DISCRETE FRACTIONAL INTEGRAL OPERATORS AND THEIR RELATIONS TO NUMBER THEORY

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in Mathematics

by
Ezgi SERT

July 2018
İzmir

We approve the thesis of **Ezgi SERT**

Examining Committee Members:

Asst. Prof. Dr. Faruk TEMUR
Department of Mathematics, İzmir Institute of Technology

Assoc. Prof. Dr. Salahattin ÖZDEMİR
Department of Mathematics, Dokuz Eylül University

Prof. Dr. Engin BÜYÜKAŞIK
Department of Mathematics, İzmir Institute of Technology

06 July 2018

Asst. Prof. Dr. Faruk TEMUR
Supervisor, Department of Mathematics
İzmir Institute of Technology

Prof. Dr. Engin BÜYÜKAŞIK
Head of the Department of
Mathematics

Prof. Dr. Aysun SOFUOĞLU
Dean of the Graduate School of
Engineering and Sciences

ACKNOWLEDGMENTS

I would like to express my deepest and warm gratitude to my supervisor, Asst. Prof. Dr. Faruk Temur, for all his helpful comments and discussions. I have learned so much from our study together. I would not succeed without his motivating talks, guidance, patience, encouragement and kind cooperation throughout my thesis. I will always remain indebted to him.

I am grateful to Prof. Dr. Engin Büyükaşık who helps me so much, has put up with all my never ending questions, and has supported me throughout my undergraduate and master degree education.

I would like to thank to Assoc. Prof. Dr. Salahattin Özdemir for participating in my thesis committee.

I am grateful to my colleagues; Anıl Kolay, Merve Özvatan, and Esma Dirican for their unconditional help and encouragement.

Finally, I want to thank my family for their endless support and looking for my happiness.

ABSTRACT

DISCRETE FRACTIONAL INTEGRAL OPERATORS AND THEIR RELATIONS TO NUMBER THEORY

The aim of this thesis is to get estimates on discrete fractional integral operators by using number theory. These operators, starting with the studies of Arkipov and Oskolkov, have been investigated for a long time. Fourier analysis and topics related to it have been used in these studies. However, this study will put forward new results on these operators with the help of arithmetic.

ÖZET

AYRIK KESİRLİ İNTEGRAL OPERATÖRLERİ VE SAYI TEORİSİYLE İLİŞKİLERİ

Bu tezin amacı sayılar teorisini kullanarak ayrık kesirli integral operatörleri hakkında eşitsizlikler elde etmektir. Bu operatörler Arkipov ve Oskolkov'un çalışmalarından beri incelenmektedir. Fourier analizi ve ilgili konular bu çalışmalarda kullanılmaktadır. Ancak, bu çalışma aritmetiğin yardımıyla operatörler hakkında yeni sonuçlar elde edecektir.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Let $f : \mathbb{Z}^l \to \mathbb{C}$ be a function and $P : \mathbb{Z}^{k+l} \to \mathbb{Z}^l$ a polynomial having integer coefficients. Discrete fractional integral operator is defined by

$$\mathcal{I}_\lambda f(n) = \sum_{m \in \mathbb{Z}_*^k} \frac{f(P(m,n))}{|m|^{\lambda k}}, \tag{1.1}$$

where $\mathbb{Z}_*^k = \mathbb{Z}^k - \{0\}$ and λ is positive. $P(m,n)$ is called the phase polynomial of $\mathcal{I}_\lambda f(n)$.

We will consider integral binary quadratic forms as phase polynomials

$$q(m,n) = am^2 + bmn + cn^2. \tag{1.2}$$

The discriminant of q is defined by $\Delta := b^2 - 4ac$. The form is called definite when $\Delta < 0$, and indefinite when $\Delta > 0$. If $\Delta < 0$ and $a > 0$, then we say that q is a positive definite form. If the greatest common divisor of coefficients of q is 1, q is called primitive. We say that k is represented by the form q when $q(m,n) = k \in \mathbb{Z}$.

The main idea of this thesis is that we want to obtain estimates on certain discrete fractional integral operators by using number theory, and thus develop the theory of discrete fractional integrals.

We state our theorems for both positive definite forms and indefinite forms, but their proofs will be shown in chapter 5 and chapter 6.

Theorem 1.1 *Let $f \in l^p(\mathbb{Z})$ where $1 \le p \le \infty$ and q a positive definite integral binary quadratic form with discriminant Δ. Then the operator*

$$\mathcal{I}_\lambda f(n) = \sum_{m \in \mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda}$$

satisfies $\|\mathcal{I}_\lambda f\|_p \le C_{p,\lambda,\Delta}\|f\|_p$. It is valid for $\lambda > 1 - \frac{1}{p}$ when p is finite, and it is available for $\lambda > 1$ when p is infinite. It follows from this result that we have a sharpness part in *the following sense.*

- *For $p = 1$ and $r \in \mathbb{N}$, there is a form q and a function f such that $\|\mathcal{I}_{\log^r} f\|_1 = \infty$, where*

$$\mathcal{I}_{log^r} f(n) = \sum_{m \in \mathbb{Z}_*} \frac{f(q(m,n))}{\log^r(1+|m|)}$$

- *For $1 < p < \infty$, there is a form q and a function f such that $\|\mathcal{I}_\lambda f\|_p = \infty$, where $\lambda = 1 - \frac{1}{p}$.*

- *For $p = \infty$, there is a form q and a function f such that $\|\mathcal{I}_\lambda f\|_\infty = \infty$, where $\lambda = 1$.*

Theorem 1.2 *Let $f \in l^p(\mathbb{Z})$ where $1 \leq p \leq \infty$ and q an indefinite integral binary quadratic form with non-square discriminant Δ. Then the operator*

$$\mathcal{I}_\lambda f(n) = \sum_{m \in \mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda}$$

satisfies $\|\mathcal{I}_\lambda f\|_p \leq C_{p,\lambda,\Delta}\|f\|_p$. It is valid for $\lambda > 1 - \frac{1}{p}$ when p is finite, and it is available for $\lambda > 1$ when p is infinite. It follows from this result that we have a sharpness part in the following sense.

- *For $p = 1$ and $r \in \mathbb{N}$, there is a form q and a function f such that $\|\mathcal{I}_{\log^r} f\|_1 = \infty$, where*

$$\mathcal{I}_{log^r} f(n) = \sum_{m \in \mathbb{Z}_*} \frac{f(q(m,n))}{\log^r(1+|m|)}$$

- *For $1 < p < \infty$, there is a form q and a function f such that $\|\mathcal{I}_\lambda f\|_p = \infty$, where $\lambda = 1 - \frac{1}{p}$.*

- *For $p = \infty$, there is a form q and a function f such that $\|\mathcal{I}_\lambda f\|_\infty = \infty$, where $\lambda = 1$.*

In chapter 2, we briefly summarize the history of discrete analogues in harmonic analysis within the context of singular integrals, before dealing with the theory of discrete fractional integral operators by using number theory. We define the notation and terminology that will be used later. We state some essential results concerning these operators proved by Arkipov and Oskolkov, Stein, Wainger, Oberlin and Ionescu. After giving information on the general idea of these operators, we concentrate on our main operator $\mathcal{I}_\lambda f(n)$. We explain the reason why we study the number theory of the representation of an integer by a polynomial instead of using methods of the previous works. We prove that Theorem 1.2 fails when the discriminant is a square number, and that our results are sharp.

In chapter 3, we are concerned with the representation problem over the field of real numbers. This study is of great importance to understand the structure of binary quadratic forms over the ring of integers. We divide this study into two parts: first we study positive definite quadratic forms, and then indefinite quadratic forms of non-square discriminant. In both cases, we study the curves obtained from the solutions of these quadratic forms to prove a lemma about the distribution of representations of integers. These results will be useful for our main theorems.

In chapter 4, we deal with the number theory of quadratic forms by utilizing results uncovered by Gauss, Dirichlet, Jacobi and Pall. We want to understand the set of all representations of integer k by the form q defined by

$$R_k := \{(m,n) \in \mathbb{Z}^2 : q(m,n) = k\}.$$

To prove our main theorems, we need to find an upper bound on the cardinality of R_k. We will focus on obtaining this bound. Therefore, we explain how the number theoretical information is extracted and how to get estimates on the sets R_k.

In chapter 5, Theorem 1.1 will be proved with the help of the analytic, geometric and arithmetic information about positive definite forms. Furthermore, we give certain forms and certain functions that will serve as counterexamples for the sharpness parts of the Theorem 1.1.

In chapter 6, Theorem 1.2 will be shown by using the ideas and results obtained from chapter 2 and chapter 3. We start with the specific case in which $q = [a, b, c]$ is primitive and $b = 0$. Then, we investigate any indefinite form. Moreover, we describe our counterexamples for the sharpness parts of the Theorem 1.2.

In Conclusion, we give the main points of our new results obtained in this thesis.

CHAPTER 2

PRELIMINARIES

In this chapter, we briefly explain the history of discrete analogues in harmonic analysis by summarizing the history of singular integrals, before understanding the theory of discrete fractional integral operators with the help of arithmetic. These discrete operators have been studied as analogues of their continuous counterparts for almost a century. First of all, M. Riesz showed that the Hilbert transform

$$\mathcal{H}f(x) = p.v.\frac{1}{\pi}\int_{\mathbb{R}} \frac{f(x-t)}{t}dt = \lim_{\epsilon\to 0}\int_{|t|>\epsilon}\frac{f(x-t)}{t}dt$$

is bounded on $l^p(\mathbb{R})$ for all $1 < p < \infty$. Riesz also proved that the boundedness of the Hilbert transform gives rise to the boundedness of its discrete analogue

$$\mathcal{H}f(n) = \sum_{m\in\mathbb{Z}_*}\frac{f(n-m)}{m}$$

on $l^p(\mathbb{Z})$ for all $1 < p < \infty$ where $\mathbb{Z}^k_* = \mathbb{Z}^k - \{0\}$.

Definition 2.1 *$K : \mathbb{R}^n - \{0\} \to \mathbb{C}$ is called a Calderon-Zygmund kernel if the following conditions are satisfied:*

1. *$|K(x)| \leq C|x|^{-n}$ for some $C \in \mathbb{R}$. (size condition)*
2. *$\int_{r<|x|<R} K(x)dx = 0$ for all $0 < r < R < \infty$. (cancellation condition)*
3. *$\int_{|x|>y} |K(x-y) - K(x)|dx \leq C$ when $|y| > 0$ and a fixed C. (Hörmander condition)*

Calderon and Zygmund extended the Riesz's works. They proved that

$$\mathcal{T}f(x) = p.v.\int_{\mathbb{R}^k} f(x-y)K(y)dt,$$

where K is the Calderon-Zygmund kernel, is a bounded operator on $l^p(\mathbb{R}^k)$ for all $1 < p < \infty$. As a result of this, they showed that the discrete analogue

$$\mathcal{T}f(n) = \sum_{m\in\mathbb{Z}^k_*} f(n-m)K(m),$$

is also bounded with the same range. The maximal function, which is the largest average over sets belonging to given collection, is an essential operator for harmonic analysis subjects such as the existence almost everywhere of limits and the differentiability of functions. One of the most significant of maximal functions is the Hardy-Littlewood maximal function defined by

$$\mathcal{M}f(x) = \sup \frac{1}{V(B_r)} \int_{|y|<r} |f(x-y))|dy,$$

where $V(B_r)$ is the volume of the ball B_r with radius r in $\mathbb{R}^k$. As for its discrete analogue,

$$\mathcal{M}f(n) = \sup \frac{1}{\#B_r} \sum_{|m|<r} |f(n-m))|,$$

where $\#B_r$ is the number of integer lattice points in the ball B_r [1]. After looking at these operators from historical point of view, we can investigate our main operator.

We let f be a function from $\mathbb{Z}^l$ to $\mathbb{C}$ and $P : \mathbb{Z}^{k+l} \to \mathbb{Z}^l$ a polynomial having integer coefficients. **Discrete fractional integral operator** is defined by

$$\mathcal{I}_\lambda f(n) = \sum_{m\in\mathbb{Z}^k_*} \frac{f(P(m,n))}{|m|^{\lambda k}},$$

where λ is positive. $P(m,n)$ is called **the phase polynomial of $\mathcal{I}_\lambda f(n)$**. When the phase polynomial is $n-m$, this operator, as far as boundedness is concerned, is the same as its continuous counterpart. For the continuous analogue boundedness is given by the Hardy-Littlewood-Sobolev theorem. This theorem states that

$$\tau_\lambda f(x) = \int_{\mathbb{R}^k} \frac{f(x-y)}{|\ y\ |^{k\lambda}} dy$$

is a bounded operator from $l^p(\mathbb{R}^k)$ to $l^q(\mathbb{R}^k)$ for all $1 < p < q < \infty$ and $0 < \lambda < 1$ with $\frac{1}{q} = \frac{1}{p} - (1-\lambda)$. For its discrete analogue,

$$\tau_\lambda f(n) = \sum_{m \in \mathbb{Z}_*^k} \frac{f(n-m)}{|\, m \,|^{k\lambda}}$$

τ_λ is bounded for all $1 < p < q < \infty$ with $\frac{1}{q} \leq \frac{1}{p} - (1-\lambda)$. This τ_λ is the simplest discrete fractional operator. However, when $P(m,n)$ is of a higher degree, it will be seen that the boundedness properties for the discrete analogues may hold for a larger range.

We now turn to **discrete singular Radon transforms** defined by

$$\mathcal{R}f(n) = \sum_{m \in \mathbb{Z}_*^k} f(P(m,n))K(m). \tag{2.1}$$

Arkipov and Oskolkov were the first to study these operators. The operators at issue have been investigated over the last 30 years. If the phase polynomial is $n - Q(m)$ where Q is a polynomial from $\mathbb{Z}^k$ to $\mathbb{Z}^l$, then this operator is called **translation invariant**. In that case, operator commutes with translation as follows. Let us define our translation operator $\mathcal{T}_k f = g(n) = f(n+k)$ for some functions g and f translated by k. For commutativity with translation, we need to show that $\mathcal{R}\mathcal{T}_k f = \mathcal{T}_k \mathcal{R} f$.

$$\begin{aligned}
\mathcal{R}\mathcal{T}_k f = \mathcal{R}g &= \sum_{m \in \mathbb{Z}_*^k} g(n-m)K(m) \\
&= \sum_{m \in \mathbb{Z}_*^k} f((n+k)-m)K(m) \\
&= \mathcal{R}f(n+k) \\
&= \mathcal{T}_k \mathcal{R} f.
\end{aligned}$$

Translation invariant case is studied by Fourier multipliers, and significant progress has been made using this technique. We have an example for this case, which firstly was investigated by Arkipov and Oskolkov in [2]. They found that if in (2.1) we have $m \in \mathbb{Z}_*$, $K(m) = 1/m$, $P(m,n) = n - Q(m)$, and then if we regard n as a continuous variable in $\mathbb{R}$, then taking the Fourier transform

$$\begin{aligned}
\widehat{\mathcal{R}f}(\xi) &= \sum_{m \in \mathbb{Z}_*} \frac{\hat{f}(\xi) e^{-2\pi i Q(m)\xi}}{m} \\
&= \hat{f}(\xi) \sum_{m \in \mathbb{Z}_*} \frac{e^{-2\pi i Q(m)\xi}}{m} \qquad (2.2)
\end{aligned}$$

The term given by the sum is called a multiplier in Fourier analysis. It acts on a function by changing its Fourier transform. For example, translation operator is a multiplier. The multiplier in (2.2) is $l^\infty(\mathbb{Z})$, and thus $\mathcal{R}f(n)$ is bounded on $l^2(\mathbb{Z})$ as shown [2]. We give some important results obtained on the operators as the following:

- Stein and Wainger [3, 4], Oberlin [5] and Ionescu and Wainger [6] proved that $\mathcal{I}_\lambda$: $l^p(\mathbb{Z}) \to l^q(\mathbb{Z})$ is bounded for $0 < \lambda < 1$ and $P(m, n) = n - m^2$ if and only if p, q satisfy

$$\frac{1}{q} \leq \frac{1}{p} - \frac{1}{2}(1-\lambda), \qquad \frac{1}{q} < \lambda,\ \frac{1}{p} > (1-\lambda)$$

- Ionescu and Wainger [6] showed that $\mathcal{R}f(n)$ is a bounded operator on $l^p(\mathbb{Z}^k)$ for all $1 < p < \infty$ if $P(m, n) = n - Q(m)$.
- When $P(m, n) = n - m^s$ with $s > 2$, sharp results are not available for $\mathcal{I}_\lambda$.

We will develop the theory of certain discrete fractional integral operators, which were not considered in these works. We shall consider binary quadratic forms over the ring of integers

$$q(m, n) = am^2 + bmn + cn^2.$$

When $q(m, n) = k$ for some integer k, we say that k is represented by the form q. The set of all representations of k by q is defined by

$$R_k := \{(m, n) \in \mathbb{Z}^2 : q(m, n) = k\}. \tag{2.3}$$

When considering the same form q over the real numbers, we will utilize the set

$$S_w := \{(x, y) \in \mathbb{R}^2 : q(x, y) = w\}. \tag{2.4}$$

The discriminant of q is $\Delta = b^2 - 4ac$. If $\Delta < 0$, q is called a **definite form**. It takes positive and negative values if $\Delta > 0$. Such forms are called **indefinite**. When Δ is negative, it is obvious that ac is positive. It can be concluded that a and c have the same sign. We observe that

$$ax^2 + bxy + cy^2 = w \iff 4a^2x^2 + 4abxy + 4acy^2 = 4aw, \tag{2.5}$$

and completing of squares gives

$$4aw = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - \Delta y^2. \tag{2.6}$$

Similarly, this can be done for the same form by multiplying both sides by $4c$. It follows from (2.6) that the values that definite forms take have the sign of a. If $\Delta < 0$ and $a > 0$, then the form is nonnegative for any m and n. Such forms are called **positive definite forms**. If $\Delta < 0$ and $a < 0$, then these forms are called **negative definite forms**.

A form q is called **primitive** if the greatest common divisor of the coefficients of q is 1. If m and n are coprime, then (m, n) is called a **proper representation** of k. If m and n are not coprime, then it is called an **improper representation**. With the help of the coprimality, we can find remarkable results which enable us to understand the structure of proper representations. Therefore, we define the set of all proper representations of k by q

$$R'_k := \{(m, n) \in \mathbb{Z}^2 : q(m, n) = k \quad \text{and} \quad gcd(m, n) = 1\}. \tag{2.7}$$

We will use the notation $\#A$ which denotes the cardinality of the set A.

We prove that Theorem 1.2 fails when Δ is a square discriminant. To see this, let $q(m, n)$ be a form with square discriminant. That is to say, $\Delta = d^2$, $d \in \mathbb{N} \cup \{0\}$. When $c \neq 0$, $(2cj, (-b \pm dj)) \in \mathbb{Z}^2$ for any $j \in \mathbb{Z}$. If we plug them into q, then the results will be 0. Hence, we consider a function

$$f(k) = \begin{cases} 1 & \text{if } k \text{ is } 0 \\ 0 & \text{if } k \text{ is not } 0. \end{cases} \tag{2.8}$$

When we take the $l^1(\mathbb{Z})$ norm of $\mathcal{I}_\lambda f$

$$
\begin{aligned}
\|\mathcal{I}_\lambda f\|_{l^1(\mathbb{Z})} &= \sum_{n\in\mathbb{Z}} \left| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \right| \\
&= \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \\
&\geq \sum_{j\in\mathbb{Z}_*} \frac{f(q(2cj,(-b\pm d)j))}{|2cj|^\lambda} \\
&= \sum_{j\in\mathbb{Z}_*} \frac{1}{|2cj|^\lambda},
\end{aligned}
$$

and the last sum is clearly divergent for $\lambda \leq 1$. When $c = 0$, we have $q(m,n) = am^2 + bmn$ and $(bj, -aj) \in \mathbb{Z}^2$ for all $j \in \mathbb{Z}$. If we plug them into q, we will have 0. We assume $b \neq 0$ with f as in (2.8). Then

$$
\begin{aligned}
\|\mathcal{I}_\lambda f\|_{l^1(\mathbb{Z})} &= \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \\
&\geq \sum_{j\in\mathbb{Z}_*} \frac{f(q(bj,-aj))}{|2bj|^\lambda} \\
&\geq \sum_{j\in\mathbb{Z}_*} \frac{1}{|2bj|^\lambda},
\end{aligned}
$$

and this result diverges for $\lambda \leq 1$. When b and c are both zero, we have $a \neq 0$ and $q(m,n) = am^2$. In that case, we consider

$$
f(k) = \begin{cases} 1 & \text{if } k \text{ is } a \\ 0 & \text{if } k \text{ is not } a, \end{cases}
$$

and use the points $(1, j)$ for all $j \in \mathbb{Z}$. We obtain

$$
\begin{aligned}
\|\mathcal{I}_\lambda f\|_{l^1(\mathbb{Z})} &= \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \\
&\geq \sum_{j\in\mathbb{Z}_*} \frac{f(q(1,j))}{1^\lambda}.
\end{aligned}
$$

The last sum diverges as every summand has the same value 1. We will investigate $l^1(\mathbb{Z})$ estimates to understand our main theorems. Let f be a function in $l^1(\mathbb{Z})$, and

$$\mathcal{I}_\lambda f(n) = \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n)}{|m|^\lambda}$$

be our operator with any quadratic form $q(m,n) = am^2 + bmn + cn^2$. When we calculate $l^1(\mathbb{Z})$ norm of $\mathcal{I}_\lambda f$, we get

$$\|\mathcal{I}_\lambda f\|_{l^1(\mathbb{Z})} = \sum_{n\in\mathbb{Z}} \left| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \right| \leq \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{|f(q(m,n))|}{|m|^\lambda}.$$

We consider the sets $A_k := \{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : q(m,n) = k\}$ for each $k \in \mathbb{Z}$. These sets give us a partition of $\mathbb{Z}_* \times \mathbb{Z}$. Each element of $\mathbb{Z}_* \times \mathbb{Z}$ is in one of these sets A_k, and if k is different from l, then the sets $A_k \cap A_l$ are empty. Consequently,

$$= \sum_{(m,n)\in\mathbb{Z}_*\times\mathbb{Z}} \frac{|f(q(m,n))|}{|m|^\lambda} = \sum_{k\in\mathbb{Z}} |f(k)| \left(\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} \right).$$

Since $f \in l^1(\mathbb{Z})$, if we could prove that

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} \leq C,$$

where C is a constant not depending on k, we would get the estimate

$$\|\mathcal{I}_\lambda f\|_{l^1(\mathbb{Z})} \leq C\|f\|_{l^1(\mathbb{Z})}.$$

Hence, $l^1(\mathbb{Z})$ estimates motivate us to study the quantity

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda}. \tag{2.9}$$

This quantity obviously concerns the number of representations of k by q, and the structure and distribution of these representations. When the number of representations of k is small, the last sum will be bounded by a constant. This case will be used to prove

Theorem 1.1. On the other hand, when it is large or infinite, we will observe that the first coordinates of these representations increase fast. We will prove Theorem 1.2 by using this.

CHAPTER 3

GEOMETRY AND ANALYSIS OF BINARY QUADRATIC FORMS

In this part, we will concentrate on the representation problem over the field of real numbers. This study helps us understand the structure of binary quadratic forms over the ring of integers. We will consider the set S_w as defined by (2.4). This investigation gives rise to different results for positive definite forms and indefinite forms. We therefore investigate them separately.

3.1. Positive definite forms

In this section, we suppose that $q(x, y) = ax^2 + bxy + cy^2$ is positive definite. This means that a, c are positive and $-2\sqrt{ac} < b < 2\sqrt{ac}$. Needless to say, $q(x, y) = w$ is an ellipse that is centered at the origin. Since we have $4aw = (2ax + by)^2 - \Delta y^2$ from chapter 1, the set S_w is empty when w is negative. When $w = 0$, the set has only the origin. We therefore suppose that w is positive. We observe that S_w always includes the points $(\pm\sqrt{w/a}, 0), (0, \pm\sqrt{w/c})$ whatever the value of b is. We will see that the 4 lines passing through these points with slopes $\pm\sqrt{a/c}$ determine the behavior of S_w to a great extent. Although it is well-known that the ellipse encloses a convex region, we want to demonstrate this. Therefore, we want to prove that the region $(x, y) : q(x, y) \leq w$ is convex. Let (x_1, y_1), (x_2, y_2) be in this region, and let $z_1 = 2ax_1 + by_1$, $z_2 = 2ax_2 + by_2$. Then $z_i^2 - \Delta y_i^2 \leq 4aw$, $i = 1, 2$. Let $0 < r < 1$, and $(x_3, y_3) = r(x_1, y_1) + (1 - r)(x_2, y_2)$. If we let $z_3 = 2ax_3 + by_3$, then $z_3 = rz_1 + (1 - r)z_2$. Then we obtain

$$
\begin{aligned}
z_3^2 - \Delta y_3^2 &= (rz_1 + (1 - r)z_2)^2 - \Delta(ry_1 + (1 - r)y_2)^2 \\
&= r^2(z_1^2 - \Delta y_1^2) + (1 - r)^2(z_2^2 - \Delta y_2^2) \\
&+ 2r(1 - r)(z_1z_2 - \Delta y_1y_2) \\
&\leq 4aw(r^2 + (1 - r)^2) + r(1 - r)(z_1^2 + z_2^2 - \Delta(y_1^2 + y_2^2) \\
&= 4aw.
\end{aligned}
$$

This, as stated above, implies $q(x_3, y_3) \leq w$. Thus S_w is the curve bounding this convex region. By convexity, the region contains the parallelogram with vertices $(\pm\sqrt{w/a}, 0)$ and $(0, \pm\sqrt{w/c})$. The gradient of q is 0 when (x, y) is the origin which is not an element of S_w. This implies that S_w is a smooth plane curve for $w > 0$. We now want to write it as graphs of functions. We can solve the equation $ax^2 + bxy + cy^2 = w$ for y if and only if $x^2 \leq -4cw/\Delta$ holds, and we have two functions

$$y = f_1(x) = \frac{-bx + \sqrt{\Delta x^2 + 4cw}}{2c}, \quad y = f_2(x) = \frac{-bx - \sqrt{\Delta x^2 + 4cw}}{2c}.$$

It follows from the second derivative test that f_1 is concave and f_2 is convex. We can find dy/dx and dx/dy using implicit differentiation and setting these equal to zero allows us to find elements (x, y) of S_w for which x or y takes extremal values. We see that

$$\frac{dy}{dx} = -\frac{2ax + by}{bx + 2cy}, \quad \frac{dx}{dy} = -\frac{2cy + bx}{by + 2ax}.$$

Setting these equal to zero we obtain the lines with slopes $-2a/b$ and $-b/2c$. Thus the extremal values are attained when these lines intersect the curve S_w. We observe that for $b = 0$ these are the coordinate lines just as expected, and as $b \uparrow 2\sqrt{ac}$, or $b \downarrow -2\sqrt{ac}$ they get closer to each other, until at the limit they have slopes $-\sqrt{a/c}$ and $\sqrt{a/c}$ respectively. Let $b < 0$. The points of S_w on the line $y = \sqrt{a/c}x$ satisfy $ax^2 + b\sqrt{a/c}x^2 + ax^2 = w$, which implies $x^2 = w(2a + b\sqrt{a/c})^{-1}$. As b decreases to $-2\sqrt{ac}$, x^2 increases to infinity, and therefore y^2 increases to infinity. On the other hand points on the line $y = -\sqrt{c/a}x$ satisfy $x^2 = w(a - b\sqrt{c/a} + c^2/a)^{-1}$, and as b decreases to $-2\sqrt{ac}$, x^2 decreases to $wa/(a + c)^2$, and y^2 decreases to $wc/(a + c)^2$. Thus decreasing b to $-2\sqrt{ac}$ lengthens the set S_w in the direction of the line $y = \sqrt{a/c}x$, and shortens it in the direction of the line $y = -\sqrt{c/a}x$. Performing the same analysis for the case $b > 0$ shows that increasing b to $2\sqrt{ac}$ lengthens the set S_w in the direction of the line $y = -\sqrt{a/c}x$, and shortens it in the direction of the line $y = \sqrt{c/a}x$.

An arbitrary line in $\mathbb{R}^2$ has an equation either of the form $y = ux + v$ or $x = uy + v$ where $u, v \in \mathbb{R}$. When we plug x and y into $ax^2 + bxy + cy^2 = w$, we obtain respectively

$$x^2(cu^2 + bu + a) + x(2cuv + bv) + cv^2 = w,$$
$$y^2(au^2 + bu + c) + y(2auv + bv) + av^2 = w.$$

Since we investigate $\Delta < 0$, $(cu^2 + bu + a)$ and $(au^2 + bu + c)$ cannot be zero. Thus, we have at most 2 different (x, y) for each of these equations. That is, S_w can be intersected by a line at at most two points.

Lemma 3.1 *Let $q(x, y) = ax^2 + bxy + cy^2$ be a positive definite binary quadratic form, and let w be an integer. Then $q(x, y) = w$ has at most 4 solutions $(x, y) \in \mathbb{Z}^2$ satisfying*

$$|x| \leq \frac{|w|^{1/4}}{\sqrt{-\Delta}}. \tag{3.1}$$

Proof We want to obtain the solutions on the curve S_w defined by graphs of functions

$$y = f_1(x) = \frac{-bx + \sqrt{\Delta x^2 + 4cw}}{2c}, \quad y = f_2(x) = \frac{-bx - \sqrt{\Delta x^2 + 4cw}}{2c}$$

for $x^2 \leq -4cw/\Delta$. Any of them can be located on only one of these graphs. We observe that the lines

$$l_1(x) = -\frac{b}{2c}x + \sqrt{\frac{m}{c}}, \qquad l_2(x) = -\frac{b}{2c}x - \sqrt{\frac{m}{c}}$$

are tangent to f_1 at $\sqrt{w/c}$ and f_2 at $-\sqrt{w/c}$. We will show that they remain close to $l_1(x)$ and $l_2(x)$. When we look at the differences between $f_1(x)$, $f_2(x)$, and these lines for x satisfying (3.1), we can obtain the following:

$$\begin{aligned}
\sqrt{\frac{w}{c}} - \frac{\sqrt{\Delta x^2 + 4cw}}{2c} &= \Big(\frac{w}{c}\Big)^{1/2} - \Big(\frac{\Delta x^2}{4c^2} + \frac{w}{c}\Big)^{1/2} \\
&= \Big(\frac{\Delta x^2}{4c^2}\Big)\Big[\Big(\frac{\Delta x^2}{4c^2} + \frac{w}{c}\Big)^{1/2} + \Big(\frac{w}{c}\Big)^{1/2}\Big]^{-1} \\
&\leq \Big(-\frac{\Delta x^2}{4c^2}\Big)\Big[\frac{3}{2}\Big(\frac{w}{c}\Big)^{1/2}\Big]^{-1} \\
&= \frac{-\Delta x^2}{6c^{3/2}w^{1/2}} \\
&\leq \frac{1}{6c^{3/2}}.
\end{aligned}$$

It is understood from inequality that we can get these solutions satisfying $y = f_1(x)$ lie inside the set

$$S_1 = \Big\{(x, y) \in \mathbb{R}^2 : |x| \leq \frac{|w|^{1/4}}{\sqrt{-\Delta}}, \ \ |y - (-\frac{b}{2c}x + \sqrt{\frac{w}{c}})| \leq \frac{1}{6c^{3/2}}\Big\}$$

and $y = f_2(x)$ lie inside the set

$$S_2 = \left\{(x, y) \in \mathbb{R}^2 : |x| \le \frac{|w|^{1/4}}{\sqrt{-\Delta}},\ \ |y - (-\frac{b}{2c}x - \sqrt{\frac{w}{c}})| \le \frac{1}{6c^{3/2}}\right\}.$$

But, when (x, y) is in $\mathbb{Z}^2$, $2cy + bx = n$ is clearly in $\mathbb{Z}$. Hence, we can find n as

$$y = -\frac{b}{2c}x + \frac{n}{2c}.$$

Therefore, when considering the set of parallel lines

$$\left\{(x, y) \in \mathbb{R} : y = -\frac{b}{2c}x + \frac{n}{2c}\right\},$$

each member (x, y) in $\mathbb{Z}^2$ is contained on exactly one of these lines. However, we have at most one such line in each of the sets S_1 and S_2. Therefore, we conclude that there are at most 4 solutions. □

3.2. Indefinite forms of non-square discriminant

We suppose that $q(x, y) = ax^2 + bxy + cy^2$ is indefinite of non-square discriminant. We thus have $a \neq 0$ and $c \neq 0$. We shall suppose $c > 0$ and analyze the set S_w for each w. The case $c < 0$ follows by multiplying both sides -1. The sign of w plays an important role to understand the geometry of the set S_w.

Suppose that $w = 0$. Then $q(x, y) = ax^2 + bxy + cy^2 = 0$ has the solutions

$$y = l_1(x) = \frac{-b + \sqrt{\Delta}}{2c}x, \qquad y = l_2(x) = \frac{-b - \sqrt{\Delta}}{2c}x. \tag{3.2}$$

Hence, S_w has two lines passing through the origin. When considering the simple case $b = 0$, slopes obviously become $\pm\frac{\sqrt{\Delta}}{2c} = \pm\sqrt{|\frac{a}{c}|}$, which are additive inverses of each other. If $b < 0$, the directions of $l_1(x)$ and $l_2(x)$ will turn counterclockwise as $b \to -\infty$. On the other hand, if $b > 0$, the directions of $l_1(x)$ and $l_2(x)$ will turn clockwise as $b \to \infty$. We observe that these lines determine the graphs of the set S_w even when w is nonzero.

Suppose that $w > 0$. It is known that the set S_w forms a hyperbola centered at the origin, and clearly is a smooth plane curve. Then $q(x, y) = ax^2 + bxy + cy^2 = w$ has the solutions

$$y = f_1(x) = \frac{-bx + \sqrt{\Delta x^2 + 4cw}}{2c}, \qquad y = f_2(x) = \frac{-bx - \sqrt{\Delta x^2 + 4cw}}{2c}. \tag{3.3}$$

Since we have $cw > 0$, our functions are well-defined and also smooth for every $x \in \mathbb{R}$. It follows from the second derivative test that $f_1(x)$ is convex and $f_2(x)$ is concave. When $x > 0$, we obtain $f_1(x) > l_1(x)$, $f_2(x) < l_2(x)$, and when $x \leq 0$, we get $f_1(x) > l_2(x)$, $f_2(x) < l_1(x)$ similarly.

Since we have

$$\sqrt{\Delta x^2 + 4cw} - \sqrt{\Delta x^2} = 4cw(\sqrt{\Delta x^2 + 4cw} + \sqrt{\Delta x^2})^{-1} \tag{3.4}$$

the difference $\sqrt{\Delta x^2 + 4cw} - \sqrt{\Delta x^2}$ will be zero when $x^2 \to \infty$. This result means that as $x \to \infty$ we get $f_1(x) - l_1(x)$ goes to 0, $f_2(x) - l_2(x)$ goes to 0, and as $x \to -\infty$ we get $f_1(x) - l_2(x)$ goes to zero 0, $f_2(x) - l_1(x)$ goes to 0.

Suppose that $w < 0$. Then $q(x, y) = ax^2 + bxy + cy^2 = 0$ can be solved with respect to y if and only if $x^2 < -4cw/\Delta$, and solutions are

$$y = g_1(x) = \frac{-bx + \sqrt{\Delta x^2 + 4cw}}{2c}, \qquad y = g_2(x) = \frac{-bx - \sqrt{\Delta x^2 + 4cw}}{2c}.$$

It can be seen that $g_1(x)$ and $g_2(x)$ intersect only when $x^2 = -4cw/\Delta$. If $x > 0$, we get $l_2(x) < g_2(x) \leq g_1(x) < l_1(x)$ and if $x < 0$, we get $l_1(x) < g_2(x) \leq g_1(x) < l_2(x)$. Because of (3.4), when $x \to \infty$ we get $g_1(x) - l_1(x) \to 0$, $g_2(x) - l_2(x) \to 0$, and when $x \to -\infty$ we get $g_1(x) - l_2(x) \to 0$, $g_2(x) - l_1(x) \to 0$. With second derivative test we see that g_1 is convex and g_2 is concave for $x > \sqrt{-4cw/\Delta}$, and g_2 is convex and g_1 is concave for $x < -\sqrt{-4cw/\Delta}$. Then $q(x, y) = ax^2 + bxy + cy^2 = 0$ has the solutions

$$x = h_1(y) = \frac{-by + \sqrt{\Delta y^2 + 4aw}}{2a}, \qquad x = h_2(y) = \frac{-by - \sqrt{\Delta y^2 + 4aw}}{2a}.$$

Lemma 3.2 *Let $q(x,y) = ax^2+bxy+cy^2$ be an indefinite form of non-square discriminant, and let w be an integer. Then $q(x,y) = w$ has at most 4 solutions $(x,y) \in \mathbb{Z}^2$ satisfying*

$$|x| \leq \frac{|w|^{1/4}}{\sqrt{\Delta}}. \tag{3.5}$$

Proof We first assume $w = 0$. In this case the solution $(x,y) \in \mathbb{Z}^2$ we are looking for must satisfy $y = l_1(x) = \frac{-b+\sqrt{\Delta}}{2c}x$ and $y = l_2(x) = \frac{-b-\sqrt{\Delta}}{2c}x$, but since Δ is non-square, the only element of $\mathbb{Z}^2$ satisfying these lines is the origin. So there is only 1 solution in this case.

We suppose $w > 0$. Then solutions are located on the graphs of functions

$$y = f_1'(x) = \frac{-bx + \sqrt{\Delta x^2 + 4cw}}{2c}, \qquad y = f_2'(x) = \frac{-bx - \sqrt{\Delta x^2 + 4cw}}{2c},$$

and every solution can be only located on one of these graphs since our graphs do not intersect. The lines

$$y = l_1'(x) = -\frac{b}{2c}x + \sqrt{\frac{w}{c}}, \qquad y = l_2'(x) = -\frac{b}{2c}x - \sqrt{\frac{w}{c}},$$

are tangent to f_1' at $\sqrt{m/c}$, f_2' at $-\sqrt{m/c}$. We will show that they stay close to f_1', f_2' for x satisfying (3.5). When we look at the differences between $f_1'(x)$, $f_2'(x)$ and these lines for x satisfying (3.5), we can obtain a similar result as in Lemma 3.1

$$\frac{\sqrt{\Delta x^2 + 4cw}}{2c} - \sqrt{\frac{w}{c}} \leq \frac{1}{8c^{3/2}}.$$

This result enables us to consider the problem to the number of intersections S_w. Therefore, we can have at most 4 solutions with two lines.

We suppose $w < 0$. In that case we have $x^2 \geq -4cw/\Delta$. However, this gives rise to a contradiction due to our assumption Lemma 3.2. Thus, we have no solution. □

CHAPTER 4

ARITHMETIC OF QUADRATIC FORMS

We now want to understand the set R_k. Having understood that proving our theorems require finding an upper bound on the cardinality of R_k, we will concentrate upon finding such a bound. In the 19th and early 20th century, Gauss, Dirichlet, Pall and others made great contributions to this topic by using the theory of quadratic residues and the number of automorphs of q. In this chapter we will explain how this relation is established, and how to obtain an estimate on R_k.

We suppose that $q(m,n) = ax^2 + bxy + cy^2$ is a binary quadratic form. This form can be expressed as $q = [a,b,c]$ and written as a matrix

$$[q] := \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}.$$

Then we can easily get $\Delta = -\det[q]$. Let us consider a linear transformation

$$m = \alpha M + \beta N, \quad n = \gamma M + \delta N. \tag{4.1}$$

Indeed, we can write this transformation as a matrix

$$\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} M \\ N \end{bmatrix},$$

where α, β, γ, and δ are integers with $\alpha\delta - \beta\gamma \neq 0$. Then $q(m,n)$ is transformed into

$$Q(M,N) = AM^2 + BMN + CN^2, \tag{4.2}$$

where $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$, $B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$, $C = a\beta^2 + b\beta\delta + c\delta^2$. We will denote this transformation by T. Hence, we get $Tq = Q$.

Two quadratic forms q and Q are called **equivalent** if one of them can be changed to the other by a linear transformation of the form $m = \alpha M + \beta N$, $n = \gamma M + \delta N$, where α, β, γ, and δ are integers satisfying $\alpha\delta - \beta\gamma = \pm 1$. When the determinant of this matrix is 1, we will say that two equivalent forms are **properly equivalent**. Otherwise, they are called **improperly equivalent**. For both cases, since we have $q(m,n) = q(\alpha M + \beta N, \gamma M + \delta N) = Q(M,N)$, this implies that q and Q represent the same integers. Equivalent forms are denoted by the symbol "$\sim$". In this thesis, we will merely concentrate on properly equivalent forms. We sometimes say equivalent forms instead of saying properly equivalent forms. Furthermore, proper equivalence is an equivalence relation. To see this, we let $\alpha = \delta = 1$ and $\gamma = \beta = 0$. For a reflexive relation,

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix}.$$

To get symmetry,

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix}$$

transforms q into Q. Then

$$\begin{pmatrix} M \\ N \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

transforms Q into q.
To see transitivity, if

$$\begin{pmatrix} M \\ N \end{pmatrix} = \begin{pmatrix} \eta & \theta \\ \varsigma & \tau \end{pmatrix} \begin{pmatrix} m'' \\ n'' \end{pmatrix}$$

then transforms Q to Q', and then

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \eta & \theta \\ \varsigma & \tau \end{pmatrix} \begin{pmatrix} m'' \\ n'' \end{pmatrix} = \begin{pmatrix} \alpha\eta + \beta\varsigma & \alpha\theta + \beta\tau \\ \gamma\eta + \delta\varsigma & \gamma\theta + \delta\tau \end{pmatrix} \begin{pmatrix} m'' \\ n'' \end{pmatrix}$$

transforms q to Q'. Therefore, proper equivalance relation gives partition forms into equivalence class when a discriminant is given [7].

When we want to find all integer solutions of $m^2 + n^2 = 5$, we will see that this form is equivalent to $5m^2 + 6mn + 2n^2 = 5$, which comes from the transformation

$$[T] = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

In the same way, we can find infinitely many forms which are equivalent to $m^2 + n^2$. This example illustrates the reason why we investigate transformations and equivalent forms.

We can easily calculate that

$$[Q] = [T]^*[q][T]$$

where $[T]^*$ is the transpose of $[T]$. The determinant of $Q = (2a\alpha\beta + b\alpha\delta + b\gamma\beta + 2c\gamma\delta)^2 - 4(a\alpha^2 + b\alpha\gamma + c\gamma^2)(a\beta^2 + b\beta\delta + c\delta^2) = (b^2 - 4ac)(\alpha\delta - \beta\gamma)^2 = b^2 - 4ac$ is the same as the determinant of q.

We consider another matrix $[S]$ that also has determinant 1, and transforms q to Q. Then the inverse matrix $[S]^{-1}$ must transform Q to q, and so

$$[q] = [S]^{-1*}[Q][S]^{-1} = [S]^{-1*}[T]^*[q][T][S]^{-1} = ([T][S]^{-1})^*[q][T][S]^{-1}.$$

If a matrix which has determinant 1 leaves q unchanged, it is called an **automorph** of this form. Thus, $[T][S]^{-1}$ is an automorph of q. Let us denote $[A] := [T][S]^{-1}$. When $[A]$ is multiplied from the right hand side by $[S]$, we get $[T]$. Therefore, when we obtain a matrix which transforms q to an equivalent form Q, and multiply that matrix with the automorphs of q, we will find all matrices which have determinant 1 and transform q to Q.

On the one hand, we observe that if $\gcd(m, n) = g$, and $q(m, n) = k$ for some $g \in \mathbb{N}$ and $k \in \mathbb{Z}$, then we will get $\gcd(m/g, n/g) = 1$, and $q(m/g, n/g) = k/g^2$. On the other hand, if $\gcd(m,n) = 1$ with $q(m,n) = k/g^2$, then we have $\gcd(mg, ng) = g$ and $q(mg, ng) = k$. Improper representations of k with the greatest common divisor g are mapped bijectively to proper representations of k/g^2. In other words, this $(m,n) \mapsto (m/g, n/g)$ is a bijective map from the proper representations of k/g^2 to improper representations of k with the greatest common divisor g. Hence, when $k \neq 0$, we have

$$R_k = \bigcup_{g^2|k} g \cdot R'_{k/g^2}. \tag{4.3}$$

When $k = 0$, the set R_k contains the union in (4.3) and $(0,0)$.

We suppose $k \neq 0$ and investigate the structure of the proper representations R'_k. When we have a pair (α,γ) satisfying $q(\alpha,\gamma) = k$ and $\gcd(\alpha,\gamma) = 1$, we will get a pair β, δ satisfying $\alpha\delta - \gamma\beta = 1$. This relation comes from the property of coprimality. If we choose another pair β', δ' satisfying the same condition, then we get $\alpha\delta - \gamma\beta = \alpha\delta' - \gamma\beta'$. We take common parenthesis $\alpha(\delta' - \delta) = \gamma(\beta' - \beta)$. Since α and γ are coprime, either α or γ is nonzero. Suppose that $\alpha \neq 0$. It follows from the property of divisibility that α divides $\beta' - \beta$. Thus, we write $\beta' = \beta + t\alpha$ for some unique integer t. This gives rise to $\alpha(\delta' - \delta) = \gamma t\alpha$, and since $\alpha \neq 0$, we obtain $\delta' = \delta + t\gamma$. If $\gamma \neq 0$, we will get a unique integer t for the case α and γ such that

$$\beta' = \beta + t\alpha, \qquad \delta' = \delta + t\gamma. \tag{4.4}$$

On the other hand, for any integer t, we get unique β' and δ' written above and they also satisfy $\alpha\delta' - \gamma\beta' = 1$. Then we have the matrix

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

which has determinant 1, and transforms q to an equivalent form $Q = [k, u, v]$, where

$$k = a\alpha^2 + b\alpha\gamma + c\gamma^2, \;\; u = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \;\; v = a\beta^2 + b\beta\delta + c\delta^2. \tag{4.5}$$

Conversely, the matrix

$$\begin{bmatrix} \alpha & \beta' \\ \gamma & \delta' \end{bmatrix}$$

transforms q into the form $[k, u', v']$ satisfying

$$u' = 2a\alpha\beta' + b(\alpha\delta' + \beta'\gamma) + 2c\gamma\delta', \quad v' = a(\beta')^2 + b\beta'\delta' + c(\delta')^2. \tag{4.6}$$

When we write $\beta + t\alpha$, $\delta + t\gamma$ instead of β', δ' respectively, we have

$$\begin{aligned} u' &= 2a\alpha\beta' + b(\alpha\delta' + \beta'\gamma) + 2c\gamma\delta' \\ &= 2a\alpha(\beta + t\alpha) + b[\alpha(\delta + t\gamma) + (\beta + t\alpha)\gamma] + 2c\gamma(\delta + t\gamma) \\ &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta + 2t[a\alpha^2 + b\alpha\gamma + c\gamma^2] \\ &= u + 2tk. \end{aligned} \tag{4.7}$$

Thus, we find a unique pair β, δ where $0 \leq u < 2|k|$. As the form q and its equivalent form have the same discriminant, we obtain $u^2 - 4kv = \Delta$. Since k is different from 0 and u is given, we can get a unique v for this relation.

Hence, we find a one-to-one and onto correspondence between solutions u, v of the previous relations and solutions u satisfying

$$u^2 \equiv \Delta \pmod{4|k|}, \quad \text{and} \quad 0 \leq u < 2|k|. \tag{4.8}$$

Up to now, the outcome of our investigations is as follows: when we choose β and δ for a pair (α, γ) as shown, we have a unique matrix which has determinant 1 and transforming q to an equivalent form $Q = [k, u, v]$ where $u^2 \equiv \Delta \pmod{4|k|}$, and $0 \leq u < 2|k|$. It can be seen that our representations are mapped to matrices injectively. Then matrices are mapped to forms where $u^2 \equiv \Delta \pmod{4|k|}$, and $0 \leq u < 2|k|$. But, we see that the matrices

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{bmatrix}$$

are mapped to the same form. On the other hand, we have two possibilities for a form satisfying (4.8). One of these possibilities is that it is not equivalent to q, which means that we have no representation. The other case is that it is equivalent to q. When we find a matrix which transforms q to Q, and multiply this matrix with the automorphs of q, we will get this type of matrices and the first columns of these matrices are the representations related to Q. By doing so, we get a number of matrices for each form satisfying (4.8). When q is mapped by two matrices to distinct forms, these matrices must be different. On the other hand, when q is mapped by two matrices to the same form, this means that the automorphs will be the same. It follows from the last two arguments that any two of these matrices cannot be the same. Since we obtain $u' = u + 2tk$, the first columns of any two of matrices cannot be the same. Therefore, we conclude that the first columns of matrices are what we are looking for as proper representations.

We want to understand the cardinality and structure of solutions of (4.8). These two will help us obtain an upper bound for proper representation R'_k. Besides this, if we find each solution of (4.8) that is equivalent to q, we will completely obtain the number of proper representations.

Let p be an odd prime satisfying $\gcd(a, p) = 1$. When the congruence $x^2 \equiv a \pmod{p}$ has a solution, a is called a quadratic residue of p. Otherwise, it is called a quadratic non-residue of p. Assume that p is an odd prime and $\gcd(a, p) = 1$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

The Properties of The Legendre Symbol: Suppose that p is an odd prime with $gcd(a, p) = 1$, and $gcd(b, p) = 1$. Then we have the following properties:

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

3. $\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \pmod{p}$

4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Moreover, we give the most famous result proved by Fermat as follows: Let p be an odd prime. Then,

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

Indeed,

$$\left(\frac{-1}{p}\right) = 1 \quad \Leftrightarrow p = 4k + 1$$

Such tools will be importance to describe our counterexamples for Theorem 1.1 [8].

The number of solutions of (4.8) is contingent upon the relation between Δ and k. Dirichlet was the first person to calculate this when Δ and k are coprime [8]. The general case was shown by G. Pall [9, 10]. We now summarize some results of their studies. We write the number of solutions of (4.8) as;

$$\Gamma_t(s) = \#\{u : u^2 \equiv t \ (\text{mod } 4s), \quad 0 \leq u < 2s\}, \tag{4.9}$$

where for all $t \in \mathbb{Z}$ and $s \in \mathbb{N}$. Since we have $u^2 \equiv (u + 2ls)^2 \ (\text{mod } 4s)$, we obtain

$$\Gamma_t(s) = \frac{1}{2}\#\{u : u^2 \equiv t \ (\text{mod } 4s)\}. \tag{4.10}$$

When t is divided by 4, remainders must be 0, 1, 2, 3. The remainders 2, 3 cannot be obtained from a perfect square. We thus investigate the rest of remainders, which are 0 and 1. These remainders play an important role for us because all discriminants have these remainders when divided by 4. We easily see that $\Gamma_t(1) = 1$. Before we continue this, we will state the necessary knowledge of number of roots of a congruence.

Let $f(x)$ be a polynomial over the ring of integers defined by $f(x) = a_0x^r + a_1x^{(r-1)} + ... + a_r \equiv 0 \ (\text{mod } k)$ and not all coefficients divisible by k. If $f(l)$ is divisible by k for some $l \in \mathbb{Z}$, then l is called a root of the congruence [8].

Theorem 4.1 [8] If $m_1, ..., m_t$ are relatively prime in pairs and m is their product, the number of roots of $f(x) = a_0x^r + a_1x^{(r-1)} + ... + a_r \equiv 0 \ (\text{mod } m)$ is the product of the numbers of roots

$$f(x) \equiv 0 \ (\mathrm{mod}\ m_1), \ \ ..., \ \ f(x) \equiv 0 \ (\mathrm{mod}\ m_t) \ .$$

Theorem 4.2 [8] Let p be a prime not dividing c. If $p > 2$, the number of roots of

$$x^2 \equiv c \ (\mathrm{mod}\ p^n)$$

is the same as the number (0 or 2) of roots when $n = 1$. If $p = 2$, $n \geq 3$, there is no root or just four roots, according as $c \not\equiv 1$ or $c \equiv 1$ (mod 8). If $p = 2$, $n = 2$, there is no root or are two roots, according as $c \equiv 3$ or $c \equiv 1$ (mod 4).

Let us continue and analyze the prime factorization when $s = p_0^{a_0} p_1^{a_1} \dots p_j^{a_j}$ with $p_0 = 2$. With the help of Theorem 4.1,

$$\begin{aligned} \Gamma_t(s) &= \frac{1}{2}\#\{u : u^2 \equiv t \ (\mathrm{mod}\ p_0^{a_0+2} p_1^{a_1} \dots p_j^{a_j})\} \\ &= \frac{1}{2}\#\{u : u^2 \equiv t \ (\mathrm{mod}\ p_0^{a_0+2})\} \prod_{i=1}^{j} \#\{u : u^2 \equiv t \ (\mathrm{mod}\ p_i^{a_i})\}. \end{aligned} \tag{4.11}$$

Since we have $\Gamma_t(1) = 1$, we again use the Theorem 4.1 for positive i. Then we get

$$\begin{aligned} \Gamma_t(p_i^{a_i}) &= \frac{1}{2}\#\{u : u^2 \equiv t \ (\mathrm{mod}\ 4p_i^{a_i})\} \\ &= \frac{1}{2}\#\{u : u^2 \equiv t \ (\mathrm{mod}\ 4)\}\#\{u : u^2 \equiv t \ (\mathrm{mod}\ p_i^{a_i})\} \\ &= \#\{u : u^2 \equiv t \ (\mathrm{mod}\ p_i^{a_i})\}. \end{aligned} \tag{4.12}$$

Hence, we conclude

$$\Gamma_t(s) = \prod_{i=0}^{j} \Gamma_t(p_i^{a_i}). \tag{4.13}$$

We now need to calculate $\Gamma_t(p^a)$ for prime p and positive a. We easily get $\Gamma_t(p^a) = p^{\lfloor a/2 \rfloor}$ for $t = 0$. Otherwise, with the help of Theorem 4.2, we can obtain the outcomes, which are mostly related to divisibility properties between p and t. In 1931, G. Pall computed all outcomes in nine cases [9]. For these nine cases, we obtain an upper bound $\Gamma_t(p^a) \leq 2p^{\lfloor c/2 \rfloor}$, where c is the power of p as a factor of t. If $d(s) = (a_1 + 1)(a_2 + 1) \cdots (a_j + 1)$ is the number of positive divisors of s, it is possible to write $\Gamma_t(s) \leq d(s)\sqrt{|t|}$.

For any positive ε, we have $d(s) \leq C_\varepsilon s^\varepsilon$ [11]. Combining them, we conclude

$$\Gamma_t(s) \leq C_\varepsilon s^\varepsilon \sqrt{|t|}. \tag{4.14}$$

We focus on the number of automorphs. When we consider positive definite forms or indefinite forms with nonzero square discriminant, we have at most 6 automorphs [8, 9, 10]. This implies that we have an upper bound for the cardinality of R'_k by multiplying by 6 which comes from the number of automorphs of q. Therefore, we obtain

$$\#R'_k \leq 6C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|}. \tag{4.15}$$

We now can pass from R'_k to R_k because of the bijectivity relation using (4.3). Therefore,

$$\#R_k = \sum_{g^2|k} \#R'_{k/g^2} \leq 6d(|k|)C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|} \leq C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|}. \tag{4.16}$$

When we consider the cases when the discriminant is zero or positive non-square, it is known that there are infinitely many automorphs which are found by using the theory of Pell-like equations. Pell's equation is $x^2 - \Delta y^2 = 1$ in which Δ is a positive integer which is not a perfect square, and the equation $x^2 - \Delta y^2 = k$ is called Pell-like equation where k is an integer.

Theorem 4.3 [8] Every automorph

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

of a primitive, integral form [a, b, c] of discriminant $\Delta > 0$ has

$$\alpha = \frac{1}{2}(t - bu), \quad \beta = cu, \quad \gamma = au, \quad \delta = \frac{1}{2}(t + bu), \tag{4.17}$$

where t and u are integral solutions of

$$t^2 - \Delta u^2 = 4. \tag{4.18}$$

Conversely, if t and u are integral solutions of (4.18), the numbers (4.17) are integers and define an automorph.

Theorem 4.4 [8] Equation (4.18) has a solution with $u \neq 0$.

Let q be primitive. Since we assume positive non-square discriminant, it must be at least 5. According to Theorem 4.3, we find automorphs of q as stated. We see that $(\pm 2, 0)$ satisfy this equation, and we have no solution when $t = 0$. On account of Theorem 4.4, $t^2 - \Delta u^2 = 4$ has a solution with $t \neq 0, u \neq 0$. It is clear that $(-t, u), (t, -u), (-t, -u)$ also satisfy this equation when (t, u) is a solution of this equation. Thus, it is enough to obtain the positive solutions. When $(t, u), (t', u')$ are solutions, $t < t'$ leads to $u < u'$. This relation implies that (T, U) is a solution that is positive and minimum. We will call (T, U) the least positive solution of the equation. It can be easily seen that $U \geq 1$ and $T \geq 3$ since $\Delta \geq 5$.

Theorem 4.5 [8] For $\Delta > 0$, all sets of integral solutions t, u of (4.18) are given by

$$\frac{1}{2}(t + \sqrt{\Delta}u) = \pm[\frac{1}{2}(T + \sqrt{\Delta}U)]^k, \qquad (k = 0, \pm 1, \pm 2 \ldots), \tag{4.19}$$

where T, U give the least positive solution .

According to Theorem 4.5, we find all integer solutions of $t^2 - \Delta u^2 = 4$ given by

$$(t + \sqrt{\Delta}u) = i2^{-j+1}(T + \sqrt{\Delta}U)^j, \quad i = \pm 1, \quad j = 0, \pm 1, \pm 2 \ldots \tag{4.20}$$

and automorphs associated with our solutions defined by

$$i[A]^j, \quad i = \pm 1, \quad j = 0, \pm 1, \pm 2 \ldots \tag{4.21}$$

The matrix $[A]$ denotes the automorph associated with the least positive solution. We investigate the relation between these solutions and matrices. We have only solutions $(\pm 2, 0)$ with one entry 0 if we take $i = \pm 1$ and $j = 0$. If i, j are positive, then (t, u) will be a positive solution. We get a negative solution $(-t, -u)$ when we take entries $-i, j$. We have solutions $(t, -u)$ and $(-t, u)$ respectively if we consider entries $i, -j$ and $-i, -j$. As we have $(T + \sqrt{\Delta}U)/2 > 2$, distinct pairs of i, j lead to different solution (t, u), and thus we obtain a different solution coming from (4.20) for every pair of i, j. Since a and c are nonzero, and if $u \neq u'$, we obtain different automorphs. If $u = u'$ we must get $t \neq t'$. This result gives rise to different values on the diagonal of corresponding automorph matrices.

CHAPTER 5

THE CASE OF POSITIVE DEFINITE FORMS

The goal of this chapter is to prove the first theorem put forward in the introduction by using the analytic, geometric and arithmetic knowledge of positive definite quadratic forms as given in chapter 3 and chapter 4.

Proof Let us start with the basic step $p = \infty$. By using the norm of $l^\infty(\mathbb{Z})$,

$$\|\mathcal{I}_\lambda f\|_\infty = \sup_{n\in\mathbb{Z}} \Big| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^\lambda} \Big| \leq \|f\|_\infty \sum_{m\in\mathbb{Z}_*} \frac{1}{|m|^\lambda} = C_\lambda \|f\|_\infty.$$

We easily see that the constant only depends on λ, but not the form q. We turn to the case $p = 1$. In this case, we need to return to the analysis in chapter 2. Since we are concerned with the positive definite forms, we need our sets A_k for only positive integers k. We partition our sets A_k as follows

$$A'_k := \{(m,n) \in A_k : |m| \leq |k|^{1/4}(-\Delta)^{-1/2}\}, \qquad A''_k := A_k \setminus A'_k. \tag{5.1}$$

Then by using Lemma 3.1 , we get

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} = \sum_{(m,n)\in A'_k} \frac{1}{|m|^\lambda} + \sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda} \leq 4 + \sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda}.$$

When we replace ε in (4.16) by $\lambda/8$, we obtain an estimate for the cardinality of the set A''_k.

$$\sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda} \leq C_\lambda k^{\lambda/8} \sqrt{|\Delta|} k^{-\lambda/4} |\Delta|^{\lambda/2} = C_\lambda |\Delta|^{(\lambda+1)/2} k^{-\lambda/8} \leq C_{\lambda,\Delta}.$$

We conclude that

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^{\lambda}} \leq C_{\lambda,\Delta}.$$

We obtain

$$\|\mathcal{I}_{\lambda} f\|_1 \leq C_{\lambda,\Delta}\|f\|_1.$$

Our constant C depends on λ and Δ as seen.

When $1 < p < \infty$, our methods alter slightly from the previous case $p = 1$. By using the Hölder inequality, we introduce the partition sets A_k. Assume $\lambda' = \lambda - 1 + p^{-1}$. Then

$$\|\mathcal{I}_{\lambda} f\|_p^p = \sum_{n\in\mathbb{Z}} \Big| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^{\lambda}} \Big|^p \leq \sum_{n\in\mathbb{Z}} \Big(\sum_{m\in\mathbb{Z}_*} \frac{|f(q(m,n))|}{|m|^{\lambda'/2}} \frac{1}{|m|^{1-p^{-1}+\lambda'/2}} \Big)^p$$

When applying the Hölder inequality to the right hand side parenthesis, we obtain

$$\leq \sum_{n\in\mathbb{Z}} \Big[\sum_{m\in\mathbb{Z}_*} \frac{|f(q(m,n))|^p}{|m|^{\lambda' p/2}} \Big] \Big[\sum_{m\in\mathbb{Z}_*} \frac{1}{|m|^{1+\lambda' p/2(p-1)}} \Big]^{p-1}.$$

It follows from this inequality that the first parenthesis creates the sets A_k, and the second parenthesis gives rise to a constant. Therefore,

$$\leq C_{p,\lambda} \sum_{k\in\mathbb{N}} |f(k)|^p \sum_{(m,n)\in A_k} \frac{1}{|m|^{\lambda' p/2}}.$$

Then we obtain

$$\|\mathcal{I}_{\lambda} f\|_p \leq C_{p,\lambda,\Delta}\|f\|_p.$$

C depends on p, λ and Δ as shown.

Let us prove the sharpness part of this theorem. We now consider the case $p = \infty$. Let f be a nonzero constant function and q an arbitrary positive definite form. It is obvious that λ cannot be 1.

Suppose that $p = 1$. We firstly deal with the case $r = 1$. Later, we will handle any r for this case. We let $q(m,n) = m^2 + n^2$. Jacobi proved that the number of representations of k as a sum of two squares is $4d(k)$ when k is an odd positive integer and all prime factors of k are of the form $4z + 1$ [8]. The set A_k has at least $4d(k) - 2 \geq 2d(k)$ elements. Hence, when we look at the numbers $k_j := (5 \cdot 13)^j$, $j \in \mathbb{N}$, we get $\#A_{k_j} \geq 2(j+1)^2$. Taking logarithm, we get $j = \log k_j / \log 65$. Thus, we rewrite

$$\#A_{k_j} \geq \frac{2}{\log^2 65} \log^2 k_j.$$

Let us define

$$f(k) := \begin{cases} j^{-2} & \text{if } k = k_j \\ 0 & \text{otherwise} \end{cases}.$$

This function obviously is in $l^1(\mathbb{Z})$. However,

$$\begin{aligned} \|\mathcal{I}_{log} f\|_1 = \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{\log(1+|m|)} &= \sum_{k\in\mathbb{N}} f(k) \sum_{(m,n)\in A_k} \frac{1}{\log(1+|m|)} \\ &= \sum_{j\in\mathbb{N}} f(k_j) \sum_{(m,n)\in A_{k_j}} \frac{1}{\log(1+|m|)} \\ &\geq \sum_{j\in\mathbb{N}} j^{-2} \frac{2}{\log^2 65} \log^2 k_j \frac{1}{\log k_j} \\ &= \frac{2}{\log 65} \sum_{j\in\mathbb{N}} j^{-1}, \end{aligned}$$

and this will obviously be divergent. This argument can be applied for any r by considering a larger number of primes of the form $4z + 1$ rather than only $5, 13$. Let us consider the case $1 < p < \infty$. We define the form $q(m,n) := m^2 + n^2$, and a function

$$f(k) := \begin{cases} j^{-\frac{1}{p}} \log^{-\frac{1+p}{2p}} j & \text{if } k = j^2, \quad j \in \mathbb{N} - \{1\} \\ 0 & \text{otherwise} \end{cases}. \tag{5.2}$$

Then we obtain

$$
\begin{aligned}
\|\mathcal{I}_{1-p^{-1}} f\|_p^p = \sum_{n\in\mathbb{Z}} \Big| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{|m|^{1-p^{-1}}} \Big|^p \geq \Big| \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,0))}{|m|^{1-p^{-1}}} \Big|^p \\
= \Big(2 \sum_{m\geq 2} \frac{m^{-p^{-1}} \log^{-\frac{1+p}{2p}} m}{m^{1-p^{-1}}} \Big)^p \\
= \Big(2 \sum_{m\geq 2} \frac{1}{m \log^{\frac{1+p}{2p}} m} \Big)^p,
\end{aligned}
\tag{5.3}
$$

and this result is clearly divergent. □

CHAPTER 6

THE CASE OF INDEFINITE FORMS

In this chapter, the second theorem claimed in the introduction will be shown with the help of some results obtained from chapter 3 and chapter 4. We are faced with a more complicated case in comparison to positive definite forms since the number of representations is infinite and the automorphs of the form q are constructively obtained. We will start with the specific case, in which the form $q = [a, b, c]$ is primitive and $b = 0$ to get estimates for our operator $\mathcal{I}_\lambda f$ by using (4.21) as contrasted with (4.16) in Theorem 1.1. We will deal with the general case $q(m, n) = ax^2 + bxy + cy^2$ later.

Proof For $p = \infty$ the same method as in the proof of Theorem 1.1 yields

$$\|\mathcal{I}_\lambda f\|_\infty \leq C_\lambda \|f\|_\infty.$$

Let us consider the case $p = 1$. Firstly, we suppose that the form $q(m, n) = am^2 + cn^2$ satisfying $a > 0$, $c < 0$ and $\gcd(a, c) = 1$. Since $b = 0$ and the determinant of $[q]$ is $-4ac$, it must be at least 8. We use the sets A_k, for all $k \in \mathbb{Z}$. The set A_0 is empty because of (3.2). Suppose $k \neq 0$. Let us consider the sets

$$A'_k := \{(m, n) \in \mathbb{Z}_* \times \mathbb{Z}_* : q(m, n) = k\}.$$

Then the sets $A_k \setminus A'_k$ involve at most 2 elements. Therefore, we have

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} \leq 2 + \sum_{(m,n)\in A'_k} \frac{1}{|m|^\lambda}.$$

If $(m, n) \in A'_k$, we have $(-m, -n), (m, -n), (-m, n) \in A'_k$ as might be expected.

Thus, when we consider the sets

$$A''_k := \{(m, n) \in \mathbb{N} \times \mathbb{N} : q(m, n) = k\},$$

we obtain

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} \leq 2 + \sum_{(m,n)\in A'_k} \frac{1}{|m|^\lambda} = 2 + 4 \cdot \sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda}.$$

We henceforth investigate the sum over A''_k. We partition A''_k as

$$A''_k = \bigcup_{g^2|k} A''_{k,g}, \qquad A''_{k,g} := \{(m,n) \in \mathbb{N} \times \mathbb{N} : q(m,n) = k,\ \gcd(m,n) = g\}.$$

The map $(m,n) \mapsto (m/g, n/g)$ is a one-to-one correspondence from $A''_{k,g}$ onto $A''_{k/g^2,1}$ as seen in chapter 4. Therefore, we obtain a solution for every representation in $A''_{k/g^2,1}$ by solving

$$u_g^2 \equiv \Delta \pmod{4|k/g^2|}, \quad \text{and} \quad 0 \leq u_g < 2|k/g^2|, \tag{6.1}$$

and the associated form is $[k, u_g, v_g]$. We thus partition

$$A''_{k/g^2,1} = \bigcup_{u_g} A''_{k/g^2,1,u_g}.$$

These induce decompositions of $A''_{k,g}$. We denote the subsets coming from these decompositions A''_{k,g,u_g}. Hence,

$$\sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda} = \sum_{g^2|k} \sum_{u_g} \sum_{(m,n)\in A''_{k,g,u_g}} \frac{1}{|m|^\lambda}.$$

Then we obtain

$$\sum_{(m,n)\in A''_{k,g,u_g}} \frac{1}{|m|^\lambda} = \frac{1}{g^\lambda} \sum_{(m,n)\in A''_{k/g^2,1,u_g}} \frac{1}{|m|^\lambda}.$$

Let the sets $A''_{k/g^2,1,u_g}$ be nonempty. Then we can find the elements of these sets by obtaining a matrix that transforms q to an equivalent form $[k/g^2, u_g, v_g]$ and multiplying that matrix with the automorphs of q. We let that $[U_g]$ be a matrix transforming q to $[k/g^2, u_g, v_g]$, and let $[A]$ be the automorph of q associated with the least positive solution (T, U) of the equation $t^2 - \Delta u^2 = 4$. We denote these

$$[U_g] := \begin{bmatrix} \alpha_{u_g} & \beta_{u_g} \\ \gamma_{u_g} & \delta_{u_g} \end{bmatrix}, \quad [A] := \begin{bmatrix} T/2 & -cU \\ aU & T/2 \end{bmatrix}. \tag{6.2}$$

By our assumption, we obtain $T^2 = \Delta U^2 + 4 \geq \Delta + 4 \geq 12$, and this result implies $T \geq 2\sqrt{3}$. Since the first columns of the matrices give the proper representations as stated in chapter 4, the elements $(m, n) \in A''_{k/g^2,1,u_g}$ are the first columns of the matrices in the below chains where both entries of the first column are positive

$$\begin{gathered} \dots [A]^{-2}[U_g],\ \ [A]^{-1}[U_g],\ \ [A]^0[U_g],\ \ [A][U_g],\ \ [A]^2[U_g] \dots \\ \dots - [A]^{-2}[U_g],\ -[A]^{-1}[U_g],\ -[A]^0[U_g],\ -[A][U_g],\ -[A]^2[U_g] \dots \end{gathered} \tag{6.3}$$

Let

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

be any matrix from these chains.

As we get

$$\begin{bmatrix} T/2 & -cU \\ aU & T/2 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} T\alpha/2 - cU\gamma & T\beta/2 - cU\delta \\ aU\alpha + T\gamma/2 & aU\beta + T\delta/2 \end{bmatrix},$$

if $\alpha > 0, \gamma > 0$, we have $T\alpha/2 - cU\gamma > 0$, $aU\alpha + T\gamma/2 > 0$, and also

$$T\alpha/2 - cU\gamma > \sqrt{3}\alpha. \tag{6.4}$$

Thus, if we have a matrix in one of the chains (6.3) with

$$\alpha > 0, \quad \gamma > 0, \tag{6.5}$$

then we observe that each matrix on the right of this matrix in the chain satisfies the same property. This gives rise to that if we have matrices satisfying (6.5), then all of them must be situated in only one chain. Since we have $T\alpha/2 - cU\gamma > \sqrt{3}\alpha$, there must be a leftmost matrix satisfying (6.5). We introduce the leftmost matrix as shown below

$$[U'_g] := \begin{bmatrix} \alpha_{u'_g} & \beta_{u'_g} \\ \gamma_{u'_g} & \delta_{u'_g} \end{bmatrix}.$$

We conclude that we obtain all elements of $(m, n) \in A''_{k/g^2,1,u_g}$ by looking at the first columns of $[A]^j[U'_g]$ for $j \geq 0$, and the first entry of the first column of $[A]^j[U'_g]$ cannot be less than $T\alpha/2 - cU\gamma > 3^{j/2}\alpha_{u'_g}$. As a result, we obtain

$$\sum_{(m,n)\in A''_{k/g^2,1,u_g}} \frac{1}{|m|^\lambda} \leq \frac{1}{\alpha^\lambda_{u'_g}} \sum_{j=0}^{\infty} \frac{1}{3^{j\lambda/2}} \leq \frac{C_\lambda}{\alpha^\lambda_{u'_g}}.$$

We get

$$\sum_{(m,n)\in A''_{k,g,u_g}} \frac{1}{|m|^\lambda} \leq \frac{C_\lambda}{(g\alpha_{u'_g})^\lambda}.$$

We find only one representation for $(g\alpha_{u'_g}, g\gamma_{u'_g}) \in A''_{k,g,u_g}$ by multiplying the sets $A''_{k/g^2,1,u_g}$ with g. It follows from this result that we obtain an estimate in the infinite sum over representations of $q = am^2 + cn^2$ with $a > 0$, $c < 0$ and $\gcd(a, c) = 1$. Indeed,

$$\sum_{(m,n)\in A''_k} \frac{1}{|m|^\lambda} = \sum_{g^2|k} \sum_{u_g} \sum_{(m,n)\in A''_{k,g,u_g}} \frac{1}{|m|^\lambda} \leq C_\lambda \sum_{g^2|k} \sum_{u_g} \frac{1}{(g\alpha_{u'_g})^\lambda}.$$

Since we have at most 4 representations $q(m, n) = k$ satisfying $|m| \leq |k|^{1/4}\Delta^{-1/2}$ by Lemma 3.2, we get

$$\leq C_\lambda \Big[4 + \frac{\Delta^{\lambda/2}}{|k|^{\lambda/4}} \sum_{g^2|k} \sum_{u_g} 1\Big].$$

The last double sum enable us to get the summation over g of number of solutions of (6.1). Furthermore, we know from chapter 4 that this number has an upper bound $d(|k|)\sqrt{\Delta}$ for each g. The number of g has again an upper bound $d(|k|)$. Hence, when we utilize the relation $d(|k|) \leq C_\lambda |k|^{\lambda/16}$, the double sum will be bounded by $C_\lambda |k|^{\lambda/8}\sqrt{\Delta}$. We thus obtain

$$\leq C_\lambda\Big[4 + \frac{\Delta^{\lambda/2}}{|k|^{\lambda/4}} C_\lambda |k|^{\lambda/8}\sqrt{\Delta}\Big] \leq C_\lambda[4 + C_\lambda \Delta^{(1+\lambda)/2}] \leq C_\lambda \Delta^{(1+\lambda)/2}.$$

We conclude

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda} \leq C_\lambda \Delta^{(1+\lambda)/2}. \tag{6.6}$$

Then we have

$$\|\mathcal{I}_\lambda f\|_1 \leq C_\lambda \Delta^{(1+\lambda)/2} \|f\|_1.$$

We turn to the general case. We suppose that $q(m,n) = am^2 + bmn + cn^2$ is an indefinite form of non-square discriminant. Non-square discriminant gives $a \neq 0$, $c \neq 0$. Then we can write

$$\|I_{\lambda,q} f\|_1 \leq \sum_{k\in\mathbb{Z}} |f(k)| \sum_{(m,n)\in A_k} \frac{1}{|m|^\lambda},$$

with $A_k := \{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : am^2 + bmn + cn^2 = k\}$. Then we get

$$\begin{aligned}
&\{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : am^2 + bmn + cn^2 = k\}\\
=&\{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : 4acm^2 + 4bcmn + 4c^2n^2 = 4ck\}\\
=&\{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : (bm + 2cn)^2 - \Delta m^2 = 4ck\}\\
=&\{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : \Delta m^2 - (bm + 2cn)^2 = -4ck.\}
\end{aligned}$$

Let $q'(x,y) := \Delta x^2 - y^2$, and the sets $A_{q',k} := \{(m,n) \in \mathbb{Z}_* \times \mathbb{Z} : \Delta m^2 - n^2 = k\}$. We easily get $\Delta(q') = 4\Delta(q)$. When $(m,n) \in A_k$, $(m, bm + 2cn)$ will be in $A_{q',-4ck}$, and also this map

$(m, n) \mapsto (m, bm + 2cn)$ is injective. Hence,

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^{\lambda}} \leq \sum_{(m,n)\in A_{q',-4ck}} \frac{1}{|m|^{\lambda}}. \tag{6.7}$$

With the help of the form q' defined above and the relation (6.6) with $\Delta(q') = 4\Delta(q)$, we get

$$\sum_{(m,n)\in A_{q',-4ck}} \frac{1}{|m|^{\lambda}} \leq C_{\lambda} 2^{1+\lambda} \Delta^{(1+\lambda)/2} = C_{\lambda} \Delta^{(1+\lambda)/2}, \tag{6.8}$$

and hence,

$$\|I_{\lambda,q} f\|_1 \leq C_{\lambda} \Delta^{(1+\lambda)/2} \|f\|_1 = C_{\lambda,\Delta} \|f\|_1.$$

Let us consider the case $1 < p < \infty$ and $q(m, n) = am^2 + bmn + cn^2$ an indefinite form of non-square discriminant. Applying the same process as done for the positive definite case gives

$$\|\mathcal{I}_{\lambda} f\|_p^p \leq C_{p,\lambda} \sum_{k\in\mathbb{N}} |f(k)|^p \sum_{(m,n)\in A_k} \frac{1}{|m|^{\lambda' p/2}}$$

satisfying $\lambda' = \lambda - 1 + p^{-1}$. By using (6.7) and (6.8), we obtain

$$\sum_{(m,n)\in A_k} \frac{1}{|m|^{\lambda' p/2}} \leq C_{p,\lambda} \Delta^{(1+\lambda' p/2)/2},$$

and thus

$$\|\mathcal{I}_{\lambda} f\|_p \leq C_{p,\lambda} \Delta^{1/2p+\lambda'/4} \|f\|_p = C_{p,\lambda,\Delta} \|f\|_p.$$

Let us deal with the sharpness part of the theorem. This is clear for the case $p = \infty$.

If $p = 1$, it will be easy to prove unboundedness when $r = 1$ by utilizing the infinitude of number of automorphs of the form. To show it, suppose that $q(m, n) := m^2 - 8n^2$ and

$$f(k) = \begin{cases} 1 & \text{if } k = 4 \\ 0 & \text{otherwise} \end{cases}.$$

By using (4.20) for $k = 4$, we obtain

$$(t + 2\sqrt{2}u) = i2(3 + 2\sqrt{2})^j, \quad i = \pm 1, \quad j = 0, \pm 1, \pm 2 \ldots.$$

It is enough to use positive representations $t_j > 0$, $u_j > 0$ when we consider $i = 1$ and $j > 0$. It is possible to write $t_j \leq 2 \cdot 6^j$. Hence,

$$\begin{aligned} \|\mathcal{I}_{log} f\|_1 = \sum_{k \in \mathbb{N}} f(k) \sum_{(m,n) \in A_k} \frac{1}{\log(1 + |m|)} &= \sum_{(m,n) \in A_4} \frac{1}{\log(1 + |m|)} \\ &\geq \sum_{(t_j, u_j)} \frac{1}{\log\left(1 + t_j\right)} \\ &\geq \sum_{(t_j, u_j)} \frac{1}{\log 6^{j+1}}, \end{aligned}$$

and this is divergent. However, this argument cannot be utilized for the cases when $r \geq 2$. We therefore utilize the arithmetic of quadratic forms as given in chapter 4. We mentioned the specific form $q(m, n) = m^2 + n^2$ in chapter 4. When this form represents k, we have $|m| \leq k$. However, there is no inequality of this type for indefinite forms, or rather it is known that $|m| \geq C|k|$ can be true for arbitrary $C \in \mathbb{N}$. But, we can find for every solution of (6.1) a representation $(m, n) = k$ satisfying $|m| \leq 10|k|$, and this will be enough. We thus compute the number of solutions of (6.1), and need to be certain of every solution giving representations of k.

Let $q(m, n) := m^2 - 2n^2$. Then $\Delta = 8$. We choose primes $7, 17$, which can be expressed as $8l - 1$, $8l + 1$ respectively. Let us consider $k_j = (7 \cdot 17)^{2j+1}$, $j \in \mathbb{N}$ and a function

$$f(k) = \begin{cases} j^{-2} & \text{if } k = k_j \\ 0 & \text{otherwise} \end{cases}.$$

We calculate the number of solutions of (6.1). When g is a square divisor of k_j, it has the form $7^{i_1}17^{i_2},\ 0 \leq i_1, i_2 \leq j$, and thus our congruence relation is

$$u_g^2 \equiv 8 \pmod{4 \cdot 7^{2(j-i_1)+1} \cdot 17^{2(j-i_2)+1}}, \quad 0 \leq n < 2 \cdot 7^{2(j-i_1)+1} \cdot 17^{2(j-i_2)+1},$$

and we also have half the number of solutions of

$$u_g^2 \equiv 8 \pmod{4 \cdot 7^{2(j-i_1)+1} \cdot 17^{2(j-i_2)+1}}. \tag{6.9}$$

By using Theorem 4.1, we find the number of roots of this congruence. Let us consider these congruences

$$\begin{aligned} n^2 &\equiv 8 \pmod{4}, \\ n^2 &\equiv 8 \pmod{7^{2(j-i_1)+1}}, \\ n^2 &\equiv 8 \pmod{17^{2(j-i_2)+1}}. \end{aligned} \tag{6.10}$$

The product of number of solutions of (6.10) is the number of solutions of (6.9). In the first congruence in (6.10), we clearly have 2 solutions. In the rest of congruences, we use the Theorem 4.1. As a result, we obtain 4 solutions for every choice of i_1, i_2. As we have exactly $j+1$ choices for every i_1, i_2, our congruences get exactly $4(j+1)^2 \geq \log^2 k_j / \log^2 119$ solutions. For every solution $[k_j/g^2, u_g, v_g]$, we are looking for a matrix $[U_g]$ which has determinant 1, and mapping q to this solution as shown in (6.2). We have just one equivalence class of forms for $\Delta = 8$. This result can be seen page 99-104 of [8]. Therefore, there exists a matrix $[U_g]$ transforms q to $[k_j/g^2, u_g, v_g]$. As we have $\alpha_{u_g}^2 - 2\gamma_{u_g}^2 = k_j/g^2 > 0$, we obtain $\alpha_{u_g} \neq 0$. We know that the matrix $-[U_g]$ also transforms q to $[k_j/g^2, u_g, v_g]$, so we may suppose $\alpha_{u_g} > 0$. All representations associated with u_g are as given by (6.3), and we have the automorph $[A]$ and the inverse of automorph $[A]$ is expressed by

$$[A] := \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}, \qquad [A]^{-1} = \begin{bmatrix} 3 & -4 \\ -2 & 3 \end{bmatrix}.$$

We note that we need to pick only one representation to u_g. If $\alpha_{u_g} \leq 10k_j/g^2$, we suppose that $(g\alpha_{u_g}, g\gamma_{u_g})$ is this representation. But, we now assume $\alpha_{u_g} > 10k_j/g^2$. We thus obtain $\gamma_{u_g}^2 > 49k_j/g^2$, and γ_{u_g} might be positive or negative. When this is positive, it follows from the matrix $[A]^{-1}[U_g]$ that we get this representation $(3\alpha_{u_g} - 4\gamma_{u_g}, -2\alpha_{u_g} + 3\gamma_{u_g})$, where we get $0 < 3\alpha_{u_g} - 4\gamma_{u_g} < \alpha_{u_g}/3$, and $0 < -2\alpha_{u_g} + 3\gamma_{u_g}$. When $3\alpha_{u_g} - 4\gamma_{u_g} \leq 10k_j/g^2$, this representation will be multiplied by g and correspond to u_g. If it does not happen, we will again do the same procedure. It can be easily seen that we have a representation by applying this process a finite many of times. Likewise, if $\gamma_{u_g} < 0$, it follows from the matrix $[A][U_g]$ that we have the representation $(3\alpha_{u_g} + 4\gamma_{u_g}, 2\alpha_{u_g} + 3\gamma_{u_g})$, where we get $0 < 3\alpha_{u_g} + 4\gamma_{u_g} < \alpha_{u_g}/3$, and $2\alpha_{u_g} + 3\gamma_{u_g} < 0$. If $3\alpha_{u_g} + 4\gamma_{u_g} \leq 10k_j/g^2$, then this representation will be multiplied by g and correspond to u_g, if not, we will again do the same process. As a result of these, we find a representation $(g\alpha_{u_g}, g\gamma_{u_g})$ satisfying $0 < \alpha_{u_g} \leq 10k_j/g^2$ for every solution u_g. After we find all representations, we get

$$\begin{aligned}
\|\mathcal{I}_{log} f\|_1 = \sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}_*} \frac{f(q(m,n))}{\log(1+|m|)} &= \sum_{k\in\mathbb{N}} f(k) \sum_{(m,n)\in A_k} \frac{1}{\log(1+|m|)} \\
&= \sum_{j\in\mathbb{N}} f(k_j) \sum_{(m,n)\in A_{k_j}} \frac{1}{\log(1+|m|)} \\
&\geq \sum_{j\in\mathbb{N}} j^{-2} \frac{\log^2 k_j}{\log^2 119} \frac{1}{2\log k_j} \\
&\geq \frac{1}{\log 119} \sum_{j\in\mathbb{N}} j^{-1},
\end{aligned}$$

and this obviously diverges. This example can be extended for any $r \in \mathbb{N}$. It is known that 8 is a quadratic residue for any prime p which can be expressed as $8l \pm 1$. By definition of quadratic residue, we obtain 2 solutions coming from $u_g^2 \equiv 8 \pmod{p}$. Hence, when we consider more primes rather than only 7, 17, we do the same process to prove unboundedness results for any $r \in \mathbb{N}$.

If $1 < p < \infty$ and $\lambda = 1 - p^{-1}$, we can again consider the form $q(m,n) := m^2 - 2n^2$, and f as given in (5.2). Then we can find our result by applying the same process as shown in (5.3).

$\square$

CHAPTER 7

CONCLUSION

In this thesis, we proved Theorem 1.1 and Theorem 1.2 to obtain estimates on certain discrete fractional integral operators by using number theory. We expressed step by step how arithmetic, analytic and geometric properties are used for the operator $\mathcal{I}_\lambda f$, and how to obtain estimates for this operator. We decided to use binary quadratic forms as phase polynomials since the theory of binary quadratic forms is well-developed. We believe that the same methods can be applied for higher rank forms, but the theory of these forms are much harder. We proved that Theorem 1.2 fails when the discriminant is a square number by demonstrating a certain function and taking $l^1(\mathbb{Z})$ norm of $\mathcal{I}_\lambda f$. $l^1(\mathbb{Z})$ estimates give rise to the quantity in (2.9), and we concluded that this quantity obviously is about the number of representations of k by the form q, and also structure and distribution of these representations. It follows that this sum is bounded by a constant when $\#A_k$ is small. That case was used to show Theorem 1.1. However, when considering $\#A_k$ that is large or infinite, we observe that the first coordinates of our representations quickly increase. This case was used to prove Theorem 1.2 by using the idea of our first theorem.

We turned to study the geometry and analysis of binary quadratic forms to understand the representation problem and distribution of the representations of numbers over the real numbers. We sketch the curves obtained from both positive definite forms and indefinite forms to gain intuition. Although we proved lemmas for both forms with different methods, we obtained that any quadratic forms having non-square discriminant get at most 4 solutions $(x, y) \in \mathbb{Z}^2$ satisfying

$$|x| \leq \frac{|w|^{1/4}}{\sqrt{-\Delta}}.$$

These lemmas play an important role of proving our main theorems.

In chapter 4, we exploited the classical theory of binary quadratic forms by using results given by Dirichlet, Gauss, Jacobi, and Pall. To prove our theorems, we concentrated on the number of solutions of a given form $q(m, n) = k$ satisfying conditions (4.8), and the number of automorphs of q. We concluded that the first one is related to quadratic residues uncovered by firstly Dirichlet, and the second one is about the sign of Δ. If $\Delta < 0$, then we have finite automorphs. We showed that if $\Delta < 0$,

$$\#R'_k \leq C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|}.$$

We proved that improper representations of k with the greatest common divisor g are mapped bijectively to proper representations of k/g^2. Therefore, we get information about $\#R_k$ by using $\#R'_k$,

$$\#R_k = \sum_{g^2|k} \#R'_{k/g^2} \leq d(|k|) C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|} \leq C_\varepsilon |k|^\varepsilon \sqrt{|\Delta|}.$$

If the discriminant is 0 or positive non-square, then there are infinitely many automorphs. With the help of the Theorems 4.3, 4.4, 4.5, we find the automorphs of q by solving the Pell-like equation $t^2 - \Delta u^2 = 4$, or vice versa. We obtain all integer solutions of $t^2 - \Delta u^2 = 4$ given by

$$\frac{1}{2}(t + \sqrt{\Delta} u) = \pm [\frac{1}{2}(T + \sqrt{\Delta} U)]^k, \qquad (k = 0, \pm 1, \pm 2 \ldots),$$

where T, U give the least positive solution, and the automorphs associated with our solutions given by

$$i[A]^j, \quad i = \pm 1, \quad j = 0, \pm 1, \pm 2 \ldots$$

These results form the main part of our proofs.

We proved Theorem 1.1. We used $\#R_k$ to get estimates for our operator $\mathcal{I}_\lambda f$. We gave estimates for our theorem

- $||\mathcal{I}_\lambda f||_\infty \leq C_\lambda ||f||_\infty$,
- $||\mathcal{I}_\lambda f||_1 \leq C_{\lambda,\Delta} ||f||_1$,
- $||\mathcal{I}_\lambda f||_p \leq C_{p,\lambda,\Delta} ||f||_p$.

We proved Theorem 1.2. Firstly, we obtained estimates for the specific case, in which $q = [a, b, c]$ is primitive and $b = 0$

- $||\mathcal{I}_\lambda f||_\infty \leq C_\lambda ||f||_\infty$,
- $||\mathcal{I}_\lambda f||_1 \leq C_{\lambda,\Delta^{(1+\lambda)/2}} ||f||_1$.

Later, we dealt with the general case $q(m,n) = am^2 + bmn + cn^2$. We concluded that

- $||\mathcal{I}_\lambda f||_\infty \leq C_\lambda ||f||_\infty$
- $||I_{\lambda,q} f||_1 \leq C_{\lambda,\Delta} ||f||_1$,
- $||\mathcal{I}_\lambda f||_p \leq C_{p,\lambda,\Delta} ||f||_p$

Furthermore, we demonstrated our counterexamples for the sharpness parts of these theorems.

REFERENCES

[1] Pierce, L. B., Discrete analogues in harmonic analysis. Princeton University: 2009.

[2] Arkhipov, G. I.; Oskolkov, K. I. i., On a special trigonometric series and its applications. Sbornik: Mathematics 1989, 62 (1), 145-155.

[3] Stein, E.; Wainger, S., Discrete analogues in harmonic analysis II: Fractional integration. Journal d'Analyse Mathématique 2000, 80 (1), 335-355.

[4] Stein, E. M.; Wainger, S., Two discrete fractional integral operators revisited. Journal d'Analyse Mathématique 2002, 87 (1), 451.

[5] Oberlin, D. M., Two discrete fractional integrals. Mathematical Research Letters 2001, 8 (1), 1-6.

[6] Ionescu, A.; Wainger, S., L^p boundedness of discrete singular Radon transforms. Journal of the American Mathematical Society 2006, 19 (2), 357-383.

[7] Buell, D. A., Binary quadratic forms: classical theory and modern computations. Springer Science & Business Media: 1989.

[8] Dickson, L. E., Introduction to the Theory of Numbers. 1929.

[9] Pall, G., The structure of the number of representations function in a positive binary quadratic form. Mathematische Zeitschrift 1933, 36 (1), 321-343.

[10] Pall, G., The structure of the number of representations function in a binary quadratic form. Transactions of the American Mathematical Society 1933, 35 (2), 491-509.

[11] Hardy, G. H.; Wright, E. M., An introduction to the theory of numbers. Oxford university press: 1979.