorem 2.5 we have that for $\underline{k} \in \mathcal{K}$ there exists $(x(\underline{k}), y(\underline{k})) \in \mathbb{Z}^2$ such that $(x(\underline{k}), y(\underline{k}))$ is a solution of $x^2 - Dy^2 = 4E$. We recall that $Q(D, E)$ is the set of all equivalence classes of the equation $x^2 - Dy^2 = 4E$.

Suppose first that $E > 0$. We define the mapping

$$\lambda : \mathcal{K} \mapsto Q(D, E)$$

by

$$\lambda(\underline{k}) = [(x(\underline{k}), y(\underline{k}))].$$

We show that λ is injective. Suppose $\lambda(\underline{k}) = \lambda(\underline{l})$ for $\underline{k}, \underline{l} \in \mathcal{K}$. Then $[(x(\underline{k}), y(\underline{k}))] = [(x(\underline{l}), y(\underline{l}))]$. Hence there exists a unit η of $\mathcal{O}_K$ with $N(\eta) = 1$ such that

$$\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} = \eta \left(\frac{x(\underline{l}) + y(\underline{l})\sqrt{D}}{2} \right).$$

Thus

$$\left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle = \left\langle \frac{x(\underline{l}) + y(\underline{l})\sqrt{D}}{2} \right\rangle$$

so

$$\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \prod_{i=1}^r P_i^{l_i} P_i'^{a_i - l_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k}$$

and, by the uniqueness of the factorization of a nonzero ideal of $\mathcal{O}_K$ into prime ideals, we obtain $k_i = l_i$, $i = 1, 2, \dots, r$, so that $\underline{k} = \underline{l}$. Hence λ is injective. Now we show that λ is surjective. Let $[(x, y)]$ be a class in $Q(D, E)$ so that (x, y) is a solution of $x^2 - Dy^2 = 4E$. Then

$$\frac{x + y\sqrt{D}}{2} \cdot \frac{x - y\sqrt{D}}{2} = \frac{x^2 - Dy^2}{4} = E = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_t^{2c_t}.$$

This gives the prime ideal decomposition in $\mathcal{O}_K$

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = \prod_{i=1}^r P_i^{k_i} P_i'^{l_i} \prod_{j=1}^s Q_j^{m_j} \prod_{k=1}^t R_k^{n_k}$$

for some

$$k_i \in \{0, 1, \dots, a_i\}, i = 1, 2, \dots, r,$$

$$l_i \in \{0, 1, \dots, a_i\}, i = 1, 2, \dots, r,$$

$$m_j \in \{0, 1, \dots, 2b_j\}, j = 1, 2, \dots, s,$$

$$n_k \in \{0, 1, \dots, 2c_k\}, k = 1, 2, \dots, t.$$

Taking conjugates we obtain

$$\left\langle \frac{x - y\sqrt{D}}{2} \right\rangle = \prod_{i=1}^r P_i'^{k_i} P_i^{l_i} \prod_{j=1}^s Q_j^{m_j} \prod_{k=1}^t R_k^{n_k}.$$

Thus

$$\begin{aligned} \left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \left\langle \frac{x - y\sqrt{D}}{2} \right\rangle &= \prod_{i=1}^r P_i^{k_i+l_i} P_i'^{k_i+l_i} \prod_{j=1}^s Q_j^{2m_j} \prod_{k=1}^t R_k^{2n_k} \\ &= \prod_{i=1}^r P_i^{a_i} P_i'^{a_i} \prod_{j=1}^s Q_j^{2b_j} \prod_{k=1}^t R_k^{2c_k} \end{aligned}$$

so that

$$k_i + l_i = a_i, \quad i = 1, 2, \dots, r,$$

$$2m_j = 2b_j, \quad j = 1, 2, \dots, s,$$

$$2n_k = 2c_k, \quad k = 1, 2, \dots, t.$$

Hence

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = \prod_{i=1}^r P_i^{k_i} P_i'^{a_i-k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k}.$$

Thus in $H^+(K)$ we have

$$[< 1 >]_+ = \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = \prod_{i=1}^r [P_i]_+^{k_i} [P_i']_+^{a_i-k_i} \prod_{j=1}^s [Q_j]_+^{b_j} \prod_{k=1}^t [R_k]_+^{c_k}$$

$$\begin{aligned}
 &= \prod_{i=1}^r [P_i]_+^{2k_i - a_i} \prod_{j=1}^s [Q_j]_+^{b_j} \\
 &= \prod_{i=1}^r \left(\prod_{w=1}^m H_w^{V_{H_w}([P_i]_+)} \right)^{2k_i - a_i} \prod_{j=1}^s \left(\prod_{w=1}^m H_w^{V_{H_w}([Q_j]_+)} \right)^{b_j} \\
 &= \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}
 \end{aligned}$$

and so we have

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for $w = 1, 2, \dots, m$. Let $\underline{k} = (k_1, \dots, k_r)$. Clearly $\underline{k} \in \mathcal{K}$. Also $\lambda(\underline{k}) = [(x(\underline{k}), y(\underline{k}))]$,

where

$$\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle.$$

But

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = \prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k}.$$

Thus

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = \left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle$$

so

$$\frac{x + y\sqrt{D}}{2} = \theta \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right),$$

where θ is a unit of $\mathcal{O}_K$. Now

$$N \left(\frac{x + y\sqrt{D}}{2} \right) = N \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right) = E > 0.$$

Thus $N(\theta) = 1$. Therefore (x, y) and $(x(\underline{k}), y(\underline{k}))$ are strictly associated solutions. Hence $[(x, y)] = [(x(\underline{k}), y(\underline{k}))]$. Thus $\lambda(\underline{k}) = [(x, y)]$ and so λ is surjective. Therefore λ is bijective and $N(D, E) = |Q(D, E)| = |\mathcal{K}|$ as asserted.

If $E < 0$ and $H^+(K) = H(K)$ then we define the same mapping $\lambda : \mathcal{K} \mapsto Q(D, E)$.

The injectivity of λ follows in the same way as when $E > 0$. If (x, y) is a solution of $x^2 - Dy^2 = 4E$ then by an argument similar to the case when $E > 0$ we obtain

$$[< 1 >]_+ = \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i)V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}$$

for some $\underline{k} = (k_1, \dots, k_r) \in \mathbb{Z}^r$, where $k_i \in \{0, 1, \dots, a_i\}$. Therefore

$$\sum_{i=1}^r (2k_i - a_i)V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w},$$

for $w = 1, 2, \dots, m$. Also $\lambda(\underline{k}) = [x(\underline{k}), y(\underline{k})]$, where

$$\prod_{i=1}^r P_i^{k_i} P_i'^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle.$$

Thus

$$\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle = \left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle$$

so we have

$$\frac{x + y\sqrt{D}}{2} = \theta \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right),$$

where θ is a unit of $\mathcal{O}_K$. Now

$$N \left(\frac{x + y\sqrt{D}}{2} \right) = N \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right) < 0.$$

Thus $N(\theta) = 1$. Therefore (x, y) and $(x(\underline{k}), y(\underline{k}))$ are strictly associated solutions. Hence $[(x, y)] = [(x(\underline{k}), y(\underline{k}))]$. Thus $\lambda(\underline{k}) = [(x, y)]$ and so λ is surjective. Therefore λ is bijective and $N(D, E) = |Q(D, E)| = |\mathcal{K}|$.

case (2): Here $r \geq 1$. Let $c_1, \dots, c_m$ be the unique integers in the representation of $[\sqrt{D}]_+$ in Theorem 2.4. Let

$\mathcal{K}$ = the set of $k = (k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $k_i \in \{0, 1, \dots, a_i\}$ ($i = 1, \dots, r$) and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w},$$

for all $w \in \{1, \dots, m\}$. We define the mapping

$$\lambda : \mathcal{K} \mapsto Q(D, E)$$

by

$$\lambda(\underline{k}) = [(x(\underline{k}), y(\underline{k}))],$$

where $x(\underline{k}), y(\underline{k})$ are defined in the proof of case (1)(b) of Theorem 2.5. λ is injective for the same reasons as in case (1). To show that λ is surjective we note first that for a solution (x, y) of the equation $x^2 - Dy^2 = 4E$, we have $N\left(\frac{x + y\sqrt{D}}{2}\right) < 0$.

Hence

$$[\langle \sqrt{D} \rangle]_+ = \left[\left\langle \frac{x + y\sqrt{D}}{2} \right\rangle \right]_+ = \prod_{w=1}^m H_w^{\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+)}$$

for some $k_i \in \{0, 1, \dots, a_i\}$. Thus

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w},$$

for $w = 1, 2, \dots, m$. Also $\lambda(\underline{k}) = [(x(\underline{k}), y(\underline{k}))]$, where

$$\prod_{i=1}^r P_i^{k_i} P_i^{a_i - k_i} \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \left\langle \frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right\rangle.$$

Thus

$$\frac{x + y\sqrt{D}}{2} = \theta \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right),$$

where θ is a unit of $\mathcal{O}_K$. Now

$$N \left(\frac{x + y\sqrt{D}}{2} \right) = N \left(\frac{x(\underline{k}) + y(\underline{k})\sqrt{D}}{2} \right) < 0.$$

Thus $N(\theta) = 1$. Therefore (x, y) and $(x(\underline{k}), y(\underline{k}))$ are strictly associated solutions.

Hence $[(x, y)] = [(x(\underline{k}), y(\underline{k}))]$. Thus $\lambda(\underline{k}) = [(x, y)]$ and so λ is surjective. Therefore λ

is bijective and $N(D, E) = |Q(D, E)| = |\mathcal{K}|$ as asserted.

case (3) :

Let (x_1, y_1) and (x_2, y_2) be two solutions of $x^2 - Dy^2 = 4E$, where there are no primes

p_i such that $p_i \mid E$ and $\left(\frac{D}{p_i}\right) = +1$. We have

$$\left\langle \frac{x_1 + y_1\sqrt{D}}{2} \right\rangle = \prod_{j=1}^s Q_j^{b_j} \prod_{k=1}^t R_k^{c_k} = \left\langle \frac{x_2 + y_2\sqrt{D}}{2} \right\rangle.$$

Hence

$$\frac{x_1 + y_1\sqrt{D}}{2} = \theta \left(\frac{x_2 + y_2\sqrt{D}}{2} \right),$$

where θ is a unit of $\mathcal{O}_K$. Now

$$N \left(\frac{x_1 + y_1\sqrt{D}}{2} \right) = N \left(\frac{x_2 + y_2\sqrt{D}}{2} \right).$$

Hence we have $N(\theta) = 1$. This implies that $[(x_1, y_1)] = [(x_2, y_2)]$. Therefore we have $N(D, E) = 1$. $\square$

We can easily deduce the following result from Theorem 3.1.

Theorem 3.2. *Let $N(D, E)$ be the number of classes of solutions of the equation $x^2 - Dy^2 = 4E$, where D is a positive discriminant and E is a nonzero integer. Let $r_1, \dots, r_t$ be the primes dividing E such that $\left(\frac{D}{p_i}\right) = -1$. Then*

(1) *If there is a prime r_i that does not divide E to an even power we have that $N(D, E) = 0$.*

(2) *If all the primes r_i divide E to an even power we have*

$$N(D, E) = N\left(D, \frac{E}{r_1^{2c_1} \dots r_t^{2c_t}}\right),$$

where $r_i^{2c_i} \parallel E$, $i \in \{1, \dots, t\}$.

Proof: Case (1) follows from Theorem 2.4 and Case (2) can obviously be deduced from Theorem 3.1 as $N(D, E)$ is independent of the primes r_i , $i \in \{1, \dots, t\}$. $\square$

3.2 Examples

In this section we use Theorem 3.1 to determine the number $N(D, E)$ of classes of solutions of some equations of the form $x^2 - Dy^2 = 4E$, where D is a positive discriminant and E is a nonzero integer.

Example 3.1. (*Example 2.1 revisited*)

We show that $N(5, 275) = 2$. From Example 2.1 we have the congruence

$$(2k_1 - 1)0 + 2(0) \equiv 0 \pmod{1},$$

where $k_1 \in \{0, 1\}$. This congruence is satisfied for both $k_1 = 0$ and $k_1 = 1$. Therefore by Theorem 3.1 we have that $N(5, 275) = 2$. Computation shows that the two classes of solutions are $[(35, 5)]$ and $[(35, -5)]$.

Example 3.2. (Example 2.2 revisited)

We show that $N(33, -186) = 4$. From Example 2.2 we obtain the congruence

$$2k_1 + 2k_2 + 1 \equiv 1 \pmod{2},$$

where $k_1, k_2 \in \{0, 1\}$. This congruence holds for $(k_1, k_2) = (0, 0), (0, 1), (1, 0)$ and $(1, 1)$. Therefore Theorem 3.1 implies that $N(33, -186) = 4$. A simple computation shows that the four classes of solutions are $[(\pm 9, 5)], [(\pm 57, 11)]$.

Example 3.3. (Example 2.3 revisited)

We show that $N(105, 7774) = 12$. From Example 2.3 we obtain the following two congruences

$$2k_2 - 2 \equiv 0 \pmod{2},$$

$$2k_1 + 2k_2 + 2k_3 - 4 \equiv 0 \pmod{2},$$

where $k_1 \in \{0, 1\}$, $k_2 \in \{0, 1, 2\}$, $k_3 \in \{0, 1\}$. The two congruences are solvable for every triple (k_1, k_2, k_3) . Therefore Theorem 3.1 implies that $N(105, 7774) = 2 \times 3 \times 2 =$

12. Computation shows that the 12 classes of solutions are

$[(\pm 179, 3)]$, $[(\pm 199, 9)]$, $[(\pm 221, 13)]$, $[(\pm 311, 25)]$, $[(\pm 571, 53)]$ and $[(\pm 689, 65)]$.

Example 3.4. (Example 2.4 revisited)

We show that $N(145, -120) = 4$. From Example 2.4 we obtain the following two congruences

$$3 \equiv 1 \pmod{2},$$

$$2k_1 \equiv 0 \pmod{2},$$

where $k_1 \in \{0, 1, 2, 3\}$. The two congruences hold for every k_1 . Therefore Theorem 3.1 implies that $N(145, -120) = 4$. Computation shows that the four classes of solutions are $[(\pm 10, 2)]$ and $[(\pm 155, 13)]$.

Example 3.5. (Example 2.5 revisited)

We show that $N(105, -216) = 4$. From Example 2.5 we obtain the following two congruences

$$3 \equiv 1 \pmod{2},$$

$$2k_1 \equiv 0 \pmod{2},$$

where $k_1 \in \{0, 1, 2, 3\}$. The two congruences hold for every k_1 . Therefore Theorem 3.1 shows that $N(105, -216) = 4$. Computation shows that the four classes of solutions are $[(\pm 9, 3)]$ and $[(\pm 54, 6)]$.

Example 3.6. (*Example 2.7 revisited*)

We show that $N(60, 9261) = 4$. From Example 2.7 we obtain the following congruences

$$0 \equiv 0 \pmod{2},$$

$$2k_1 \equiv 0 \pmod{2},$$

where $k_1 \in \{0, 1, 2, 3\}$. The two congruences hold trivially for all k_1 . Therefore Theorem 3.1 shows that $N(60, 9261) = 4$. Computation shows that the four classes of solutions are

$$[(198, 6)], [(-198, 6)], [(252, 21)], [(-252, 21)].$$

Chapter 4

Special cases of Theorems 2.5 and 3.1

Theorem 2.5 gives us a necessary and sufficient condition for the solvability of the equation $x^2 - Dy^2 = 4E$, where D is a positive discriminant and E is a nonzero integer, in integers x and y . In this chapter we first show that the solvability of this equation can be used to determine the solvability of equations of the form $x^2 - Fy^2 = G$ and $2x^2 - Fy^2 = G$. We then use Theorem 3.1 to give sufficient conditions to determine the value of $N(D, E)$ for some particular values of E .

4.1 Solvability of $x^2 - Fy^2 = G$ and $2x^2 - Fy^2 = G$

The solvability of the equations $x^2 - Fy^2 = G$ and $2x^2 - Fy^2 = G$, where F is a positive squarefree integer which is not a discriminant (so that $F \equiv 2$ or $3 \pmod{4}$), and G is nonzero integer, is closely related to the solvability of the equation $x^2 - Dy^2 = 4E$, where D is a positive discriminant and E is a nonzero integer, as we show in the following simple theorem.

Theorem 4.1. *Let F be a positive squarefree integer and G be a nonzero integer.*

- (1) *If $F \equiv 2$ or $3 \pmod{4}$ the equation $x^2 - Fy^2 = G$ is solvable in integers if and only if the equation $x^2 - 4Fy^2 = 4G$ is solvable in integers.*
- (2) *If $F \equiv 3 \pmod{4}$ the equation $2x^2 - Fy^2 = G$ is solvable in integers if and only if the equation $x^2 - 8Fy^2 = 8G$ is solvable in integers.*

Proof:

case (1) :

($\implies$.) Let $(u, v) \in \mathbb{Z}^2$ be a solution of $x^2 - Fy^2 = G$. Then $u^2 - Fv^2 = G$ and $4(u^2 - Fv^2) = (2u)^2 - 4Fv^2 = 4G$. Therefore the equation $x^2 - 4Fy^2 = 4G$ is solvable with $(x, y) = (2u, v)$.

($\impliedby$.) Let $(u_1, v_1) \in \mathbb{Z}^2$ be a solution of $x^2 - 4Fy^2 = 4G$. Then $(u_1)^2 - 4F(v_1)^2 = 4G$.

We have $u_1^2 \equiv 0 \pmod{4}$. This implies that $u_1 \equiv 0 \pmod{2}$. Let $u_1 = 2u_2$, where $u_2 \in \mathbb{Z}$. Then $(2u_2)^2 - 4Fv_1^2 = 4G$, that is $u_2^2 - Fv_1^2 = G$. Therefore the equation $x^2 - Fy^2 = G$ is solvable with $(x, y) = (u_2, v_1)$.

case (2) :

($\implies$.) Let $(u, v) \in \mathbb{Z}^2$ be a solution of $2x^2 - Fy^2 = G$. Then $2u^2 - Fv^2 = G$ and $8(2u^2 - Fv^2) = (4u)^2 - 8Fv^2 = 8G$. Therefore the equation $x^2 - 8Fy^2 = 8G$ is solvable with $(x, y) = (4u, v)$.

($\impliedby$.) Let $(u_1, v_1) \in \mathbb{Z}^2$ be a solution of $x^2 - 8Fy^2 = 8G$. Then $(u_1)^2 - 8F(v_1)^2 = 8G$.

We have $u_1^2 \equiv 0 \pmod{8}$. This implies that $u_1 \equiv 0 \pmod{4}$. Let $u_1 = 4u_2$, where

$u_2 \in \mathbb{Z}$. Then $(4u_2)^2 - 8Fv_1^2 = 8G$, that is $2u_2^2 - Fv_1^2 = G$. Therefore the equation $2x^2 - Fy^2 = G$ is solvable with $(x, y) = (u_2, v_1)$. $\square$

We emphasize that $4F$ in case (1) and $8F$ in case (2) are discriminants of real quadratic fields.

4.2 Special case when $H^+(K) \simeq \mathbb{Z}_2^s$

In this section we show that it is very easy to determine the solvability of the equation $x^2 - Dy^2 = 4E$ and the value of $N(D, E)$ when $H^+(K) \simeq \mathbb{Z}_2^s$. We first treat the case $s = 0$, that is when $H^+(K)$ is trivial.

Theorem 4.2. *Let D be a positive discriminant of a real quadratic field. Let $K = \mathbb{Q}(\sqrt{D})$ and let E be a nonzero integer.*

Let $p_1, \dots, p_r$ be the primes dividing E such that $\left(\frac{D}{p_i}\right) = +1$.

Let $q_1, \dots, q_s$ be the primes dividing E such that $\left(\frac{D}{q_j}\right) = 0$.

Let $r_1, \dots, r_k$ be the primes dividing E such that $\left(\frac{D}{r_i}\right) = -1$.

If $H^+(K) \simeq \{e\}$ then we have :

(1) *The equation $x^2 - Dy^2 = 4E$ is solvable $\iff$ each prime r_i divides E to an even power.*

(2) *If $x^2 - Dy^2 = 4E$ is solvable and there exists at least one prime p_i dividing E then $N(D, E) = (a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$, where $a_i = V_{p_i}(E)$ ($1 \leq i \leq r$).*

(3) *If $x^2 - Dy^2 = 4E$ is solvable and there are no primes p_i dividing E then*

$$N(D, E) = 1.$$

Proof:

case (1) :

($\Rightarrow$;) This follows by applying the converse of Theorem 2.4.

($\Leftarrow$;) Let $E = \pm p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} r_1^{2c_1} \cdots r_k^{2c_k}$, where $0 \leq a_i$, $0 \leq b_j$, $0 \leq c_l$.

By hypothesis we have $H^+(K) = \{[\langle 1 \rangle]_+\}$. Hence $H(K) = \{[\langle 1 \rangle]\}$. By Theorem 2.5

(cases (1)(a) and (2)(a)) we have that the equation $x^2 - Dy^2 = 4E$ is solvable if and

only if there exists $(k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $0 \leq k_i \leq a_i$ and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{1}, \quad (1)$$

if there exist at least one prime p_i dividing E or

$$\sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{1} \quad (2)$$

if there is no prime p_i dividing E . Clearly (1) and (2) hold trivially. This implies

that $x^2 - Dy^2 = 4E$ is solvable .

case (2) :

If the equation $x^2 - Dy^2 = 4E$ is solvable we can see that (1) is true for all $(k_1, \dots, k_r) \in$

$\mathbb{Z}^r$ such that $0 \leq k_i \leq a_i$. By Theorem 3.1 we deduce that $N(D, E) = (a_1 + 1) \cdots (a_r +$

1). This proves case (2).

case (3) :

This follows from Theorem 3.1 (3). $\square$

We now treat the case $H^+(K) \simeq \mathbb{Z}_2^s$, $s \geq 1$.

Theorem 4.3. *Let D be the discriminant of a real quadratic field K so that $K = \mathbb{Q}(\sqrt{D})$. Let E be a nonzero integer. Let $p_1, \dots, p_r$ be the primes dividing E such that $\left(\frac{D}{p_i}\right) = 1$. For $i = 1, 2, \dots, r$ let a_i be the integer such that $p_i^{a_i} \parallel E$.*

If $H^+(K) \simeq \mathbb{Z}_2^s$, $s \geq 1$, and $x^2 - Dy^2 = 4E$ is solvable then

$$(1) \ N(D, E) = (a_1 + 1) \cdots (a_r + 1), \text{ if } r \geq 1,$$

$$(2) \ N(D, E) = 1, \text{ if } r = 0.$$

Proof:

case (1) : $r \geq 1$

Let $H_1, \dots, H_m$ be the m generators of $H^+(K)$. We assume that $x^2 - Dy^2 = 4E$ is solvable. Suppose $E > 0$ or $E < 0$ and $H(K) = H^+(K)$. By Theorem 2.5 there exist $(k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $0 \leq k_i \leq a_i$ and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{h_w}, \quad (3)$$

where $w = 1, \dots, m$ and $h_w = 2$. The congruences (3) can be rewritten as

$$-\sum_{i=1}^r a_i V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv 0 \pmod{2},$$

for all $w = 1, \dots, m$. As these congruences are independent of $(k_1, \dots, k_r)$ we have

$N(D, E) =$ number of $(k_1, \dots, k_r) \in \mathbb{Z}^r$ with $0 \leq k_i \leq a_i$ ($i = 1, \dots, r$) so that

$$N(D, E) = (a_1 + 1) \cdots (a_r + 1).$$

If $E < 0$ and $H(K) \neq H^+(K)$ then by Theorem 2.5 there exist $(k_1, \dots, k_r) \in \mathbb{Z}^r$ such that $0 \leq k_i \leq a_i$ and

$$\sum_{i=1}^r (2k_i - a_i) V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{h_w}, \quad (4)$$

where $w = 1, \dots, m$, $c_1, \dots, c_m$ are the unique integers of the representation of $[\sqrt{D}]_+$ and $h_w = 2$ for all $w \in \{1, \dots, m\}$. The congruences (4) can be rewritten as

$$-\sum_{i=1}^r a_i V_{H_w}([P_i]_+) + \sum_{j=1}^s b_j V_{H_w}([Q_j]_+) \equiv c_w \pmod{2},$$

where $w = 1, 2, \dots, m$. As above we have $N(D, E) = (a_1 + 1) \cdots (a_r + 1)$.

case 2: $r = 0$

This follows in a similar manner from Theorem 3.1. □

4.3 Special case when E is equal to a prime power

In this section we determine the solvability and the number of classes of solutions of the equation $x^2 - Dy^2 = 4E$, when E is a prime power. In this special case we show that $N(D, E)$ depends on the order of the ideal class of a prime ideal in the group $H(K)$ or $H^+(K)$.

Theorem 4.4. *Consider the equation $x^2 - Dy^2 = 4E$, where D is the discriminant of a real quadratic field. Let $K = \mathbb{Q}(\sqrt{D})$. Let $E = \pm p^a$, where $a \in \mathbb{N}$ and p is a*

prime such that $\left(\frac{D}{p}\right) = 1$. Let P be a prime ideal in $\mathcal{O}_K$ such that $\langle p \rangle = PP'$. Let $m_+ =$ the order of $[P]_+$ in $H^+(K)$. Then, if $E > 0$ or $E < 0$ and $H(K) = H^+(K)$, we have

$$N(D, E) = \begin{cases} a + 1, & \text{if } m_+ = 1, \\ 2 \left\lfloor \frac{a}{m_+} \right\rfloor + 1, & \text{if } a \equiv 0 \pmod{2} \text{ and } m_+ \equiv 0 \pmod{2}, \\ 2 \left(\left\lfloor \frac{a}{m_+} \right\rfloor - \left\lfloor \frac{a}{2m_+} \right\rfloor \right), & \text{if } a \equiv 1 \pmod{2}, m_+ \equiv 1 \pmod{2} \text{ and } 3 \leq m_+ \leq a, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Let $H_1, \dots, H_m$ be the fixed set of generators of $H^+(K)$ as defined in Theorem 3.1. Then we have

$$[P]_+ = H_1^{x_1} \cdots H_m^{x_m}, \text{ where } x_i \in \{0, 1, \dots, h_i - 1\}, i = 1, 2, \dots, m.$$

Hence

$$m_+ = \text{ord}_{H^+(K)}[P]_+ = \text{lcm} \left(\frac{h_1}{(h_1, x_1)}, \dots, \frac{h_m}{(h_m, x_m)} \right).$$

As $E > 0$ or $E < 0$ and $H(K) = H^+(K)$, by Theorem 3.1 we have

$$N(D, E) = \text{card}\{k \mid k \in \{0, 1, 2, \dots, a\}, (2k - a)x_w \equiv 0 \pmod{h_w}, w = 1, 2, \dots, m\}.$$

Next we show that for any $k \in \{0, 1, \dots, a\}$, we have

$$(2k - a)x_w \equiv 0 \pmod{h_w} \text{ for all } w = 1, 2, \dots, m, \text{ if and only if } 2k - a \equiv 0 \pmod{m_+}.$$

($\implies$) :

If $(2k - a)x_w \equiv 0 \pmod{h_w}$ for all $w \in \{0, 1, \dots, a\}$, then

$$(2k - a) \frac{x_w}{(x_w, h_w)} \equiv 0 \pmod{\frac{h_w}{(x_w, h_w)}},$$

for all $w \in \{0, 1, \dots, a\}$. As $\left(\frac{h_w}{(x_w, h_w)}, \frac{x_w}{(h_w, x_w)}\right) = 1$, we have

$$2k - a \equiv 0 \pmod{\frac{h_w}{(x_w, h_w)}},$$

for all $w = 1, \dots, m$. Therefore $2k - a \equiv 0 \pmod{m_+}$.

($\impliedby$) :

$$2k - a \equiv 0 \pmod{m_+} \implies 2k - a \equiv 0 \pmod{\frac{h_w}{(x_w, h_w)}} \text{ for all } w = 1, \dots, m.$$

This implies that there exists $b_w \in \mathbb{Z}$ for all $w = 1, \dots, m$, such that

$$\frac{h_w}{(x_w, h_w)} b_w = 2k - a.$$

If $x_w \geq 1$, for $w \in \{1, \dots, m\}$, we have

$$h_w \frac{x_w}{(x_w, h_w)} b_w = \frac{h_w}{(x_w, h_w)} x_w b_w = (2k - a)x_w.$$

This implies that $h_w \mid (2k - a)x_w$. Thus $(2k - a)x_w \equiv 0 \pmod{h_w}$.

If $x_w = 0$, where $w \in \{1, 2, \dots, m\}$, we have $(2k - a)0 = 0 \equiv 0 \pmod{h_w}$.

Hence, for $w \in \{1, \dots, m\}$, we have

$$(2k - a)x_w \equiv 0 \pmod{h_w}.$$

From this we can deduce that

$$N(D, E) = \text{card}\{k \mid k \in \{0, 1, \dots, a\}, 2k - a \equiv 0 \pmod{m_+}\}.$$

If $m_+ = 1$ then $N(D, E) = a + 1$.

If $m_+ \equiv 0 \pmod{2}$ and $a \equiv 0 \pmod{2}$ then

$$\begin{aligned}
 N(D, E) &= \text{card} \left\{ k \mid k \in \{0, 1, 2, \dots, a\}, k \equiv \frac{a}{2} \pmod{\frac{m_+}{2}} \right\} \\
 &= \text{card} \left\{ \lambda \in \mathbb{Z} \mid 0 \leq \frac{a}{2} + \lambda \frac{m_+}{2} \leq a \right\} \\
 &= \text{card} \left\{ \lambda \in \mathbb{Z} \mid -\frac{a}{m_+} \leq \lambda \leq \frac{a}{m_+} \right\} \\
 &= 2 \left[\frac{a}{m_+} \right] + 1.
 \end{aligned}$$

If $m_+ \equiv 0 \pmod{2}$ and $a \equiv 1 \pmod{2}$, then $2k - a \equiv 0 \pmod{m_+}$ is insolvable so that $N(D, E) = 0$.

If $m_+ \geq 3$, $m_+ \equiv 1 \pmod{2}$, $a \equiv 1 \pmod{2}$ and $m_+ > a$, then $N(D, E) = 0$ since in this case we have $0 < |2k - a| \leq a < m_+$. This implies $2k - a \not\equiv 0 \pmod{m_+}$, for all $k \in \{0, 1, \dots, a\}$. Therefore $N(D, E) = 0$.

If $m_+ \geq 3$, $m_+ \equiv 1 \pmod{2}$, $a \equiv 1 \pmod{2}$ and $m_+ \leq a$, we have

$$\begin{aligned}
 N(D, E) &= \text{card} \{ k = 0, 1, \dots, a \mid 2k - a \equiv 0 \pmod{m_+} \} \\
 &= \text{card} \left\{ \lambda \in \mathbb{Z} \mid 0 \leq \frac{m_+ + a}{2} + \lambda m_+ \leq a \right\} \\
 &= \text{card} \left\{ \lambda \in \mathbb{Z} \mid -\frac{(m_+ + a)}{2} \leq \lambda m_+ \leq \frac{a - m_+}{2} \right\} \\
 &= \text{card} \left\{ \lambda \in \mathbb{Z} \mid -\frac{a}{2m_+} - \frac{1}{2} \leq \lambda \leq \frac{a}{2m_+} - \frac{1}{2} \right\} \\
 &= \left[\frac{a}{2m_+} - \frac{1}{2} \right] + 1 + \left[\frac{a}{2m_+} + \frac{1}{2} \right] \\
 &= 2 \left(\left[\frac{a}{2m_+} + \frac{1}{2} \right] \right) = 2 \left(\left[\frac{a}{m_+} \right] - \left[\frac{a}{2m_+} \right] \right),
 \end{aligned}$$

as $[x] + \left[x + \frac{1}{2}\right] = [2x]$ for all $x \in \mathbb{R}$. □

Example 4.1. We determine the number of classes of solutions of the equation

$x^2 - 40y^2 = 119164 = 4 \cdot 29791 = 4 \cdot 31^3$. We note that $\left(\frac{40}{31}\right) = +1$ so that we can apply Theorem 4.4. The prime ideal decomposition of $\langle 31 \rangle$ is

$$\langle 31 \rangle = \langle 31, 17 + \sqrt{10} \rangle \langle 31, 17 - \sqrt{10} \rangle = PP', \quad N(P) = N(P') = 31.$$

We observe that $11 - 3\sqrt{10} \in P$, as $11 - 3\sqrt{10} = 31(1 + \sqrt{10}) + (17 + \sqrt{10})(-2\sqrt{10})$.

Hence there exists an integral ideal B such that $PB = \langle 11 - 3\sqrt{10} \rangle$.

Taking norms, we obtain

$$31N(B) = N(P)N(B) = N(PB) = N(\langle 11 - 3\sqrt{10} \rangle) = |11^2 - 10 \cdot 3^2| = 31$$

so that $N(B) = 1$, $B = \langle 1 \rangle$, $P = \langle 11 - 3\sqrt{10} \rangle$. As $N(11 - 3\sqrt{10}) = 31$, we have

$[P]_+ = [\langle 1 \rangle]_+$. Hence $m_+ = 1$. Thus we have $N(40, 29791) = 4$ by Theorem 4.4.

Computation shows that the four classes of solutions are $[(\pm 358, 15)]$ and $[(\pm 682, 93)]$.

Example 4.2. We determine the number of classes of solutions of the equation $x^2 -$

$65y^2 = -116 = -4 \cdot 29$. We first note that the fundamental unit of $K = \mathbb{Q}(\sqrt{65})$

is $8 + \sqrt{65}$ of norm -1 . Thus $H(K) = H^+(K)$ by Theorem 2.2. We have that

$\left(\frac{65}{29}\right) = +1$. Thus we can apply Theorem 4.4. Moreover

$$\langle 29 \rangle = \langle 29, 6 + \sqrt{65} \rangle \langle 29, 6 - \sqrt{65} \rangle = PP'.$$

Clearly $12 + 2\sqrt{65} \in P$ as $12 + 2\sqrt{65} = 29(0) + 2(6 + \sqrt{65})$. Hence there exists an integral ideal B such that $PB = \langle 12 + 2\sqrt{65} \rangle$. Taking norms we obtain $N(B) = 1$. As $N(12 + 2\sqrt{65}) = 29$, we have $[P]_+ = [\langle 1 \rangle]_+$. Hence $m_+ = 1$. Thus we have $N(65, -29) = 2$ by Theorem 4.4. Computation shows that the two classes of solutions are $[(\pm 12, 2)]$.

Theorem 4.5. Consider the equation $x^2 - Dy^2 = 4E$, where D is the discriminant of a real quadratic field. Let $K = \mathbb{Q}(\sqrt{D})$. Let $E = \pm q^b$, where $b \in \mathbb{N}$ and q is a prime such that $\left(\frac{D}{q}\right) = 0$. Let Q be the prime ideal in $\mathcal{O}_K$ such that $\langle q \rangle = Q^2$. Let $m =$ the order of $[Q]$ in $H(K)$ and $m_+ =$ the order of $[Q]_+$ in $H^+(K)$. Then we have the following cases :

(1) If $E > 0$ or $E < 0$ and $H(K) = H^+(K)$ then

$$N(D, E) = \begin{cases} 1, & \text{if } m_+ \mid b, \\ 0, & \text{otherwise.} \end{cases}$$

(2) If $E < 0$, $H(K) \neq H^+(K)$ and either (i) $m = 1$ or (ii) $m = 2$ and $b \equiv 1 \pmod{2}$ then

$$N(D, E) = \begin{cases} 1, & m = 1, m_+ = 2 \text{ and } b \equiv 1 \pmod{2}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Let $H_1, \dots, H_m$ be the fixed set of generators of $H^+(K)$ as defined in Theorem 3.1. We have $[Q]_+ = H_1^{x_1} \dots H_m^{x_m}$, where $x_i \in \{0, 1, \dots, h_i - 1\}$, $i = 1, 2, \dots, m$. Then

$$[\langle 1 \rangle]_+ = [\langle q \rangle]_+ = [Q^2]_+ = [Q]_+^2 = H_1^{2x_1} \dots H_m^{2x_m}$$

so that $m_+ = 1$ or 2 and

$$2x_i \equiv 0 \pmod{h_i}, \quad i = 1, 2, \dots, m.$$

Suppose that $h_1, \dots, h_l$ are odd and $h_{l+1}, \dots, h_m$ are even. Then

$$x_i = \begin{cases} 0, & i = 1, 2, \dots, l, \\ \varepsilon_i \frac{h_i}{2}, & i = l+1, \dots, m, \end{cases}$$

where $\varepsilon_i = 0$ or 1 , $i = l+1, \dots, m$.

case (1) : $E > 0$ or $E < 0$ and $H(K) = H^+(K)$.

$$m_+ = 1 \implies [Q]_+ = [< 1 >]_+$$

$$\implies x_w = 0 \text{ for } w = 1, 2, \dots, m$$

$$\implies bx_w \equiv 0 \pmod{h_w} \text{ for } w = 1, 2, \dots, m$$

$$\implies N(D, E) = 1, \text{ by Theorem 3.1.}$$

$$m_+ = 2, 2 \mid b \implies bx_w \equiv 0 \pmod{h_w} \text{ for } w = 1, 2, \dots, m \text{ as } 2x_w \equiv 0 \pmod{h_w}$$

$$\implies N(D, E) = 1, \text{ by Theorem 3.1.}$$

$$m_+ = 2, 2 \nmid b \implies \text{there exists } s \in \{l+1, \dots, m\} \text{ such that } \varepsilon_s = 1$$

$$\implies \text{there exists } s \in \{l+1, \dots, m\} \text{ such that } x_s = \frac{h_s}{2}$$

$$\implies bx_s \equiv \frac{h_s}{2} \pmod{h_s} \text{ for some } s \in \{l+1, \dots, m\}$$

$$\implies bx_s \not\equiv 0 \pmod{h_s} \text{ for some } s \in \{l+1, \dots, m\}$$

$$\implies N(D, E) = 0, \text{ by Theorem 3.1.}$$

Since $m_+ = 1$ or 2 , we have shown that

$$N(D, E) = \begin{cases} 1, & \text{if } m_+ \mid b, \\ 0, & \text{otherwise.} \end{cases}$$

case (2) : $E < 0$, $H(K) \neq H^+(K)$ and $m = 1$ or $m = 2$ and $b \equiv 1 \pmod{2}$

$$m = 1, m_+ = 2 \text{ and } b \equiv 1 \pmod{2} \implies [Q]_+ = [< \sqrt{D} >]_+$$

$$\implies x_w = c_w \text{ for } w = 1, 2, \dots, m$$

$$\implies bx_w \equiv c_w \pmod{h_w} \text{ for } w = 1, 2, \dots, m.$$

$$\implies N(D, E) = 1, \text{ by Theorem 3.1.}$$

$$m = 1, m_+ = 2 \text{ and } b \equiv 0 \pmod{2} \implies [Q]_+ = [< \sqrt{D} >]_+$$

$$\implies x_w = c_w \text{ for } w = 1, 2, \dots, m$$

$$\implies \text{there exists } s \in \{l+1, \dots, m\} \text{ such that } \varepsilon_s = 1$$

$$\implies \text{there exists } s \in \{l+1, \dots, m\} \text{ such that } x_s = \frac{h_i}{2} = c_s$$

$$\implies bx_s \equiv 0 \not\equiv \frac{h_s}{2} = c_s \pmod{h_s}$$

$$\implies N(D, E) = 0, \text{ by Theorem 3.1.}$$

$$m = 2 \text{ and } b \equiv 1 \pmod{2} \implies [Q]_+ \neq [< \sqrt{D} >]_+$$

$$\implies \text{there exist } s \in \{l+1, \dots, m\} \text{ such that } x_s \neq c_s$$

$$\text{If } x_s = 0, c_s = \frac{h_s}{2} \text{ then } bx_s = 0 \not\equiv \frac{h_s}{2} = c_s \pmod{h_s}$$

$$\text{If } x_s = \frac{h_s}{2}, c_s = 0 \text{ then } bx_s \equiv \frac{h_s}{2} \not\equiv 0 = c_s \pmod{h_s}$$

$$\implies N(D, E) = 0, \text{ by Theorem 3.1.}$$

$$m = 1 \text{ and } m_+ = 1 \implies x_i = 0 \text{ for all } i \in \{1, \dots, m\}$$

By Theorem 2.4 there exist c_j , where $j = 1, 2, \dots, m$, such that $c_j = \frac{h_j}{2}$

$$\implies bx_i = 0 \not\equiv \frac{h_j}{2} \pmod{h_j}$$

$$\implies N(D, E) = 0, \text{ by Theorem 3.1.}$$

Therefore we have shown that if $E < 0$, $H(K) \neq H^+(K)$ and $m = 1$ or $m = 2$ and $b \equiv 1 \pmod{2}$, then we have

$$N(D, E) = \begin{cases} 1, & \text{if } m = 1, m_+ = 2 \text{ and } b \equiv 1 \pmod{2}, \\ 0, & \text{otherwise.} \end{cases}$$

□

Example 4.3. We determine the number of classes of solutions of the equation

$x^2 - 321y^2 = 108 = 4 \cdot 27$. We first note that $27 = 3^3$ and $\left(\frac{321}{3}\right) = 0$. We have

$\langle 3 \rangle = \langle 3, \sqrt{321} \rangle^2 = Q^2$, $N(Q) = 3$. $18 + \sqrt{321} \in Q$, as $18 + \sqrt{321} = 6 \cdot 3 + 1 \cdot \sqrt{321}$.

Hence there exists an integral ideal B such that $QB = \langle 18 + \sqrt{321} \rangle$. Thus

$$3N(B) = N(Q)N(B) = N(QB) = N(\langle 18 + \sqrt{321} \rangle) = |18^2 - 321| = 3$$

so that

$$N(B) = 1, B = \langle 1 \rangle \text{ and } Q = \langle 18 + \sqrt{321} \rangle.$$

As $N(18 + \sqrt{321}) = 3$ is positive this implies that $[Q]_+ = [\langle 1 \rangle]_+$. Hence $m_+ = 1$

divides $b = 3$. Therefore we have $N(321, 27) = 1$ by Theorem 4.5. Computation shows that the unique class of solutions is $[(108, 6)]$.

Example 4.4. We determine the number of classes of solutions of the equation $x^2 - 165y^2 = -44 = -4 \cdot 11$. We first note that the fundamental unit of $\mathbb{Q}(\sqrt{165})$ is $1079 + 84\sqrt{165}$ and $N(1079 + 84\sqrt{165}) = +1$. Thus $H(K) \neq H^+(K)$. We have $\left(\frac{165}{11}\right) = 0$. Further $\langle 11 \rangle = \langle 11, \sqrt{165} \rangle^2 = Q^2$. Also $77 + 6\sqrt{165} \in Q$ (as $77 + 6\sqrt{165} = 7 \cdot 11 + 6 \cdot \sqrt{165}$). Hence there exists an integral ideal B such that $QB = \langle 77 + 6 \cdot \sqrt{321} \rangle$. Taking norms we obtain $N(B) = 1$. This implies that $[Q] = [\langle 1 \rangle]$. Hence $m = 1$. As $N(77 + 6\sqrt{165}) = -11$, we have $[Q]_+ = [\langle \sqrt{D} \rangle]_+$. Therefore $m_+ = 2$. We have $H(K) \neq H^+(K)$, $E < 0$, $m = 1$, $m_+ = 2$ and $b \equiv 1 \pmod{2}$. Therefore $N(165, -11) = 1$ by Theorem 4.5. Computation shows that the unique class of solutions is $[(11, 1)]$.

Theorem 4.6. Consider the equation $x^2 - Dy^2 = 4E$, where D is a positive discriminant. Let $E = \pm r^{2c}$, where $c \in \mathbb{N}$ and r is a prime such that $\left(\frac{D}{r}\right) = -1$. We have

$$N(D, E) = \begin{cases} 1, & \text{if } E > 0 \text{ or } E < 0 \text{ and } H(K) = H^+(K), \\ 0, & \text{if } E < 0 \text{ and } H(K) \neq H^+(K). \end{cases}$$

Proof:

If $E > 0$ then $x^2 - Dy^2 = 4E$ is solvable with $x = 2r^c$, $y = 0$. Thus $N(D, E) = 1$ by Theorem 3.1.

If $E < 0$ then by Theorem 3.2 we have $N(D, -4r^{2c}) = N(D, -4)$.

If $H(K) = H^+(K)$ then $N(\eta_1) = -1$. This implies that $x^2 - Dy^2 = -4$ is solvable.

Thus $N(D, -4r^{2c}) = 1$ by Theorem 3.1.

If $H(K) \neq H^+(K)$ then $N(\eta_1) = +1$. This implies that $x^2 - Dy^2 = -4$ is insolvable.

Thus $N(D, -4r^{2c}) = 0$. □

Example 4.5. We show that the equation $x^2 - 33y^2 = -100 = -4 \cdot 25 = -4 \cdot 5^2$ is insolvable. We first note that $\left(\frac{33}{5}\right) = -1$ and that the power of 5 in E is even. The fundamental unit of $K = \mathbb{Q}(\sqrt{33})$ is $23 + 4\sqrt{33}$ and $N(23 + 4\sqrt{33}) = +1$. Therefore, $H(K) \neq H^+(K)$ and by Theorem 4.6 we have $N(33, -25) = 0$.

4.4 The equation $x^2 - Dy^2 = \pm 4p^r q^s$.

In this section we consider the solvability of the equation $x^2 - Dy^2 = \pm 4p^r q^s$, where p and q are distinct primes with $p \equiv q \equiv 3 \pmod{4}$. We begin by stating a theorem on the parity of the class number $h(pq)$ of $\mathbb{Q}(\sqrt{pq})$.

Theorem 4.7. Let $K = \mathbb{Q}(\sqrt{pq})$, where p, q are distinct primes such that $p \equiv q \equiv 3 \pmod{4}$. Let $h(pq)$ be the class number of K . Then we have $h(pq) \equiv 1 \pmod{2}$ and $h^+(pq) = 2 \cdot h(pq) \equiv 2 \pmod{4}$.

Proof: See [2, Theorem 1, p. 101]. □

We can use Theorem 4.7 to prove the following

Theorem 4.8. Let p, q be distinct primes such that $p \equiv q \equiv 3 \pmod{4}$. Let $r, s \in \mathbb{N}$.

Then we have

(1) If r is odd and s is even then

- (a) The equation $x^2 - p q y^2 = 4 p^r q^s$ is solvable if and only if $\left(\frac{p}{q}\right) = 1$.
- (b) The equation $x^2 - p q y^2 = -4 p^r q^s$ is solvable if and only if $\left(\frac{p}{q}\right) = -1$.
- (2) If r and s are odd then
- (a) $x^2 - p q y^2 = 4 p^r q^s$ is insolvable.
- (b) $x^2 - p q y^2 = -4 p^r q^s$ is solvable.
- (3) If r and s are even then
- (a) $x^2 - p q y^2 = 4 p^r q^s$ is solvable.
- (b) $x^2 - p q y^2 = -4 p^r q^s$ is insolvable.

Proof: We set $h = h(\mathbb{Q}(\sqrt{pq}))$.

case (1) : r is odd and s is even.

We first note that the equation $x^2 - p q y^2 = 4 p^r q^s$ is solvable if and only if $x^2 - p q y^2 = 4 p$ is solvable and the equation $x^2 - p q y^2 = -4 p^r q^s$ is solvable if and only if $x^2 - p q y^2 = -4 p$ is solvable. Thus it is enough to show the result for the equations $x^2 - p q y^2 = 4 p$ and $x^2 - p q y^2 = -4 p$. As $\left(\frac{pq}{p}\right) = 0$, we have $\langle p \rangle = P^2$, where P is a prime ideal of $\mathcal{O}_K$. By Theorem 4.7, we have that $h \equiv 1 \pmod{2}$. Hence we have in $H(K)$ that

$$[P]^2 = [\langle 1 \rangle] \text{ and } [P]^h = [\langle 1 \rangle].$$

Thus $[P] = [\langle 1 \rangle]$. By Theorem 4.7, we have that $h^+(pq) = 2h(pq)$. Thus $[\sqrt{D}]_+ \neq [\langle 1 \rangle]_+$ and either $[P]_+ = [\langle 1 \rangle]_+$ or $[P]_+ = [\sqrt{D}]_+$ but not both. As $[P] = [\langle 1 \rangle]$,

there exists $\frac{a + b\sqrt{pq}}{2} \in \mathcal{O}_K$ such that $\left\langle \frac{a + b\sqrt{pq}}{2} \right\rangle = Q$. Taking norms we obtain $|a^2 - pqb^2| = 4p$. Let $H_1, \dots, H_m$ be the generators of $H^+(K)$. If $\left[\left\langle \frac{a + b\sqrt{pq}}{2} \right\rangle \right]_+ = [< 1 >]_+$, then by Theorem 2.5, we have

$$V_{H_w}([Q]_+) \equiv 0 \pmod{h_w},$$

for all $w = 1, 2, \dots, m$. This implies that the equation $x^2 - pqy^2 = 4p$ is solvable and the equation $x^2 - pqy^2 = -4p$ is insolvable.

In the same way we have that $\left[\left\langle \frac{a + b\sqrt{pq}}{2} \right\rangle \right]_+ = [< \sqrt{D} >]_+$ implies that the equation $x^2 - pqy^2 = 4p$ is insolvable and the equation $x^2 - pqy^2 = -4p$ is solvable.

Therefore one and only one of the equations $x^2 - pqy^2 = 4p$ and $x^2 - pqy^2 = -4p$ is solvable.

case (1)(a) :

($\implies$) : Suppose that $x^2 - pqy^2 = 4p$ is solvable and $\left(\frac{p}{q}\right) = -1$. Then since $x^2 - pqy^2 = 4p$ is solvable we have $x^2 \equiv 4p \pmod{q}$. But $\left(\frac{4p}{q}\right) = 1 \cdot \left(\frac{p}{q}\right) = -1$. A contradiction. Therefore $\left(\frac{p}{q}\right) = +1$.

($\impliedby$) : We know that one and only one of $x^2 - pqy^2 = 4p$ and $x^2 - pqy^2 = -4p$ is solvable. Suppose that $\left(\frac{p}{q}\right) = +1$ and $x^2 - pqy^2 = -4p$ is solvable. Then we have that $x^2 \equiv -4p \pmod{q}$. But $\left(\frac{-4p}{q}\right) = \left(\frac{-4}{q}\right) \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) \left(\frac{4}{q}\right) \left(\frac{p}{q}\right) = -1 \cdot 1 \cdot 1 = -1$, which is a contradiction. Therefore $x^2 - pqy^2 = 4p$ is solvable.

case (1)(b) :

($\implies$) : Suppose that $x^2 - pqy^2 = -4p$ is solvable and $\left(\frac{p}{q}\right) = +1$. Then since $x^2 - pqy^2 = -4p$ is solvable we have $x^2 \equiv -4p \pmod{q}$. But $\left(\frac{-4p}{q}\right) = \left(\frac{-1}{q}\right) \cdot 1 \cdot 1 = -1$, a contradiction. Therefore $\left(\frac{p}{q}\right) = -1$.

($\impliedby$) : We know that one and only one of $x^2 - pqy^2 = 4p$ and $x^2 - pqy^2 = -4p$ is solvable. Suppose that $\left(\frac{p}{q}\right) = -1$ and $x^2 - pqy^2 = 4p$ is solvable. Then we have that $x^2 \equiv 4p \pmod{q}$. But $\left(\frac{4p}{q}\right) = \left(\frac{4}{q}\right) \left(\frac{p}{q}\right) = 1 \cdot -1 = -1$, which is a contradiction. Therefore, $x^2 - pqy^2 = -4p$ is solvable.

case (2) : r and s are odd.

We first note that the equation $x^2 - pqy^2 = 4p^r q^s$ is solvable if and only if $x^2 - pqy^2 = 4pq$ is solvable and the equation $x^2 - pqy^2 = -4p^r q^s$ is solvable if and only if $x^2 - pqy^2 = -4pq$ is solvable. As $\left(\frac{pq}{p}\right) = 0$ and $\left(\frac{pq}{q}\right) = 0$, we have $\langle p \rangle = P^2$ and $\langle q \rangle = Q^2$, where P and Q are prime ideals of $\mathcal{O}_K$. By Theorem 4.8, we have that $h \equiv 1 \pmod{2}$. Hence we have in $H(K)$ that

$$[P]^2 = [\langle 1 \rangle], [P]^h = [\langle 1 \rangle], [Q]^2 = [\langle 1 \rangle] \text{ and } [Q]^h = [\langle 1 \rangle].$$

Thus $[P] = [Q] = [\langle 1 \rangle]$. By Theorem 4.8, we have that $h^+(pq) = 2h(pq)$. Thus $[\sqrt{D}]_+ \neq [\langle 1 \rangle]_+$ and $[P]_+ = [\langle 1 \rangle]_+$ or $[P]_+ = [\sqrt{D}]_+$ but not both and $[Q]_+ = [\langle 1 \rangle]_+$ or $[Q]_+ = [\sqrt{D}]_+$ but not both. If $[P]_+ = [Q]_+ = [\langle 1 \rangle]_+$, we have that the equation $x^2 - pqy^2 = 4p$ and $x^2 - pqy^2 = 4q$ are solvable. By case 1, this implies that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. This is a contradiction since as $p \equiv 3$

(mod 4), the quadratic reciprocity law implies $\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right)$. Thus we cannot have $[P]_+ = [Q]_+ = [< 1 >]_+$. In the same way, we can prove that we cannot have $[P]_+ = [Q]_+ = [\sqrt{D}]_+$. Thus $[P]_+ \neq [Q]_+$. Let $H_1, \dots, H_m$ be the generators of $H^+(K)$. If $[P]_+ = [< 1 >]_+$ and $[Q]_+ = [< \sqrt{D} >]_+$ then

$$V_{H_w}([P]_+) + V_{H_w}([Q]_+) = V_{H_w}([Q]_+) \neq 0 \text{ for all } w = 1, \dots, m.$$

We obtain the same result if $[P]_+ = [\sqrt{D}]_+$ and $[Q]_+ = [< 1 >]_+$.

Therefore, by Theorem 2.5 and the fact that $[P]_+ \neq [Q]_+$, we have that the equation $x^2 - pqy^2 = 4pq$ is not solvable.

If $[P]_+ = [< 1 >]_+$ and $[Q]_+ = [< \sqrt{D} >]_+$ then

$$V_{H_w}([P]_+) + V_{H_w}([Q]_+) = V_{H_w}([Q]_+) \equiv c_w \text{ for all } w = 1, \dots, m,$$

where $c_1, \dots, c_m$ are the unique integers in the representation of $[\sqrt{D}]_+$.

We get the same result if $[P]_+ = [< \sqrt{D} >]_+$ and $[Q]_+ = [< 1 >]_+$. Therefore, by Theorem 2.5 and the fact that $[P]_+ \neq [Q]_+$, we have that the equation $x^2 - pqy^2 = -4pq$ is solvable.

case (3) : r and s are even.

The equation $x^2 - pqy^2 = 4p^r q^s$ is obviously solvable as

$$(2p^{\frac{r}{2}} q^{\frac{s}{2}})^2 - pq(0)^2 = 4p^r q^s.$$

In the proof of case 2, we have shown that $[P]_+ \neq [Q]_+$. Suppose that $x^2 - pqy^2 =$

$-4p^r q^s$ is solvable. Then by Theorem 2.5 we have

$$rV_{H_w}([P]_+) + sV_{H_w}([Q]_+) \equiv 0 + 0 = 0 \neq c_w \text{ for all } w = 1, \dots, m.$$

This is a contradiction. Therefore $x^2 - pqy^2 = -4p^r q^s$ is insolvable. $\square$

4.5 Number of classes of solutions of more general equations

In this section we extend Definition 1.3 to equations of the form $x^2 - my^2 = n$, where m is a squarefree integer and n is a nonzero integer. We write $N^*(m, n)$ to denote the number of classes of solutions of the equation $x^2 - my^2 = n$. We will see that $N^*(m, n) = N(4m, n)$ holds for particular values of m and n .

Definition 4.1. Let m be a squarefree integer. We write $S^*(m, n)$ to denote the set of solutions of the equation $x^2 - my^2 = n$, that is, $S^*(m, n) = \{(x, y) \in \mathbb{Z}^2 \mid x^2 - my^2 = n\}$.

Theorem 4.9. If $S^*(m, n) \neq \emptyset$ then $S^*(m, n)$ is an infinite set.

Proof: Let $K = \mathbb{Q}(\sqrt{m})$. We first remark that if $u + v\sqrt{m}$ is a solution of $x^2 - my^2 = n$ and $a + b\sqrt{m}$ a solution of $r^2 - ms^2 = 1$ then $(u + v\sqrt{m})(a + b\sqrt{m}) = (au + bvm) + (bu + av)\sqrt{m}$ is also a solution of $x^2 - my^2 = n$.

case (1) : $m \not\equiv 1 \pmod{4}$.

Let $\eta = u_1 + v_1\sqrt{m}$ be the fundamental unit of norm +1 of K . Then $u_1^2 - mv_1^2 = 1$ and $(u_1 + v_1\sqrt{m})(a + b\sqrt{m})$ is a solution of $x^2 - my^2 = n$.

As $\eta^z \in U^+(K)$, for all $z \in \mathbb{N}$, we have $\eta^z(a + b\sqrt{m})$ is a solution of $x^2 - my^2 = n$.

Therefore there are infinitely many solutions to the equation $x^2 - my^2 = n$.

case (2) : $m \equiv 1 \pmod{4}$.

Let η be the fundamental unit of norm $+1$ of $\mathcal{K}$. Then $\eta = \frac{x_1 + y_1\sqrt{m}}{2}$, where $x_1 \equiv y_1 \pmod{2}$. Let $\frac{t + u\sqrt{m}}{2} = \left(\frac{x_1 + y_1\sqrt{m}}{2}\right)^3$. Then

$$t = \frac{x_1^3 + 3x_1(x_1^2 - 4)}{4} = \frac{4x_1^3 - 12x_1}{4} = x_1^3 - 3x_1 = x_1(x_1^2 - 3) \equiv 0 \pmod{2}.$$

Thus $2 \mid t$ and $2 \mid u$. Let $t = 2r$, $u = 2s$, where $r, s \in \mathbb{Z}$. Then

$$\frac{t + u\sqrt{m}}{2} = r + s\sqrt{m} \text{ and } r^2 - ms^2 = 1.$$

Let $\theta = r + s\sqrt{m}$ and let $a + b\sqrt{m}$ be a solution of $x^2 - my^2 = n$. Then $\theta(a + b\sqrt{m})$ is a solution of $x^2 - my^2 = n$. As $\theta \in \mathcal{U}^+(K)$, we have $\theta^z \in \mathcal{U}^+(K)$ for all $z \in \mathbb{N}$. Thus $\theta^z(a + b\sqrt{m})$ is a solution to the equation $x^2 - my^2 = n$ for all $z \in \mathbb{N}$. Therefore the equation $x^2 - my^2 = n$ has infinitely many solutions. $\square$

We now introduce an equivalence relation on the set $S^*(m, n)$.

Definition 4.2. Let m be a squarefree integer and let n be a nonzero integer. Suppose $S^*(m, n) \neq \emptyset$. Let $(x_1, y_1) \in \mathbb{Z}^2$ and $(x_2, y_2) \in \mathbb{Z}^2$ be solutions of $x^2 - my^2 = n$. We say that (x_1, y_1) and (x_2, y_2) are strictly associated solutions of $x^2 - my^2 = n$, written $(x_1, y_1) \sim (x_2, y_2)$, if and only if there exists $\eta \in \mathcal{U}^+(\mathcal{O}_K)$, where $K = \mathbb{Q}(\sqrt{m})$, such that

$$x_1 + y_1\sqrt{m} = \eta(x_2 + y_2\sqrt{m}).$$

Theorem 4.10. $\sim$ is an equivalence relation on $S^*(m, n)$.

Proof: The proof is similar to the proof of Theorem 1.5. $\square$

Definition 4.3. The equivalence classes under $\sim$ are called classes of solutions. The class of solutions containing the solution (x, y) of $x^2 - my^2 = n$ is denoted by $[(x, y)]$.

Definition 4.4. Let m be a squarefree integer and n a nonzero integer. We define $N^*(m, n)$ to be the number of classes of solutions of the equation $x^2 - my^2 = n$.

The following theorem gives a relation between $N^*(m, n)$ and $N(4m, n)$ for particular values of m .

Theorem 4.11. Let m be a squarefree integer such that $m \equiv 2, 3 \pmod{4}$. Let n be a nonzero integer. Then $N^*(m, n) = N(4m, n)$.

Proof: We define $\lambda : S^*(m, n) \mapsto S(4m, n)$ by $\lambda((x, y)) = (2x, y)$.

λ is well defined as $(x, y) \in S^*(m, n) \implies x^2 - my^2 = n \implies 4(x^2 - my^2) = 4n \implies (2x)^2 - 4my^2 = 4n \implies (2x, y) \in S(4m, n)$.

λ is one-to-one as $\lambda(x_1, y_1) = \lambda(x_2, y_2) \implies (2x_1, y_1) = (2x_2, y_2)$

$\implies x_1 = x_2$ and $y_1 = y_2 \implies (x_1, y_1) = (x_2, y_2)$.

λ is onto since $(a, b) \in S(4m, n) \implies a^2 - 4mb^2 = 4n \implies 4 \mid a^2$

$\implies 2 \mid a \implies a = 2a_1 \implies 4a_1^2 - 4mb^2 = 4n \implies a_1^2 - mb^2 = n$

$\implies (a_1, b) \in S^*(m, n)$ and $\lambda((a_1, b)) = (a, b)$.

Therefore λ is a bijection.

Next we show that λ preserves $\sim$, that is, if (x, y) and (x', y') are strictly associated solutions in $S^*(m, n)$ then $\lambda((x, y))$ and $\lambda((x', y'))$ are strictly associated solutions in $S(4m, n)$. Let (x, y) and (x', y') be strictly associated in $S^*(m, n)$, that is, there exists $\varepsilon \in \mathcal{O}_K$ such that $N(\varepsilon) = +1$ and

$$x + y\sqrt{m} = \varepsilon(x' + y'\sqrt{m}). \quad (5)$$

Multiplying (5) by 2 on both sides, we obtain

$$2x + y\sqrt{4m} = \varepsilon(2x' + y'\sqrt{4m}).$$

As $\lambda((x, y)) = (2x, y)$ and $\lambda((x', y')) = (2x', y')$ we see that $\lambda(x, y)$ is associated with $\lambda(x', y')$. Thus, we have that λ preserves $\sim$. Therefore $x^2 - my^2 = n$ and $x^2 - 4my^2 = 4n$ have the same number of classes of solutions. Hence $N^*(m, n) = N(4m, n)$. $\square$

Example 4.6. We show that $N^*(15, 9261) = 4$. As $15 \equiv 3 \pmod{4}$, we have $N^*(15, 9261) = N(60, 9261) = 4$ by Theorem 4.11 and Example 3.7.

Conclusion

In this thesis we proved a theorem giving the number $N(D, E)$ of classes of solutions of the equation

$$x^2 - Dy^2 = 4E,$$

where D is a positive discriminant and E is a nonzero integer. For certain values of D and E explicit formulae were derived for $N(D, E)$ from this theorem. It would be interesting to extend this formulae to other special classes of D and E .

Appendix A

Computer program

In this appendix we give the computer program that we used to compute $N(D, E)$, where D is a positive discriminant and E is a nonzero integer. The program is based on Theorems 1.6 and 1.8. The program is written in C++ and a Number Theory library was used that allowed us to work with very large integers. This C++ library can be found on internet at the following address

<http://www.shoup.net/ntl/>

A.1 Computer program nde.c

The program is called nde.c. We begin by creating a makefile to give instructions to the compiler on how to compile the program. The name of this file is makefilende

```
# makefile for nde program

nde: nde.o
g++ -L/home/mathieul/lib -o nde nde.o -lntl -lm

nde.o: nde.c
g++ -c -I/home/mathieul/include nde.c

# g++ -c -ggdb nde.c
```

To compile the program simply type

make - k - f makefilende

To run the program type

nde

The program nde.c is as follow

```
# include <iostream.h>
# include <math.h>
# include <limits.h>
# include <NTL/ZZ.h>
# include <NTL/RR.h>

/* Inclusion of the library NTL/ZZ.h to work with arbitrary large
/* large real numbers. */

/* Global Variables */

/* Function Protoype */

ZZ ifl(ZZ z);

/*declaration of functions. */

void loopfinduv(ZZ, ZZ*, ZZ*);
int Qsquarefree(ZZ);
int main(void)

{ ZZ x , r , t , z , u , v , p , c;
  ZZ *b, *a ,l , fs , squareroot, tmpsqr;      /* Declaration of variables */
  long i,j, m ;

  int passflag;
```

```

r=1;
cout << "\n" << "This program find the number of class of solution of the
equation  $u^2 - v^2 D = 4E$  , where D is a positive discriminant and E a
nonzero integer. \n" << "\n" << "\n" << " Input a positive discriminant
for the value of D and a nonzero integer for the value of E .\n";

/* The program ask the user to input a value for D and a value for E. */
/* Note that the value for D is t and the value for E is p. */

cin >> t;
cin >> p;

if (t%4 ==0 && (t/4)%4 != 1)
{
    passflag=Qsquarefree(t/4);
}
else if(t % 4 == 1) /* We make sure that the value for D is a
                    /* positive discriminant. */
{
    passflag=Qsquarefree(t);
}
else
{
    passflag=0;
}
while ( passflag == 0 || t < 0 || t == 1 || t == 4)
/* If the entry for D is not a positive discriminant then the user is
asked to type another value */
{
    cout << "\n" << "You need to type a positive discriminant. \n" << "\n"
    << "Input another positive integer .\n";
    cin >> t;
    if (t%4 ==0 && (t/4)%4 != 1)
    {
        passflag=Qsquarefree(t/4);
    }
    else if(t % 4 == 1)
    {
        passflag=Qsquarefree(t);
    }
}

```

```

        else
        {
passflag=0;
        }
    }

    loopfinduv(t, &u, &v);

/* We find the smallest value of $v > 0$ such that  $u^2 - Dv^2 = 4$ . */
/* For this we use the function loopfinduv */

cout << "The fundamental solution of the Pell's equation  $u^2 - "$  << t << "
 $v^2 = 4$  is : \n" << u << " + " << v << " Sqrt(" << t << ") \n\n";

/* The program give the fundamental solution of the equation  $u^2 - Dv^2$ 
= 4 */

i = 0;
if ( p >= 0)                /* When E > 0, we use Theorem 1.8 {\rm (1)} */
{

for ( c = 0 ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(p)) / SqrRoot(to_RR(u+2))
+ 0.00000000000001 ) ; c++)
{
    tmpsqrt = SqrRoot(4*p+t*c*c);
    if ( tmpsqrt*tmpsqrt == 4*p+t*c*c )
    {
/* We use Theorem 1.8 to find the possible fundamental solutions of the */
equation  $u^2 - Dv^2 = 4E$ . The first loop is to find the number of
possible fundamental solutions */

i = i + 1;
    }
}
a = (ZZ*) calloc( 2*i , sizeof(ZZ));
b = (ZZ*)      calloc( 2*i , sizeof(ZZ));
j = 0;
for ( c = 0 ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(p)) / SqrRoot(to_RR(u+2))
+ 0.00000000000001 ) ; c++)
{

```

```

    tmpsqrt = SqrRoot(4*p+t*c*c);
    if ( tmpsqrt*tmpsqrt == 4*p+t*c*c )
    {
        /* Knowing the number of possible fundamental solutions the program assign */
        /* space to each possibility */
        b[j] = c ;
        a[j] = tmpsqrt;
        b[j+1] = c ;
        a[j+1] = (-1)*tmpsqrt;
        cout << ifl(a[j]) << " + " << b[j] << "Sqrt(" << t << ") is possibly a
        fundamental solution. \n" << ifl(a[j+1]) << " + " << b[j+1] <<
        "Sqrt(" << t << ") is possibly a fundamental solution .\n";
        j = j +2;
    }
    }
    l = 2*i;
    cout << "\n";

    /* We use Theorem 1.6 to verify which possible solutions are equivalent */

    for( j = 0 ; j < 2*i ; j++)
    {
        for( m = 0 ; m < 2*i && m != j ; m++)
        {
            if ( a[j]*a[m] - b[j]*b[m]*t == 2*p*((a[j]*a[m] - b[j]*b[m]*t) /(2*p))
            && b[j]*a[m] - a[j]*b[m] == 2*p*( (b[j]*a[m] - a[j]*b[m]) /(2*p) ) )
            {
                a[j] = a[m];
                b[j] = b[m];
                l = l - 1;
            }
        }
    }
    cout << " The number of classes is : " << l << "\n" << "\n";

    /* The program write that there is no solution when N(D,E) = 0. */

    if (l == 0 )
    {
        cout << "The equation has no solution .\n";
    }

```

```

}
```

```

/* The program give the fundamental solution in the case where  $N(D,E) = 1$  */
```

```

if (l == 1)
{
    cout << "The fundamental solution of this equation is :\n\n";
    for ( j = 0 ; j < l ; j++)
    {
        cout << ifl(a[j]) << " + " << b[j] << " Sqrt(" << t << ") \n";
    }
}
```

```

/* The program write all the distinct fundamental solutions if  $N(D,E) > 1$  */
```

```

if (l > 1)
{
    cout << "The fundamental solutions of this equation are :\n";
    for ( j = 0 ; j < 2*i ; j++)
    {
        fs = 0 ;
        for ( m = 0 ; m < 2*i && m != j ; m++ )
        {
            if ( a[j] != a[m] || b[j] != b[m] )
            {
                continue ;
            }
            else
            {
                fs = fs +1 ;
            }
        }
        if( fs == 0)
        {
            cout << ifl(a[j]) << " + " << b[j] << " Sqrt(" << t << ") \n";
        }
        else
        {
            continue ;
        }
    }
}
```



```

}
}
}
if (p < 0)
/* Similar to the case when E > 0 except that we use Theorem 1.8 in that case */
{
for ( c = SqrRoot(-4*p/t) ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(-p)) /
SqrRoot(to_RR(u-2)) + 0.00000000000001 ) ; c++)
{
if ( 4*p+t*c*c > 0)
{
tmpsqr = SqrRoot(4*p+t*c*c);
/* cout << "y ?? " << c << " x ?? " << tmpsqr << " x^2 ?? " <<
tmpsqr*tmpsqr << " 4p+tc^2 = " << 4*p+t*c*c << "\n"; */
if ( tmpsqr*tmpsqr == 4*p+t*c*c )
{
i = i + 1;
}
}
}
a = (ZZ*) calloc( 2*i , sizeof(ZZ));
b = (ZZ*) calloc( 2*i , sizeof(ZZ));
j = 0;
for ( c = SqrRoot(-4*p/t) ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(-p)) /
SqrRoot(to_RR(u-2)) + 0.00000000000001 ) ; c++)
{
if ( 4*p+t*c*c > 0)
{
tmpsqr = SqrRoot(4*p+t*c*c);
if ( tmpsqr*tmpsqr == 4*p+t*c*c )
{
b[j] = c ;
a[j] = tmpsqr;
b[j+1] = c ;
a[j+1] = (-1)*tmpsqr;
cout << ifl(a[j]) << " + " << b[j] << "Sqrt(" << t << ") is possibly
a fundamental solution. \n" << ifl(a[j+1]) << " + " << b[j+1] <<
"Sqrt(" << t << ") is possibly a fundamental solution .\n";
j = j +2;
}
}
}

```

```

}
}
l = 2*i;
cout << "\n";
for( j = 0 ; j < 2*i ; j++)
{
for( m = 0 ; m < 2*i && m != j ; m++)
{
    if ( a[j]*a[m] - b[j]*b[m]*t == 2*p*((a[j]*a[m] - b[j]*b[m]*t) / (2*p))
    && b[j]*a[m] - a[j]*b[m] == 2*p*( (b[j]*a[m] - a[j]*b[m]) / (2*p) ) )
    {
        a[j] = a[m];
        b[j] = b[m];
        l = l - 1;
    }
}
}
cout << " The number of classes is : " << l << "\n" << "\n";

if (l == 0 )
{
    cout << "The equation has no solution .\n";
}
if (l == 1)
{
    cout << "The fundamental solution of this equation is :\n\n";
    for ( j = 0 ; j < l ; j++)
    {
        cout << ifl(a[j]) << " + " << b[j] << " Sqrt(" << t << ") \n";
    }
}
if (l > 1)
{
    cout << "The fundamental solutions of this equation are :\n";
    for ( j = 0 ; j < l ; j++)
    {
        cout << ifl(a[j]) << " + " << b[j] << " Sqrt(" << t << ") \n";
    }
}
}

```

```

return 0;
}

ZZ ifl(ZZ z)
{
  ZZ i , k;
  if( z >= 0 )
  {
    for( i = 1 ; i <= z ; i++)
    {
      if ( i == z)
      {
        k = i;
      }
      else
      {
        continue;
      }
    }
  }
  if( z < 0 )
  {
    for( i = 1 ; i <= -z ; i++)
    {
      if ( i == -z)
      {
        k = -i;
      }
      else
      {
        continue;
      }
    }
  }
  return k ;
}

/* This function replace v in the equation  $4 + Dv^{\{2\}}$  until it */
/* is a perfect square. With the first value of v we can find the */
/* value of u and the resulting u and v give the fundamental */
/* solution of the equation  $x^{\{2\}} - Dy^{\{2\}} = 4$ . */

```

```

void loopfinduv(ZZ t, ZZ *u, ZZ *v)
{
    ZZ i,x;
    for(i=1;i<LONG_MAX;i++)
    {
        x= SqrRoot(4+t*i*i);
        if (x*x==4+t*i*i)
        {
            *v=i;
            *u=x;
            return;
        }
        cout << "The fundamental solution of the Pell's equation u^2 - "
        << t << " v^2 = 4 gives u bigger than maximum long integer\n ";
        exit(0);
    }

    /* This function verify if a given integer is squarefree or not */

    int Qsquarefree(ZZ m)
    {
        PrimeSeq s;
        ZZ p;
        s.reset(2);
        p = s.next();
        while (p <= SqrRoot(m))
        {
            if (m % (p*p) == 0)
                return 0;
            p= s.next();
        }
        return 1;
    }
}

```

A.2 Example of an output of nde.c

In this section we give an example of an output of nde.c. For this example we give the value of $N(105, 7774)$.

Input : nde

This program find the number of class of solution of the equation $u^2 - v^2 D = 4E$, where D is a positive discriminant and E a nonzero integer.

Input a positive discriminant for the value of D and a nonzero integer for the value of E .

105

7774

The fundamental solution of the Pell's equation $u^2 - 105 v^2 = 4$ is :
82 + 8 Sqrt(105)

179 + 3Sqrt(105) is possibly a fundamental solution.
-179 + 3Sqrt(105) is possibly a fundamental solution .
199 + 9Sqrt(105) is possibly a fundamental solution.
-199 + 9Sqrt(105) is possibly a fundamental solution .
221 + 13Sqrt(105) is possibly a fundamental solution.
-221 + 13Sqrt(105) is possibly a fundamental solution .
311 + 25Sqrt(105) is possibly a fundamental solution.
-311 + 25Sqrt(105) is possibly a fundamental solution .
571 + 53Sqrt(105) is possibly a fundamental solution.
-571 + 53Sqrt(105) is possibly a fundamental solution .
689 + 65Sqrt(105) is possibly a fundamental solution.
-689 + 65Sqrt(105) is possibly a fundamental solution .

The number of classes is : 12

The fundamental solutions of this equation are :

179 + 3 Sqrt(105)
-179 + 3 Sqrt(105)
199 + 9 Sqrt(105)
-199 + 9 Sqrt(105)
221 + 13 Sqrt(105)
-221 + 13 Sqrt(105)
311 + 25 Sqrt(105)

-311 + 25 Sqrt(105)

571 + 53 Sqrt(105)

-571 + 53 Sqrt(105)

689 + 65 Sqrt(105)

-689 + 65 Sqrt(105)

Appendix B

Tables

B.1 Computer program duc.c

In this appendix we give tables that give the value of $N(D, E)$ for all positive discriminants between 5 and 317 when E is a fixed positive integer between 2 and 10. To produce these tables we use the program duc.c . We note the following values of D are not in the table : 97, 193, 233, 241, 265, 281, 313. In these cases the fundamental solutions of the equation has extremely large values of y .

First we give the makefile of this program. This file is called makefileduc

```
# makefile for duc.c program

duc: duc.o
g++ -L/home/mathieul/lib -o duc duc.o -lntl -lm

duc.o: duc.c
g++ -c -I/home/mathieul/include duc.c

# g++ -c -ggdb duc.c
```

To compile this program type

```
make -k -f makefileduc
```

To run this program type duc .

We note that the program duc.c is a slight modification of nde that allow to compute $N(D, E)$ for consecutive values of D and a fixed value of E .

The program duc.c is the following

```
# include <iostream.h>
# include <math.h>
# include <limits.h>
# include <NTL/ZZ.h>
# include <NTL/RR.h>
/* Global Variables */

/* Function Prototype */

ZZ ifl(ZZ z);

void loopfinduv(ZZ, ZZ*, ZZ*);
int Qsquarefree(ZZ);
int main(void)

{ ZZ x , r , t , z , u , v , p , c;
  ZZ *b, *a , l , fs , squareroot, tmpsqrt;
  long i, j, m ;
  double y , f ;
  int passflag;
  r=1;
  cout << "\n" << "This program find the number of class of the equation
  u^2 - v^2 D = 4E,
  where E is a fixed nonzero integer and D is a positive
  discriminant between 5 and 317. \n"
  << "\n" << "\n" << "Input a nonzero
  integer for the value of E .\n";

  cin >> p;
  while ( p == 0)
```



```

{
cout << "Input a nonzero integer for the value of E \n";
cin >> p;
}
for (t = 1; t <= 317 ; t++)
{
if (t == 1 || t == 4 || t == 97 || t == 193 || t == 233 || t == 241
|| t == 265 || t == 281 || t == 313)
{
continue;
}
if (t%4 ==0 && (t/4)%4 != 1)
{
passflag=Qsquarefree(t/4);
}
else if(t % 4 == 1)
{
passflag=Qsquarefree(t);
}
else
{
passflag=0;
}
if ( passflag==0 )
{
continue;
}
cout << t << " & ";

loopfinduv(t, &u, &v);

i = 0;
if ( p >= 0)
{
for ( c = 0 ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(p)) / SqrRoot(to_RR(u+2))
+ 0.00000000000001 ) ; c++)
{
tmpsqr = SqrRoot(4*p+t*c*c);

```

```

if ( tmpsqr*tmpsqr == 4*p+t*c*c )
{
i = i + 1;
}
}
a = (ZZ*) calloc( 2*i , sizeof(ZZ));
b = (ZZ*)      calloc( 2*i , sizeof(ZZ));
j = 0;
for ( c = 0 ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(p)) / SqrRoot(to_RR(u+2))
+ 0.00000000000001 ); c++)
{
    tmpsqr = SqrRoot(4*p+t*c*c);
    if ( tmpsqr*tmpsqr == 4*p+t*c*c )
    {
        b[j] = c ;
        a[j] = tmpsqr;
        b[j+1] = c ;
        a[j+1] = (-1)*tmpsqr;
        j = j +2;
    }
}
l = 2*i;

for( j = 0 ; j < 2*i ; j++)
{
    for( m = 0 ; m < 2*i && m != j ; m++)
    {
        if ( a[j]*a[m] - b[j]*b[m]*t == 2*p*((a[j]*a[m] - b[j]*b[m]*t) /(2*p))
        && b[j]*a[m] - a[j]*b[m] == 2*p*( (b[j]*a[m] - a[j]*b[m]) /(2*p) ) )
        {
            a[j] = a[m];
            b[j] = b[m];
            l = l - 1;
        }
    }
}
cout << l << " \\ " << "\n";
}
if (p < 0)
{

```

```

for ( c = SqrRoot(-4*p/t) ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(-p))
  / SqrRoot(to_RR(u-2)) + 0.00000000000001 ) ; c++)
{
  if ( 4*p+t*c*c > 0)
  {
    tmpsqr = SqrRoot(4*p+t*c*c);
    if ( tmpsqr*tmpsqr == 4*p+t*c*c )
    {
      i = i + 1;
    }
  }
}
a = (ZZ*) calloc( 2*i , sizeof(ZZ));
b = (ZZ*)      calloc( 2*i , sizeof(ZZ));
j = 0;
for ( c = SqrRoot(-4*p/t) ; c <= to_ZZ( to_RR(v) * SqrRoot(to_RR(-p))
  / SqrRoot(to_RR(u-2)) + 0.00000000000001 ) ; c++)
{
  if ( 4*p+t*c*c > 0)
  {
    tmpsqr = SqrRoot(4*p+t*c*c);
    if ( tmpsqr*tmpsqr == 4*p+t*c*c )
    {
      b[j] = c ;
      a[j] = tmpsqr;
      b[j+1] = c ;
      a[j+1] = (-1)*tmpsqr;
      j = j +2;
    }
  }
  l = 2*i;
  for( j = 0 ; j < 2*i ; j++)
  {
    for( m = 0 ; m < 2*i && m != j ; m++)
    {
      if ( a[j]*a[m] - b[j]*b[m]*t == 2*p*((a[j]*a[m] - b[j]*b[m]*t) / (2*p))
      && b[j]*a[m] - a[j]*b[m] == 2*p*( (b[j]*a[m] - a[j]*b[m]) / (2*p) ) )
      {
        a[j] = a[m];

```

```
b[j] = b[m];  
l = l - 1;  
}  
}  
}  
cout << l << "\n";  
}  
}  
return 0;  
}
```

```
ZZ if1(ZZ z)  
{  
    ZZ i , k;  
    if( z >= 0 )  
    {  
        for( i = 1 ; i <= z ; i++)  
        {  
            if ( i == z)  
            {  
                k = i;  
            }  
            else  
            {  
                continue;  
            }  
        }  
    }  
    if( z < 0 )  
    {  
        for( i = 1 ; i <= -z ; i++)  
        {  
            if ( i == -z)  
            {  
                k = -i;  
            }  
            else  
            {  
                continue;  
            }  
        }  
    }  
}
```

```

    }
    }
    return k ;
}

void loopfinduv(ZZ t, ZZ *u, ZZ *v)
{
    ZZ i,x;
    for(i=1;i<LONG_MAX;i++)
    {

        x= SqrRoot(4+t*i*i);
        if (x*x==4+t*i*i)
    {
        *v=i;
        *u=x;
        return;
    }

    cout << "The fundamental solution of the Pell's equation u^2 - "
    << t << " v^2 = 4 gives u bigger than maximum long integer\n ";
    exit(0);
}

int Qsquarefree(ZZ m)
{
    PrimeSeq s;
    ZZ p;
    s.reset(2);
    p = s.next();
    while (p <= SqrRoot(m))
    {
        if (m % (p*p) == 0)
    return 0;
        p= s.next();
    }
    return 1;
}

```

B.2 Tables

In this section we produce tables giving the value of $N(D, E)$ when E is a positive integer between 2 and 10 and D is a positive discriminant between 5 and 317 except for the values $D = 97, 193, 241, 244, 265, 281, 313$.

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 8 = 4 \cdot 2$ for the following values of D :

Value of D	Value of $N(D, 2)$
5	0
8	1
12	0
13	0
17	2
21	0
24	0
28	1
29	0
33	0
37	0
40	0
41	2
44	0
53	0
56	1
57	0
60	0
61	0
65	0
69	0
73	2
76	0
77	0
85	0
88	0
89	2
92	1
93	0
101	0
104	0
105	0
109	0
113	2
120	0
124	1
129	0
133	0
136	1
137	2
140	0
141	0
145	0
149	0
152	0

Value of D	Value of $N(D, 2)$
156	0
157	0
161	2
165	0
168	0
172	0
173	0
177	0
181	0
184	1
185	0
188	1
197	0
201	0
204	0
205	0
209	0
213	0
217	2
220	0
221	0
229	0
232	0
236	0
237	0
248	1
249	0
253	0
257	0
264	0
268	0
269	0
273	0
277	0
280	0
284	1
285	0
293	0
296	0
301	0
305	0
309	0
312	0
316	1
317	0

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 12 = 4 \cdot 3$ for the following values of D :

Value of D	Value of $N(D, 3)$
5	0
8	0
12	0
13	2
17	0
21	0
24	1
28	0
29	0
33	1
37	2
40	0
41	0
44	0
53	0
56	0
57	0
60	0
61	2
65	0
69	1
73	2
76	0
77	0
85	0
88	2
89	0
92	0
93	0
101	0
104	0
105	0
109	2
113	0
120	0
124	0
129	0
133	0
136	0
137	0
140	0
141	1
145	0
149	0
152	0

Value of D	Value of $N(D, 3)$
156	0
157	2
161	0
165	0
168	0
172	0
173	0
177	1
181	2
184	2
185	0
188	0
197	0
201	0
204	0
205	0
209	0
213	1
217	0
220	0
221	0
229	0
232	0
236	0
237	0
248	0
249	1
253	2
257	0
264	0
268	0
269	0
273	0
277	2
280	0
284	0
285	0
293	0
296	0
301	0
305	0
309	0
312	1
316	0
317	0

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 16 = 4 \cdot 4$ for the following values of D :

Value of D	Value of $N(D, 4)$
5	1
8	1
12	1
13	1
17	3
21	1
24	1
28	1
29	1
33	3
37	1
40	1
41	3
44	1
53	1
56	1
57	3
60	1
61	1
65	3
69	1
73	3
76	1
77	1
85	1
88	1
89	3
92	1
93	1
101	1
104	1
105	3
109	1
113	3
120	1
124	1
129	3
133	1
136	1
137	3
140	1
141	1
145	1
149	1
152	1

Value of D	Value of $N(D, 4)$
156	1
157	1
161	3
165	1
168	1
172	1
173	1
177	3
181	1
184	1
185	3
188	1
197	1
201	3
204	1
205	1
209	3
213	1
217	3
220	1
221	1
229	1
232	1
236	1
237	1
248	1
249	3
253	1
257	1
264	1
268	1
269	1
273	3
277	1
280	1
284	1
285	1
293	1
296	1
301	1
305	1
309	1
312	1
316	1
317	1

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 20 = 4 \cdot 5$ for the following values of D :

Value of D	Value of $N(D, 5)$
5	1
8	0
12	0
13	0
17	0
21	0
24	0
28	0
29	2
33	0
37	0
40	0
41	2
44	2
53	0
56	0
57	0
60	0
61	2
65	0
69	0
73	0
76	2
77	0
85	0
88	0
89	2
92	0
93	0
101	2
104	0
105	0
109	2
113	0
120	0
124	2
129	0
133	0
136	0
137	0
140	0
141	0
145	0
149	2
152	0

Value of D	Value of $N(D, 5)$
156	0
157	0
161	0
165	0
168	0
172	0
173	0
177	0
181	2
184	0
185	0
188	0
197	0
201	0
204	0
205	1
209	2
213	0
217	0
220	1
221	0
229	0
232	0
236	2
237	0
248	0
249	0
253	0
257	0
264	0
268	0
269	2
273	0
277	0
280	0
284	2
285	0
293	0
296	0
301	0
305	1
309	0
312	0
316	0
317	0

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 24 = 4 \cdot 6$ for the following values of D :

Value of D	Value of $N(D, 6)$
5	0
8	0
12	1
13	0
17	0
21	0
24	0
28	0
29	0
33	0
37	0
40	2
41	0
44	0
53	0
56	0
57	2
60	0
61	0
65	0
69	0
73	4
76	2
77	0
85	0
88	0
89	0
92	0
93	0
101	0
104	0
105	0
109	0
113	0
120	1
124	0
129	2
133	0
136	0
137	0
140	0
141	0
145	2
149	0
152	0

Value of D	Value of $N(D, 6)$
156	0
157	0
161	0
165	0
168	0
172	2
173	0
177	0
181	0
184	2
185	0
188	0
197	0
201	2
204	0
205	0
209	0
213	0
217	0
220	0
221	0
229	0
232	2
236	0
237	0
248	0
249	0
253	0
257	0
264	0
268	2
269	0
273	0
277	0
280	0
284	0
285	0
293	0
296	0
301	0
305	0
309	0
312	0
316	0
317	0

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 28 = 4 \cdot 7$ for the following values of D :

Value of D	Value of $N(D, 7)$
5	0
8	2
12	0
13	0
17	0
21	1
24	0
28	0
29	2
33	0
37	2
40	0
41	0
44	0
53	2
56	0
57	2
60	0
61	0
65	0
69	0
73	0
76	0
77	0
85	0
88	0
89	0
92	0
93	2
101	0
104	0
105	0
109	2
113	2
120	0
124	0
129	0
133	1
136	0
137	2
140	0
141	2
145	0
149	2
152	0

Value of D	Value of $N(D, 7)$
156	0
157	0
161	0
165	0
168	1
172	0
173	0
177	2
181	0
184	0
185	0
188	0
197	2
201	0
204	0
205	0
209	0
213	0
217	1
220	0
221	0
229	0
232	2
236	0
237	0
248	0
249	2
253	0
257	0
264	0
268	0
269	0
273	0
277	2
280	0
284	0
285	0
293	0
296	2
301	0
305	0
309	2
312	0
316	0
317	2

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 32 = 4 \cdot 8$ for the following values of D :

Value of D	Value of $N(D, 8)$
5	0
8	1
12	0
13	0
17	4
21	0
24	0
28	1
29	0
33	0
37	0
40	0
41	4
44	0
53	0
56	1
57	0
60	0
61	0
65	0
69	0
73	4
76	0
77	0
85	0
88	0
89	4
92	1
93	0
101	0
104	0
105	0
109	0
113	4
120	0
124	1
129	0
133	0
136	1
137	4
140	0
141	0
145	0
149	0
152	0

Value of D	Value of $N(D, 8)$
156	0
157	0
161	4
165	0
168	0
172	0
173	0
177	0
181	0
184	1
185	0
188	1
197	0
201	0
204	0
205	0
209	0
213	0
217	4
220	0
221	0
229	0
232	0
236	0
237	0
248	1
249	0
253	0
257	2
264	0
268	0
269	0
273	0
277	0
280	0
284	1
285	0
293	0
296	0
301	0
305	0
309	0
312	0
316	1
317	0

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 36 = 4 \cdot 9$ for the following values of D :

Value of D	Value of $N(D, 9)$
5	1
8	1
12	1
13	3
17	1
21	1
24	1
28	3
29	1
33	1
37	3
40	3
41	1
44	1
53	1
56	1
57	1
60	1
61	3
65	1
69	1
73	3
76	3
77	1
85	3
88	3
89	1
92	1
93	1
101	1
104	1
105	1
109	3
113	1
120	1
124	3
129	1
133	3
136	1
137	1
140	1
141	1
145	1
149	1
152	1

Value of D	Value of $N(D, 9)$
156	1
157	3
161	1
165	1
168	1
172	3
173	1
177	1
181	3
184	3
185	1
188	1
197	1
201	1
204	1
205	1
209	1
213	1
217	3
220	3
221	1
229	1
232	3
236	1
237	1
248	1
249	1
253	3
257	1
264	1
268	3
269	1
273	1
277	3
280	3
284	1
285	1
293	1
296	1
301	3
305	1
309	1
312	1
316	1
317	1

Number of classes of solutions of the equation
 $u^2 - Dv^2 = 40 = 4 \cdot 10$ for the following values of D :

Value of D	Value of $N(D, 10)$
5	0
8	0
12	0
13	0
17	0
21	0
24	2
28	0
29	0
33	0
37	0
40	1
41	4
44	0
53	0
56	0
57	0
60	1
61	0
65	2
69	0
73	0
76	0
77	0
85	0
88	0
89	4
92	0
93	0
101	0
104	2
105	0
109	0
113	0
120	0
124	2
129	4
133	0
136	0
137	0
140	0
141	0
145	0
149	0
152	0

Value of D	Value of $N(D, 10)$
156	2
157	0
161	0
165	0
168	0
172	0
173	0
177	0
181	0
184	0
185	2
188	0
197	0
201	4
204	0
205	0
209	0
213	0
217	0
220	0
221	0
229	0
232	0
236	0
237	0
248	0
249	4
253	0
257	0
264	0
268	0
269	0
273	0
277	0
280	0
284	2
285	0
293	0
296	2
301	0
305	0
309	0
312	0
316	0
317	0

Bibliography

- [1] Saban Alaca and Kenneth S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, to appear.
- [2] Ezra Brown, *Class Numbers of Real Quadratic Number Fields*, Trans. Amer. Math. Soc., 190 (1977), 99-107.
- [3] S. Chowla, *On the inequality $|x^2 - y^2 - 2xyk| \geq 2k$ (x, y, k odd)*, Norske Vid. Selsk. Forh. (Trondheim) 34 (1961), 91.
- [4] Harvey Cohn, *Advanced Number Theory*, Dover Publications, New York, 1980.
- [5] L. E. Dickson, *Introduction to the Theory of Numbers*, Dover Publications, Inc., New York, 1957.
- [6] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 2nd ed., John Wiley and Sons, 1999.
- [7] W. Feit, *Some diophantine equations of the form $x^2 - py^2 = z$* , Proc. Amer. Math. Soc. 129 (2000), 623-625.
- [8] George A. Grätzer, *First Steps in LaTeX*, Birkhauser, Boston Mass., 1999.
- [9] E. Grosswald, *Topics from the Theory of Numbers*, Macmillan Co., New York, 1966.
- [10] C. U. Jensen, *On the solvability of a certain class of non-Pellian equations*, Math. Scand. 10 (1962), 71-84.
- [11] Pierre Kaplan and Kenneth S. Williams, *Pell's equations $X^2 - mY^2 = -1, -4$ and continued fractions*, J. Number Theory 23 (1986), 169-182.

- [12] Pierre Kaplan and Kenneth S. Williams, *Infrastructure of ambiguous classes and the equations $x^2 - Dy^2 = \pm 4k$ for $D = L^2 + 4kM^2$* , submitted for publication.
- [13] Al Kelly and Ira Pohl, *C by dissection*, Addison-Wesley, 1996.
- [14] Ramanujachary Kumanduri and Christina Romero, *Number Theory with Computer Applications*, Prentice Hall, 1998.
- [15] R. A. Mollin and A. J. van der Poorten, *Halfway to a solution of $x^2 - Dy^2 = -3$* , J. Théor. Nombres Bordeaux 6 (1994), 421-457.
- [16] Habib Muzaffar and Kenneth S. Williams, *A restricted Epstein zeta function and the evaluation of some definite integrals*, Acta Arith. 104 (2002), 23-65.
- [17] Trygve Nagell, *Bemerkung über die Diophantische Gleichung $u^2 - Dv^2 = C$* , Arch. Math. 3 (1952), 8-9.
- [18] Trygve Nagell, *Introduction to Number Theory*, Chelsea Pub. Co., New York Inc., 1964.
- [19] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, Inc., 1991.
- [20] Bernard Oriat, *Groupes des classes des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$, $d < 10000$* , Faculté des Sciences de Besançon.
- [21] Paulo Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, New York, 2001.
- [22] A. Schinzel and W. Sierpiński, *On the equation $x^2 - 2y^2 = k$* , Wiadom. Mat. 7 (1964), 229-232. (Polish)
- [23] W. Sierpiński, *Elementary Theory of Numbers*, Warsaw, Poland, 1964.
- [24] Ian Stewart and David Tall, *Algebraic Number Theory*, 3rd ed., Chapman and Hall, New York, 2001.
- [25] B. Stolt, *On the Diophantine equation $u^2 - Dv^2 = \pm 4N$* , Ark. Mat. 2 (1952), 1-23.
- [26] B. Stolt, *On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, II*, Ark. Mat. 2 (1952), 251-268.

- [27] P. G. Walsh, *On a question of Kaplansky*, Amer. Math. Monthly 109 (2002), 660-661.