Finiteness results for regular ternary quadratic polynomials

By

James Ricci

Faculty Advisor: Wai Kiu Chan,
Professor of Mathematics

Wesleyan University

Middletown, CT

May, 2014

A Dissertation in Mathematics

submitted in partial fulfillment of the

requirements for the degree of Doctor of Philosophy

For My Family

Abstract

In 1924, Helmut Hasse established a local-to-global principle for representations of rational quadratic forms. Unfortunately, an analogous local-to-global principle does not hold for representations over the integers. A quadratic polynomial is called regular if such a principle exists; that is, if it represents all the integers which are represented locally by the polynomial itself over $\mathbb{Z}_p$ for all primes p as well as over $\mathbb{R}$. In 1953/54 [16, 17], G.L. Watson showed that up to equivalence, there are only finitely many primitive positive definite integral regular quadratic forms in three variables. More recently, W.K. Chan and B.-K. Oh take the first step in understanding regular ternary quadratic polynomials by showing that there are only finitely many primitive positive regular triangular forms in three variables [6]. This thesis gives an analogous finiteness result for regular ternary quadratic polynomials in greater generality. By defining an invariant called the conductor and a notion of a semi-equivalence class of a quadratic polynomial, we utilize the theory of quadratic forms to obtain the following result: Given a fixed conductor, there are only finitely many semi-equivalence classes of positive regular quadratic polynomials in three variables.

Acknowledgements

First and foremost, I would like to thank my advisor, Professor Wai Kiu Chan. Your guidance, wisdom, and patience have been an indispensable source of motivation and support. I will always look up to your abilities as a teacher, depth of knowledge, and passion for mathematics and will continue to try and emulate these qualities in my own career.

The faculty and graduate community here at Wesleyan have made my experience truly enjoyable. I have felt the support and care every step of the way. I particularly want to thank Chris Rasmussen, David Pollack and Cheryl Hagner for their advice and ability to understand life as a graduate student. I will forever associate my graduate experience with my fellow first year classmates: Abbey, Bonita, Brett, and Gabriel. I need to thank the Grahams for giving me a second family here in Middletown, and thank Kemal, Merry, Dan, and the Tillary crew for always being there and providing me much needed escapes from work.

To my family, I want to thank you for your encouragement and unconditional support. You have been the main source for my desire to become a teacher and I attribute my appreciation for education and my patience to you guys. Joe, I believe a lot of my decision to come to grad school was due to you. Thank you for frequently helping put things in perspective, and for choosing a discipline that has me graduating before you.

Finally, I come to Anna Haensch, who has given me more support and perspective than anyone else these past few years. I have looked up to your abilities as a teacher, scholar, and friend since I got to Wesleyan. You have made me laugh almost every day and always know how to keep me pointed in the right direction. I will forever be thankful for everything you have done and continue to do for me.

Contents

Dedication **i**

Abstract **ii**

Acknowledgements **iii**

Introduction **1**

1 Background and Definitions **4**

1.1 Quadratic Polynomials 4

1.2 Quadratic Spaces and Lattices 7

1.3 Cosets of Lattices 13

2 Preliminaries **19**

2.1 Watson's Transformations 19

2.2 Successive Minima 27

2.3 Estimations of Character Sums 30

3 Primitive Regular Ternary $\mathbb{Z}$-cosets **38**

3.1 Local Representations of Primitive Regular Quadratic Polynomials 38

3.2 Bounding Prime Divisors of the Discriminant of a $\mathbb{Z}$-coset 43

3.3 Main Result 54

4 Regular Quadratic Forms and m-gonal Forms **58**

Bibliography **63**

Introduction

A fundamental question in the study of integral quadratic polynomials is the representation problem, which asks for a complete determination of the set of integers represented by a particular quadratic polynomial f in n variables; that is, we ask for a characterization of those integers N for which there exist integers $x_1, \ldots, x_n$ such that

$$f(x_1, \ldots, x_n) = N.$$

This question has attracted a lot of attention throughout history, most notably in David Hilbert's famous address to the International Congress of Mathematicians in 1900 in which he posed 23 problems to the mathematical community. His 11th problem asked:

> To solve a given quadratic equation with algebraic numerical coefficients in any number of variables by integral or fractional numbers belonging to the algebraic realm of rationality determined by the coefficients [11].

By restricting this problem to the scope of quadratic forms, a successful answer to this question was provided over the rationals by Helmut Hasse [10]. The solution, often known as the Hasse-Minkowski Theorem, asserts that a rational quadratic form f represents an integer N over $\mathbb{Q}$ if and only if f represents N over $\mathbb{Q}_p$ at

every prime p as well as over $\mathbb{Q}_\infty := \mathbb{R}$.

The positive solution to Hilbert's 11th problem over $\mathbb{Q}$ using this local to global principle was a major breakthrough in the realm of quadratic forms. This principle, however, fails to hold when considering solutions over the integers. It is clear that if such a global representation of N exists over $\mathbb{Z}$, then a local solution will exist over $\mathbb{R}$ and over the p-adic integers $\mathbb{Z}_p$ for every prime p. However, it is not the case that these local conditions are sufficient for finding a solution over $\mathbb{Z}$. Following terminology introduced by Dickson, we define a quadratic polynomial to be *regular* if it integrally represents every integer which is locally represented everywhere by the polynomial. In his unpublished Ph.D. thesis [16], G.L. Watson showed that there are only finitely many equivalence classes of primitive positive definite regular integral quadratic forms in three variables. In order to do so, Watson utilized certain regularity preserving transformations to produce bounds for the positive prime power divisors of the discriminants of these quadratic forms. Since then, these methods have been refined and generalized to produce many similar finiteness results for quadratic forms satisfying other regularity conditions (for example see [5], [7], [8], [12], [14]).

More recently, Chan and Oh take the first step in understanding regular ternary quadratic polynomials through the study of a particular family of quadratic polynomials called triangular forms. A triangular form is a polynomial

$$\Delta(a_1, \ldots, a_n) = a_1 \frac{x_1(x_1+1)}{2} + \cdots + a_n \frac{x_n(x_n+1)}{2}$$

where $a_1, \ldots, a_n \in \mathbb{Z}$. By restricting the discussion to triangular forms, Chan and Oh are able to show that there are only finitely many positive primitive regular triangular forms in three variables [6]. This is a very specific type of quadratic

polynomial and the next logical question to ask is if this can be extended to quadratic polynomials in more generality. By further generalizing the methods utilized in these papers, we will improve on these results and find an analogous finiteness result for regular ternary quadratic polynomials in greater generality. Our finiteness result will be based on a slightly coarser notion of equivalence and an invariant which we call the conductor of a polynomial. Further details on these conditions can be found in Chapter 1.

In order to prove the main result, we will translate the question from a discussion of quadratic polynomials to the geometric language of quadratic spaces, lattices, and cosets of lattices. Chapter 1 contains basic definitions and sets up the transition to this geometric setting. In Chapter 2 we review and expand some of the methods used in the study of regular quadratic lattices to regular cosets of quadratic lattices. The main result will be proved in Chapter 3, and then in Chapter 4 we will show how Watson's original result, and that of Chan and Oh, can be seen as consequences of Theorem 1.1. The results of this thesis also cover many new types of inhomogeneous quadratic polynomials; a concrete family of new inhomogeneous quadratic polynomials for which our main result holds will be discussed in Chapter 4.

Chapter 1

Background and Definitions

In this chapter we introduce the necessary definitions and basic concepts that will be used as a basis of this thesis. We begin with some definitions and background in the general setting of quadratic polynomials and then move into the geometric language of quadratic spaces and lattices. Finally, in the last section we discuss how quadratic polynomials are related to cosets of $\mathbb{Z}$-lattices.

1.1 Quadratic Polynomials

Throughout this thesis, unless otherwise stated, we will be working over a field F which is either $\mathbb{Q}$ or one of its p-adic completions $\mathbb{Q}_p$ for some prime p. We will occasionally use $\mathcal{O}$ to denote the ring of integers of the field F, and $\mathcal{O}^\times$ to denote the group of units for $\mathcal{O}$. As we are working over $\mathbb{Q}$, the collection of non-archimedean prime spots is in bijection with the set of all prime numbers p, and there is only one archimedean spot which we will denote as $p = \infty$ where $\mathbb{Q}_\infty = \mathbb{R}$. For more information on local fields, prime spots, and $\mathfrak{p}$-adic completions, the reader is referred to [15, §32].

Let $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ be a rational quadratic polynomial. We will call $f(\mathbf{x})$ **integral** if it is integer-valued in the sense that $f(\mathbf{x}) \in \mathbb{Z}$ for all $\mathbf{x} \in \mathbb{Z}^n$, and say that $f(\mathbf{x})$ is **positive** if $f(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathbb{Z}^n$. It can easily be shown that the coefficients of an integral polynomial f must be in $\frac{1}{2}\mathbb{Z}$.

We will use $\mathfrak{n}(f)$ to denote the $\mathbb{Z}$-ideal generated by $f(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^n$, and call a quadratic polynomial $f(\mathbf{x})$ **primitive** if $\mathfrak{n}(f) = \mathbb{Z}$. Note that if f is primitive then it must be integral, and so the coefficients of a primitive f are always contained in $\frac{1}{2}\mathbb{Z}$. An integral polynomial is called **regular** if it represents all of the integers which are represented over $\mathbb{Z}_p$ for all primes p as well as over $\mathbb{Z}_\infty := \mathbb{R}$.

Two quadratic polynomials $f(\mathbf{x})$ and $g(\mathbf{x})$ are said to be **equivalent** if there exists $T \in GL_n(\mathbb{Z})$ and $\mathbf{x}_0 \in \mathbb{Z}^n$ such that $g(\mathbf{x}) = f(\mathbf{x}T + \mathbf{x}_0)$. This defines an equivalence relation on the set of quadratic polynomials, and equivalent polynomials represent the same set of integers. However, it is easy to see that changing the constant term of a regular polynomial results in a new inequivalent regular polynomial. Similarly, scaling a regular polynomial will give a new regular polynomial. As we do not want to differentiate between these regular polynomials, we therefore expand our notion of equivalence. We say that two integral polynomials $g(\mathbf{x})$ and $f(\mathbf{x})$ are **semi-equivalent** if there exists a positive $\alpha \in \mathbb{Q}^\times$, $m \in \mathbb{Q}$, $T \in GL_n(\mathbb{Z})$, and $\mathbf{x}_0 \in \mathbb{Z}^n$ such that $g(\mathbf{x}) = \alpha f(\mathbf{x}T + \mathbf{x}_0) + m$. This is a coarser equivalence relation on the set of quadratic polynomials than that of the polynomial equivalence defined above. Furthermore, it can be seen from the above observations that semi-equivalence is in a sense the finest equivalence relation that one could use and still hope for a finiteness result.

A homogeneous quadratic polynomial of degree two is called a **quadratic**

form. Given a quadratic form with rational coefficients

$$q(\mathbf{x}) = q(x_1, \ldots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j,$$

we can associate with q a symmetric bilinear form $b : \mathbb{Q}^n \times \mathbb{Q}^n \to \mathbb{Q}$ where $b(\mathbf{x}, \mathbf{x}) = q(\mathbf{x})$. Any quadratic polynomial $f(\mathbf{x})$ can be written in the form

$$f(\mathbf{x}) = q(\mathbf{x}) + \ell(\mathbf{x}) + m$$

where q is a quadratic form, ℓ is a linear form, and $m \in \mathbb{Q}$. It will be assumed throughout this thesis that $q(\mathbf{x})$ is positive definite, meaning $q(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathbb{Q}^n$ and $q(\mathbf{x}) = 0$ if and only if $\mathbf{x} = \mathbf{0}$. In particular, this guarantees the existence of a unique vector $\mathbf{v} \in \mathbb{Q}^n$ such that $\ell(\mathbf{x}) = 2b(\mathbf{v}, \mathbf{x})$ where b is the symmetric bilinear form associated with q. We note that $\mathbf{v} \in \mathbb{Q}^n$ but not necessarily in $\mathbb{Z}^n$. The **conductor** of f is defined to be the smallest positive integer $\mathfrak{c}$ such that $\mathfrak{c}\mathbf{v} \in \mathbb{Z}^n$. Shifting a polynomial by a constant or multiplying a polynomial by a scalar does not change the vector $\mathbf{v}$ and hence does not change the conductor of f. Similarly, it can be shown that equivalent polynomials have the same conductor. Therefore the conductor is an invariant under semi-equivalence.

A quadratic polynomial is called **complete** if it takes the form $f(\mathbf{x}) = q(\mathbf{x}) + 2b(\mathbf{v}, \mathbf{x}) + q(\mathbf{v}) = q(\mathbf{x} + \mathbf{v})$. Equivalently, $f(\mathbf{x})$ is complete if $f(\mathbf{x}) = (\mathbf{x} + \mathbf{v})A(\mathbf{x} + \mathbf{v})^t$, where A is a nonsingular symmetric matrix over $\mathbb{Q}$. We note that every quadratic polynomial is complete after adjusting the constant term accordingly, and so every quadratic polynomial is semi-equivalent to a complete one.

A quadratic form $q(\mathbf{x})$ is **Minkowski reduced** if

$$q(\mathbf{e}_i) \leq q(\mathbf{b}) \text{ for all } \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{Z}^n \text{ with } \gcd(b_i, \ldots, b_n) = 1,$$

where $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ is the standard basis for $\mathbb{Z}^n$. Equivalently, we say $q(\mathbf{x})$ is Minkowski reduced if it is of the form $\mathbf{x}A\mathbf{x}^t$ where A is a Minkowski reduced symmetric matrix. A positive quadratic polynomial is called **Minkowski reduced** if its quadratic part is Minkowski reduced and the polynomial attains its minimum at the zero vector. In the ternary case, [3, Ch. 12 Lemma 1.2] gives $q(\mathbf{e}_1) \leq q(\mathbf{e}_2) \leq q(\mathbf{e}_3)$, $2b(\mathbf{e}_i, \mathbf{e}_j) \leq q(\mathbf{e}_j)$ for all $i \neq j$ and $2|b(\mathbf{v}, \mathbf{e}_i)| \leq q(\mathbf{e}_i)$ for all i, where $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ is the standard basis for $\mathbb{Z}^3$. For further information on Minkowski reduced quadratic forms the reader is referred to [3, Chapter 12].

We have now introduced the terminology and necessary concepts for describing the main result of this thesis.

Theorem 1.1. *Fix a positive integer* $\mathfrak{c}$*. There are only finitely many semi-equivalence classes of positive regular quadratic polynomials in three variables with conductor* $\mathfrak{c}$*.*

1.2 Quadratic Spaces and Lattices

As any quadratic polynomial is semi-equivalent to a complete polynomial $f(\mathbf{x}) = q(\mathbf{x}) + 2b(\mathbf{v}, \mathbf{x}) + q(\mathbf{v}) = q(\mathbf{x} + \mathbf{v})$, the properties of the quadratic components of a quadratic polynomial will encapsulate much of the data for the polynomial as a whole. It should be of no surprise then that the theory of quadratic forms can play a critical role in the analysis of quadratic polynomials. We devote this section to providing some background in the arithmetic theory of quadratic forms.

This section will cover the required notation and terminology; for a more thorough treatment, the reader is referred to either [15] or [9].

A **quadratic space** V over F is defined to be a composite object consisting of a finite dimensional vector space V over F, a quadratic map

$$Q : V \to F,$$

and a symmetric bilinear form

$$B : V \times V \to F$$

with the properties that $Q(\mathbf{x}) = B(\mathbf{x}, \mathbf{x})$ and $Q(\mathbf{x}+\mathbf{y}) = Q(\mathbf{x}) + Q(\mathbf{y}) + 2B(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}$, $\mathbf{y} \in V$. As a convention, we will use (V, Q), or even just V, to denote a quadratic space with an associated quadratic map Q and symmetric bilinear form B. Throughout this thesis we will always assume that any quadratic space V is **nondegenerate** in the sense that $B(\mathbf{x}, V) = 0$ if and only if $\mathbf{x} = \mathbf{0}$. When $F = \mathbb{Q}$ and p is a prime spot of $\mathbb{Q}$, we can extend the quadratic map on V to the quadratic $\mathbb{Q}_p$-space $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. We will denote this $\mathbb{Q}_p$-space by V_p and call this the **localization of** V **at** p.

For any fixed scalar $\alpha \in F$, we define the **scaling** of a quadratic space (V, Q) by α, denoted as V^α, to mean the vector space V provided with a new symmetric bilinear form $B^\alpha(\mathbf{x}, \mathbf{y}) = \alpha B(\mathbf{x}, \mathbf{y})$ and associated quadratic form $Q^\alpha(\mathbf{x}) = \alpha Q(\mathbf{x})$. We note that this is different than scaling a vector as $Q^\alpha(\mathbf{x}) = \alpha Q(\mathbf{x})$ whereas $Q(\alpha\mathbf{x}) = \alpha^2 Q(\mathbf{x})$. Two quadratic spaces V and W are said to be **isometric**, written $V \cong W$, if there is an invertible linear transformation σ of V onto W such that $Q(\sigma(\mathbf{x})) = Q(\mathbf{x})$ for all $\mathbf{x} \in V$.

Fixing a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ for V, the symmetric matrix $M = (a_{ij})$ such that $a_{ij} = B(\mathbf{e}_i, \mathbf{e}_j)$ with $1 \leq i, j \leq n$ is the Gram matrix for V with respect to that basis. We will use $V \cong M$ to mean that M is the Gram matrix for V with respect to some basis for V. Two matrices M and N are said to be equivalent if there exists an invertible matrix T with coefficients in F such that $M = T^t N T$. Equivalent matrices then can be seen as corresponding to a change of basis for the quadratic space V. The **discriminant** of a quadratic space V, denoted dV, is the element $\det(M)F^{\times 2} \in F^\times/F^{\times 2}$. Allowing for the adjustment by a square in $F^\times$ means that dV is independent of our choice of basis for V. Therefore, if $\det(M) = \alpha$, we will often simply say $dV = \alpha$.

We now describe the connection between quadratic spaces and the general definition of a quadratic form as a homogeneous quadratic polynomial. Consider the quadratic form

$$q(X_1, \ldots, X_n) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j \text{ with } a_{ij} \in F.$$

We can always rewrite the crossterms to be of the form $\frac{a_{ij}+a_{ji}}{2}$. Throughout this thesis we will assume that a quadratic form is written with symmetric crossterms and so can be associated with a symmetric matrix (a_{ij}) called the **Gram matrix** of q. This allows us to associate the quadratic form q with a quadratic space (V, Q), where V has a basis $\{x_1, \ldots, x_n\}$ associated with the Gram matrix of q and a quadratic map $Q : V \to F$ defined by

$$Q(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \sum_{1 \leq i,j \leq n} a_{ij} \alpha_i \alpha_j.$$

In other words, we see that the quadratic map Q is obtained from q by substituting

α_i for X_i. From now on the term quadratic form may either refer to a homogeneous quadratic polynomial or to its associated quadratic map Q.

An $\mathcal{O}$-submodule $L \subseteq V$ is called an **$\mathcal{O}$-lattice**, or just a lattice, in V if there exists a basis $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ for V such that

$$L \subseteq \mathcal{O}\mathbf{x}_1 + \cdots + \mathcal{O}\mathbf{x}_n.$$

We say that L is a lattice on V if $FL = V$. Given a lattice L, we can also associate it with the Gram matrix M of FL with respect to a basis $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ and write $L \cong M$. Change of bases will correspond to integral equivalence of matrices in this setting. The discriminant of a lattice L, denoted dL, is the element $\det(M)\mathcal{O}^{\times 2} \in \mathcal{O}^\times/\mathcal{O}^{\times 2}$ and if $\det(M) = \alpha$, we will often simply say $dL = \alpha$. For any nonarchimedean prime p in F, we define $L_p := L \otimes_{\mathcal{O}} \mathcal{O}_p$ to be the localization of the lattice L at p. This lattice is then an $\mathcal{O}_p$-lattice on the quadratic space V_p.

Let L and K be two lattices on a quadratic space V. We say that K is in the **class** of L, denoted $\mathrm{cls}(L)$, if there exists and isometry $\sigma \in O(V)$ such that $\sigma(L) = K$. If for every prime p there exists a $\sigma_p \in O(V_p)$ such that $\sigma_p(L_p) = K_p$, then K is in the **genus** of L, denoted as $\mathrm{gen}(L)$. An integer a is said to be represented by $\mathrm{gen}(L)$ if there is some lattice in $\mathrm{gen}(L)$ which represents a. Therefore, L is regular if it represents all integers which are represented by $\mathrm{gen}(L)$.

If L can be written as the direct sum of sublattices $L = L_1 \oplus \cdots \oplus L_r$ with $B(L_i, L_j) = 0$ for $1 \leq i < j \leq r$, then we say that L is the orthogonal sum of the sublattices $L_1, \ldots, L_r$, or that L has the **orthogonal splitting**

$$L = L_1 \perp \ldots \perp L_r.$$

We call the L_i from the above equation the components of the splitting. We say that a sublattice K splits L if there is a sublattice J of L such that

$$L = K \perp J.$$

If L splits into an orthogonal sum of rank one components in the sense that $L \cong (a_{ij})$ with $a_{ij} = 0$ whenever $i \neq j$, then we say that L is **diagonalizable** or that L has an **orthogonal basis** and will write $L = \langle a_1, \ldots, a_n \rangle$. A non-zero vector $\mathbf{v} \in L$ is **maximal** if it can be extended to a basis of L.

The **scale** of a lattice L, denoted $\mathfrak{s}(L)$, is the $\mathcal{O}$-module generated by the subset $B(L, L)$ in F. The **norm** of L, denoted $\mathfrak{n}(L)$, is the $\mathcal{O}$-module generated by the subset $Q(L)$ of F. It can be seen that both $\mathfrak{n}(L)$ and $\mathfrak{s}(L)$ are fractional ideals which satisfy the property

$$2\mathfrak{s}(L) \subseteq \mathfrak{n}(L) \subseteq \mathfrak{s}(L).$$

If $F = \mathbb{Q}_p$ and p is odd, then $2 \in \mathbb{Z}_p^\times$ and hence $2\mathfrak{s}(L) = \mathfrak{n}(L) = \mathfrak{s}(L)$. If $p = 2$ then either $\mathfrak{s}(L) = \mathfrak{n}(L)$ or $2\mathfrak{s}(L) = \mathfrak{n}(L)$.

Suppose V_p is a quadratic space over $\mathbb{Q}_p$ for some finite prime p, and let L_p be a $\mathbb{Z}_p$-lattice of rank n in V_p. If $\mathfrak{s}(L_p) = (\alpha)$ and $dL_p = \alpha^n$ then we call L_p **α-modular** or just modular. Furthermore, if α is in $\mathbb{Z}_p^\times$ and $dL_p \in \mathbb{Z}_p^\times$ then we call L_p a **unimodular** lattice. Equivalently, a $\mathbb{Z}_p$-lattice L_p is called α-modular if $L_p^{\alpha^{-1}}$ is unimodular. As is described in [15, §91c], a $\mathbb{Z}_p$-lattice L_p has an orthogonal basis when p is odd, and an orthogonal splitting into one or two dimensional modular lattices when $p = 2$. Therefore, by grouping the modular components of

these splittings in a suitable fashion we obtain a splitting

$$L_p = L_1 \perp \ldots \perp L_t$$

in which each component is modular and

$$\mathfrak{s}(L_1) \supsetneq \mathfrak{s}(L_2) \supsetneq \ldots \supsetneq \mathfrak{s}(L_t).$$

Any such splitting in this form is called a **Jordan splitting** of L_p. Every non-zero non-degenerate lattice L_p in a quadratic space over $\mathbb{Q}_p$ has at least one Jordan splitting, but in general these splittings are not unique. However, given any two Jordan splittings for L_p,

$$L_p = L_1 \perp \ldots \perp L_t = K_1 \perp \ldots \perp K_T,$$

we have from [15, Theorem 91.9 and §91g] that $t = T$, $\mathrm{rank}(L_i) = \mathrm{rank}(K_i)$, and $\mathfrak{n}(L_i) = \mathfrak{n}(K_i)$ for all $i \leq t$. These are called the **Jordan invariants** of L_p. As noted above, when p is odd, L_p has an orthogonal splitting. If L_p is a unimodular lattice, we have from [15, Prop. 92.1] that there exists $\epsilon \in \mathbb{Z}_p^\times$ with

$$L \cong \langle 1 \rangle \perp \ldots \perp \langle 1 \rangle \perp \langle \epsilon \rangle,$$

If $p = 2$ and L_2 is unimodular, then from [9, Theorem 8.9] we see that L_2 has an orthogonal splitting if $\mathfrak{n}(L_2) = \mathbb{Z}_2$. If $\mathfrak{n}(L_2) = 2\mathbb{Z}_2$, then L_2 can be written as an orthogonal sum consisting of binary sublattices in one of the following two forms. If the binary sublattice is isotropic then it is a **hyperbolic plane**, which

is isometric to

$$\mathbb{H} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

It represents every element of $2\mathbb{Z}_2$. If the binary sublattice is anisotropic, then it is isometric to

$$\mathbb{A} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

which represents precisely every 2-adic integer of odd order.

1.3 Cosets of Lattices

We now combine the geometric language of quadratic spaces and lattices with our study of quadratic polynomials. A $\mathbb{Z}$-**coset** is a set $L + \mathbf{v}$ where L is a $\mathbb{Z}$-lattice on a nondegenerate quadratic space (V, Q) over $\mathbb{Q}$ and $\mathbf{v}$ is a vector in V; it is called **integral** if $Q(L + \mathbf{v}) \subseteq \mathbb{Z}$. Two cosets $L + \mathbf{v}$ and $M + \mathbf{w}$ on two quadratic spaces V and W respectively are said to be **isometric**, written $L + \mathbf{v} \cong M + \mathbf{w}$, if there exists an isometry $\sigma : V \to W$ such that $\sigma(L) = M$ and $\sigma(\mathbf{v}) \in \mathbf{w} + M$. For every finite prime p, $\mathbb{Z}_p$-cosets and isometries are defined analogously. The **conductor** of a $\mathbb{Z}$-coset $L + \mathbf{v}$ will be defined to be the smallest positive integer $\mathfrak{c}$ such that $\mathfrak{c}\mathbf{v} \in L$.

Given a $\mathbb{Z}$-coset $L + \mathbf{v}$ we denote the $\mathbb{Z}$-ideal generated by $Q(\mathbf{x} + \mathbf{v})$ for all $\mathbf{x} \in L$ by $\mathfrak{n}(L + \mathbf{v})$ and the $\mathbb{Z}$-ideal generated by $Q(\mathbf{x}) + 2B(\mathbf{x}, \mathbf{v})$ for all $\mathbf{x} \in L$ by $\mathfrak{n}(\mathbf{v}, L)$. Notice that since $Q(\mathbf{x} + \mathbf{v}) = Q(\mathbf{x}) + 2B(\mathbf{x}, \mathbf{v}) + Q(\mathbf{v})$, $\mathfrak{n}(L + \mathbf{v})$ is generated by $Q(\mathbf{v})$ and $\mathfrak{n}(\mathbf{v}, L)$. This can be seen by first noting that we clearly have $Q(\mathbf{v}) \in \mathfrak{n}(L+\mathbf{v})$. Therefore, for all $\mathbf{x} \in L$, we have $Q(\mathbf{x}+\mathbf{v})-Q(\mathbf{v}) \in \mathfrak{n}(L+\mathbf{v})$ and hence $\mathfrak{n}(\mathbf{v}, L) \subseteq \mathfrak{n}(L + \mathbf{v})$. To see the reverse containment notice that for any

$\mathbf{x} \in L$, we have $Q(\mathbf{x}+\mathbf{v}) = Q(\mathbf{x})+2B(\mathbf{v},\mathbf{x})+Q(\mathbf{v})$ with $Q(\mathbf{x})+2B(\mathbf{v},\mathbf{x}) \in \mathfrak{n}(\mathbf{v}, L)$ and $Q(\mathbf{v})$ in the ideal generated by $Q(\mathbf{v})$. Therefore the ideal generated by the set of all $Q(\mathbf{x}+\mathbf{v})$ is contained in the ideal generated by $Q(\mathbf{v})$ and $\mathfrak{n}(\mathbf{v}, L)$.

A $\mathbb{Z}$-coset $L+\mathbf{v}$ is **primitive** if $\mathfrak{n}(L+\mathbf{v}) = \mathbb{Z}$. Therefore, a primitive coset $L+\mathbf{v}$ must be integral. In particular, $Q(\mathbf{v}) \in \mathbb{Z}$ and $\mathfrak{n}(\mathbf{v}, L) \subseteq \mathbb{Z}$. To aid in the comparison between integral cosets and integral polynomials, the following proposition will be useful.

Lemma 1.2. *If $L+\mathbf{v}$ is primitive with conductor $\mathfrak{c}$, then $4\mathfrak{c}\mathbb{Z} \subseteq \mathfrak{n}(\mathbf{v}, L)$.*

Proof. Let $L+\mathbf{v}$ be primitive and $\mathfrak{n}(\mathbf{v}, L) = \alpha\mathbb{Z}$. Since $\mathfrak{n}(\mathbf{v}, L) \subseteq \mathbb{Z}$, we must have $\alpha \in \mathbb{Z}$. If $\alpha = 1$, then $\mathfrak{n}(\mathbf{v}, L) = \mathbb{Z} \supseteq 4\mathfrak{c}\mathbb{Z}$ and we are done; therefore, we now assume that $\alpha \neq 1$. Let p be a prime and $k \in \mathbb{N}$ such that $p^k|\alpha$. It suffices to show that $p^k|4\mathfrak{c}$. By definition of $\mathfrak{c}$ we must have $\mathfrak{c}\mathbf{v} \in L$ and hence

$$Q(\mathfrak{c}\mathbf{v}) + 2B(\mathbf{v}, \mathfrak{c}\mathbf{v}) \in \mathfrak{n}(\mathbf{v}, L) = \alpha\mathbb{Z} \subseteq p^k\mathbb{Z}.$$

Similarly, since $2\mathfrak{c}\mathbf{v} \in L$, we have

$$Q(2\mathfrak{c}\mathbf{v}) + 2B(\mathbf{v}, 2\mathfrak{c}\mathbf{v}) \in p^k\mathbb{Z}.$$

It follows that $p^k|Q(\mathbf{v})\mathfrak{c}(\mathfrak{c}+2)$ and $p^k|Q(\mathbf{v})4\mathfrak{c}(\mathfrak{c}+1)$. The assumption of primitivity on $L+\mathbf{v}$ guarantees that $\gcd(Q(\mathbf{v}), \alpha) = 1$ and hence $p \nmid Q(\mathbf{v})$. Therefore, given any $p^k|\alpha$, we have

$$p^k|\mathfrak{c}(\mathfrak{c}+2) \tag{1.1}$$

and

$$p^k|4\mathfrak{c}(\mathfrak{c}+1). \tag{1.2}$$

First we suppose that p is odd. If $p|(\mathfrak{c}+2)$ then $p \nmid (\mathfrak{c}+1)$, $p \nmid \mathfrak{c}$, and $p \nmid 4$; thus contradicting (1.2). Therefore, $p \nmid (\mathfrak{c}+2)$ and so from (1.1), we must have $p^k|\mathfrak{c}$.

Now, suppose that $p = 2$. If $p \nmid \mathfrak{c}$, then $p \nmid \mathfrak{c}+2$ which contradicts (1.1). Therefore we must have $p|\mathfrak{c}$. This implies that $p \nmid \mathfrak{c}+1$ and therefore by (1.2) we must have $p^k|4\mathfrak{c}$. This exhausts all possibilities for p and hence, for all $k \in \mathbb{N}$, if p is a prime with $p^k|\alpha$ then $p^k|4\mathfrak{c}$. □

Corollary 1.3. *Suppose $L+\mathbf{v}$ is a primitive $\mathbb{Z}$-coset with conductor $\mathfrak{c}$ and $2\mathfrak{s}(L) = \gamma\mathbb{Z}$. If p is a prime such that $p|\gamma$, then $p|2\mathfrak{c}$.*

Proof. Let $L+\mathbf{v}$ be primitive and $\mathfrak{n}(\mathbf{v}, L) = \alpha\mathbb{Z}$. The assumption of primitivity on $L+\mathbf{v}$ guarantees that $\mathfrak{s}(L) \subseteq \frac{1}{2}\mathbb{Z}$ and hence $2\mathfrak{s}(L) \subseteq \mathbb{Z}$. Let $2\mathfrak{s}(L) = \gamma\mathbb{Z}$. If $\gamma = 1$, then for all primes p we have $p \nmid \gamma$; therefore we assume that $\gamma \neq 1$. Let p be a prime such that $p|\gamma$. Notice that since $p|\gamma$ and $\mathfrak{c}\mathbf{v} \in L$, we have

$$B(\mathbf{x}, 2\mathfrak{c}\mathbf{v}) \in 2\mathfrak{s}(L) = \gamma(\mathbb{Z}) \subseteq p\mathbb{Z} \text{ for all } \mathbf{x} \in L.$$

This implies that

$$2\mathfrak{c}B(\mathbf{x}, \mathbf{v}) \in p^k\mathbb{Z} \text{ for all } \mathbf{x} \in L. \tag{1.3}$$

By means of contradiction, suppose that $p \nmid 2\mathfrak{c}$. Then equation (1.3) guarantees that

$$p|B(\mathbf{x}, \mathbf{v}) \text{ for all } \mathbf{x} \in L.$$

However, as $\mathfrak{n}(L) \subseteq \mathfrak{s}(L)$, this would imply that

$$Q(\mathbf{x}) + 2B(\mathbf{x}, \mathbf{v}) \in p\mathbb{Z} \text{ for all } \mathbf{x} \in L.$$

This implies $p|\mathfrak{n}(\mathbf{v}, L)$ which contradicts Lemma 1.2. Therefore, we can conclude

that $p|2\mathfrak{c}$. $\square$

We will say that $L+\mathbf{v}$ is in **canonical form** if $Q(\mathbf{v}) \leq Q(\mathbf{x}+\mathbf{v})$ for all $\mathbf{x} \in L$. For any $\mathbf{x}_0 \in L$ we have $L + \mathbf{v} = L + (\mathbf{x}_0 + \mathbf{v})$. Therefore we can always choose $\mathbf{v}$ suitably so that $L + \mathbf{v}$ is in canonical form. Unless stated otherwise we will assume throughout this thesis that all $\mathbb{Z}$-cosets are presented in canonical form.

By fixing a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of L we can associate $L + \mathbf{v}$ with a complete quadratic polynomial

$$g(\mathbf{x}) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j + \sum_{1 \leq i \leq n} b_i x_i + Q(\mathbf{v})$$

whose coefficients are determined by the Gram matrix (a_{ij}) of L and $b_i := 2B(\mathbf{e}_i, \mathbf{v})$. From this we can see that

- g represents an integer a if and only if $L + \mathbf{v}$ represents a,
- the conductor for $L + \mathbf{v}$ is the same as that for g,
- $\mathfrak{n}(L + \mathbf{v}) = \mathfrak{n}(g)$ and $\mathfrak{n}(L, \mathbf{v}) = \mathfrak{n}(g - Q(\mathbf{v}))$, and
- $g(\mathbf{x})$ is primitive if and only if $L + \mathbf{v}$ is primitive.

As is described in section 4 of [6], there is a one-to-one canonical correspondence between the set of equivalence classes of complete quadratic polynomials in n-variables over $\mathbb{Q}$ and the set of isometry classes of $\mathbb{Z}$-cosets on n-dimensional quadratic spaces over $\mathbb{Q}$. Under this correspondence, the equivalence class of g corresponds to the isometry class of $L+\mathbf{v}$. As this correspondence respects primitivity, we can refine this bijection to see that it gives a one-to-one correspondence between the set of equivalence classes of primitive complete quadratic polyno-

mials and the set of isometry classes of primitive $\mathbb{Z}$-cosets. To understand how semi-equivalence fits into this correspondence, the following proposition is useful.

Proposition 1.4. *Every semi-equivalence class of quadratic polynomials in n-variables over $\mathbb{Q}$ contains a unique equivalence class of primitive complete quadratic polynomials.*

Proof. It should be clear that every semi-equivalence class contains a primitive complete quadratic polynomial. Furthermore, it can be easily shown that the polynomial equivalence defined in Section 1.1 preserves both primitivity and completeness. It then suffices to show that every semi-equivalence class contains at most one equivalence class of primitive complete quadratic polynomials. Suppose f and g are primitive complete quadratic polynomials that are semi-equivalent. We will show that f and g are actually equivalent.

By definition of semi-equivalence, there exists a positive $\alpha \in \mathbb{Q}^\times$, $m \in \mathbb{Q}$, $\mathbf{x}_0 \in \mathbb{Q}^n$, and $T \in GL_n(\mathbb{Z})$ such that $g(\mathbf{x}) = \alpha f(\mathbf{x}T + \mathbf{x}_0) + m$. Therefore, $\frac{1}{\alpha}g(\mathbf{x}) - \frac{m}{\alpha} = f(\mathbf{x}T + \mathbf{x}_0)$. Now since $f(\mathbf{x})$ is a primitive complete polynomial, so is $f(\mathbf{x}T + \mathbf{x}_0)$. Since f and g are primitive, they are integral, and hence $\frac{m}{\alpha} \in \mathbb{Z}$. Furthermore, since both g and $f(\mathbf{x}T + \mathbf{x}_0)$ are complete, we in fact must have $f(\mathbf{x}_0) = \frac{m}{\alpha} = 0$. Now, since both $g(\mathbf{x})$ and $f(\mathbf{x}T + \mathbf{x}_0)$ are primitive with $\mathfrak{n}(\frac{1}{\alpha}g(\mathbf{x})) = \mathfrak{n}(f(\mathbf{x}T + \mathbf{x}_0))$, we must have $\alpha = 1$. Therefore, $g(\mathbf{x}) = f(\mathbf{x}T + \mathbf{x}_0)$ and hence g is equivalent to f. □

This means that we can associate any quadratic polynomial with a unique isometry class of a primitive $\mathbb{Z}$-coset. We now turn our attention to the specific case when $n = 3$. By restricting to the ternary case, [6, Lemma 2.2] guarantees the existence of a Minkowski reduced primitive complete quadratic polynomial in every equivalence class. Therefore, every ternary quadratic polynomial is semi-

equivalent to a Minkowski reduced primitive complete polynomial. The correspondence of semi-equivalence classes of regular quadratic polynomials with isometry classes of regular $\mathbb{Z}$-cosets allows us to move between the language of polynomials and the geometric language of quadratic spaces and lattices. Therefore, in order to prove Theorem 1.1 we will in fact be proving the following equivalent statement:

Theorem 1.5. *Fix a positive integer* $\mathfrak{c}$. *There are only finitely many isometry classes of primitive regular ternary* $\mathbb{Z}$*-cosets with conductor* $\mathfrak{c}$.

Chapter 2

Preliminaries

In this chapter we introduce some concepts and methods that will be needed in the proof of Theorem 1.5. It should be noted that Watson's transformations, successive minima, and estimations of character sums have all been used in obtaining results for regular quadratic forms and triangular forms mentioned in the introduction. These sections will state some required results from [4, 6, 7, 17] and extend them when necessary to incorporate $\mathbb{Z}$-cosets and to fit the setting needed for Chapter 3.

2.1 Watson's Transformations

In this section we will define and examine mappings that will reduce the prime divisors of the discriminant of the lattice L for a $\mathbb{Z}$-coset $L+\mathbf{v}$, while still preserving the regularity of the coset. These mappings are modifications of the transformations used by Watson [16]. For more on Watson's transformations, the reader is referred to [4, 6, 7, 17]. We begin by stating the definition and some basic properties of Watson's transformations on $\mathbb{Z}$-lattices and then extend them to

transformations on $\mathbb{Z}$-cosets.

Definition. For any ternary $\mathbb{Z}$ or $\mathbb{Z}_p$ lattice K and any $m \in \mathbb{N}$, let

$$\Lambda_m(K) = \{\mathbf{x} \in K : Q(\mathbf{x}+\mathbf{z}) \equiv Q(\mathbf{z}) \mod m, \text{ for all } \mathbf{z} \in K\}$$

The defining condition for $\Lambda_m(K)$ is equivalent to requiring that $Q(\mathbf{x}) + 2B(\mathbf{x},\mathbf{z}) \in m\mathbb{Z}$ (or $m\mathbb{Z}_p$), for all $\mathbf{z} \in K$. Taking $\mathbf{z} = 0 \in K$ shows that for all $\mathbf{x} \in \Lambda_m(K)$, $Q(\mathbf{x}) \equiv 0 \mod m$ and so $Q(\mathbf{x}) + 2B(\mathbf{x},\mathbf{z}) \equiv 2B(\mathbf{x},\mathbf{z}) \equiv 0 \mod m$ for all $\mathbf{z} \in K$.

The following Lemma is taken from [4, Lemma 2.2].

Lemma 2.1. *Let L be a ternary $\mathbb{Z}$-lattice, m a positive integer, and p a prime. Then the following statements hold:*

(a) $\Lambda_m(L)$ is a sublattice of L and $\Lambda_m(L_p)$ is a sublattice of L_p.

(b) $\Lambda_q(L_p) = (\Lambda_q(L))_p$.

(c) $\Lambda_m(L_p) = L_p$ whenever p does not divide m.

(d) $\mathfrak{n}(\Lambda_m(L)) \subseteq m\mathbb{Z}$ and $\mathfrak{n}(\Lambda_m(L_p)) \subseteq m\mathbb{Z}_p$.

(e) If $\mathfrak{s}(L) \subseteq \mathbb{Z}$, then $pL \subseteq \Lambda_{2p}(L)$ and $pL_p \subseteq \Lambda_{2p}(L_p)$.

(f) If N splits L_p and $\mathfrak{n}(N) \subseteq 2p\mathbb{Z}_p$, then $N \subseteq \Lambda_{2p}(L_p)$.

(g) If $\mathfrak{s}L_2 \subseteq 2\mathbb{Z}_2$, then $\Lambda_4(L_2) = \{x \in L_2 : Q(x) \in 4\mathbb{Z}_2\}$.

Throughout this section we will suppose that L is a ternary $\mathbb{Z}$-lattice and $\mathfrak{s}(L) = \gamma\mathbb{Z}$ for some $\gamma \in \mathbb{Z}$. Given such an L and a prime p where $p \nmid \gamma$, we fix a splitting of L_p as $L_p = M \perp N$, where M is the leading Jordan component of

L_p and $\mathfrak{s}(N) \subsetneq \mathfrak{s}(M)$. We then note that M is unimodular since for any $p \nmid \gamma$, $\mathfrak{n}(L_p) = \mathfrak{s}(L_p) = \mathbb{Z}_p$.

Lemma 2.2. *If p is odd and $\mathfrak{s}(L_p) = \mathbb{Z}_p$, then $\Lambda_p(L_p) = pM \perp N$.*

Proof. Let $p\mathbf{m} + \mathbf{n} \in pM \perp N$. By definition of N we have $\mathfrak{s}(N) \subseteq p\mathbb{Z}_p$. This guarantees that $Q(p\mathbf{m}+\mathbf{n}) = p^2Q(\mathbf{m})+Q(\mathbf{n}) \equiv 0 \mod p$. Similarly, given $\mathbf{z} \in L_p$ with $\mathbf{z} = \mathbf{m}' + \mathbf{n}'$ for some $\mathbf{m}' \in M$, $\mathbf{n}' \in N$, we also have

$$\begin{aligned} 2B(p\mathbf{m} + \mathbf{n}, \mathbf{z}) &= 2pB(\mathbf{m}, \mathbf{m}') + 2B(\mathbf{n}, \mathbf{n}') \\ &\equiv 0 \mod p. \end{aligned}$$

Therefore,

$$\begin{aligned} Q(p\mathbf{m} + \mathbf{n} + \mathbf{z}) &= Q(p\mathbf{m} + \mathbf{n}) + Q(\mathbf{z}) + 2B(p\mathbf{m} + \mathbf{n}, \mathbf{z}) \\ &\equiv Q(\mathbf{z}) \mod p \text{ for all } \mathbf{z} \in L_p. \end{aligned}$$

Hence, $p\mathbf{m} + \mathbf{n} \in \Lambda_p(L_p)$. Conversely, let $\mathbf{x} \in \Lambda_p(L_p)$ and write $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1$, with $\mathbf{x}_0 \in M$, and $\mathbf{x}_1 \in N$. By means of contradiction suppose $\mathbf{x}_0 \notin pM$. Then $\mathbf{x}_0$ is maximal. Therefore, by [15, 82.17], there exists $\mathbf{y} \in M$ such that $B(\mathbf{x}_0, \mathbf{y}) = 1$. It then follows that $Q(\mathbf{x}) + 2B(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x}) + 2B(\mathbf{x}_0, \mathbf{y}) = Q(\mathbf{x}) + 2$. However, since $\mathbf{x} \in \Lambda_p(L_p)$, we have $Q(\mathbf{x}) \in p\mathbb{Z}_p$. Therefore $Q(\mathbf{x}) + 2 \notin p\mathbb{Z}_p$ contradicting the assumption that $\mathbf{x} \in \Lambda_p(L_p)$. Hence $\mathbf{x} \in pM \perp N$. □

A $\mathbb{Z}$-lattice L is said to **behave well** at a prime p if the rank of the unimodular Jordan component of L_p is at least two. We say that a $\mathbb{Z}$-coset $L + \mathbf{v}$ behaves well at a prime p if and only if L behaves well at p.

Lemma 2.3. *Let p be an odd prime with $\mathfrak{s}(L_p) = \mathbb{Z}_p$. If L does not behave well at p, then $\Lambda_p(L) = \{\mathbf{x} \in L : Q(\mathbf{x}) \in p\mathbb{Z}\}$. Furthermore, if L is regular, then $\Lambda_p(L)$ is also regular.*

Proof. As previously remarked in this section, it is clear that $\Lambda_p(L) \subseteq \{\mathbf{x} \in L : Q(\mathbf{x}) \in p\mathbb{Z}\}$. To show the reverse containment we first look at the localized lattice $\Lambda_p(L_p)$. In fact, it suffices to show that $\{\mathbf{x} \in L_p : Q(\mathbf{x}) \in p\mathbb{Z}_p\} \subseteq \Lambda_p(L_p)$. This is sufficient as it would imply that for all $\mathbf{x} \in L_p$, if $Q(\mathbf{x}) \equiv 0 \mod p$ then $2B(\mathbf{x}, \mathbf{z}) \equiv 0 \mod p$ for all $\mathbf{z} \in L_p$. Since L is a subset of L_p, this in particular shows that for any $\mathbf{x} \in L$, if $Q(\mathbf{x}) \equiv 0 \mod p$ then $2B(\mathbf{x}, \mathbf{z}) \equiv 0 \mod p$ for all $\mathbf{z} \in L$.

Let $\mathbf{x} \in L_p$ with $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1$ where $\mathbf{x}_0 \in M$ and $\mathbf{x}_1 \in N$. Suppose that $Q(\mathbf{x}) \in p\mathbb{Z}_p$. By Lemma 2.2, since p is odd with $\mathfrak{s}(L_p) = \mathbb{Z}_p$, it suffices to show that $\mathbf{x}_0 \in pM$. Since $Q(\mathbf{x}) = Q(\mathbf{x}_0) + Q(\mathbf{x}_1)$ with $Q(\mathbf{x}) \in p\mathbb{Z}_p$ and $Q(\mathbf{x}_1) \in \mathfrak{n}(N) = \mathfrak{s}(N) \subseteq p\mathbb{Z}_p$, it follows that $Q(\mathbf{x}_0) \in p\mathbb{Z}_p$. Suppose by means of contradiction that $\mathbf{x}_0 \notin pM$ then $\mathbf{x}_0$ is a maximal vector of M. Therefore by [15, 82.17] there exists $\mathbf{y} \in M$ such that $B(\mathbf{x}_0, \mathbf{y}) = 1$. Then $K = \mathbb{Z}_p\mathbf{x}_0 + \mathbb{Z}_p\mathbf{y}$ is a binary unimodular lattice of discriminant $dK = -1$. Thus K is a hyperbolic plane and will split L_p by [15, 82.15], contradicting the assumption that L_p does not behave well at p. Therefore, $\Lambda_p(L)_p \subseteq \{\mathbf{x} \in L_p : Q(\mathbf{x}) \in p\mathbb{Z}_p\}$ and hence $\{\mathbf{x} \in L : Q(\mathbf{x}) \in p\mathbb{Z}\} = \Lambda_p(L)$.

To prove the assertion of regularity, let n be an integer represented by the genus of $\Lambda_p(L)$. Since $\Lambda_p(L) \subseteq L$ we can see that n is represented by $\mathrm{gen}(L)$. The regularity of L then guarantees that n is represented by L. Therefore, there exists $\mathbf{x} \in L$ such that $Q(\mathbf{x}) = n$. Now for every prime q, there exists $\mathbf{y} \in \Lambda_p(L_q)$ such that $n = Q(\mathbf{y})$. From the first assertion of this lemma we know that if $\mathbf{y} \in \Lambda_p(L_p)$

then $Q(\mathbf{y}) \in p\mathbb{Z}_p$, hence $p|n$. Therefore, $\mathbf{x} \in L$ and $p|n$, implying that $p|Q(\mathbf{x})$ and $\mathbf{x} \in \Lambda_p(L)$ by the equality given in the first assertion. □

If $\mathfrak{n}L = \gamma\mathbb{Z}$ and p is odd with $p \nmid \gamma$, then it follows from Lemma 2.1 (d) and (e) that $p^2\gamma\mathbb{Z} = p^2\mathfrak{n}(L) = \mathfrak{n}(pL) \subseteq \mathfrak{n}(\Lambda_p(L)) \subseteq p\gamma\mathbb{Z}$. We can therefore scale the symmetric bilinear form on $\Lambda_p(L)$ by either $1/p$ or $1/p^2$ so that the norm ideal of the resulting lattice is still $\gamma\mathbb{Z}$. As in [4] we denote by λ_p the mapping that sends L to the following lattices on the scaled space $V^{1/p}$ or V^{1/p^2}:

$$\lambda_p(L) = \begin{cases} \Lambda_p(L)^{1/p} & \text{if } \mathfrak{n}(\Lambda_p(L)) = p\gamma\mathbb{Z}, \\ \Lambda_p(L)^{1/p^2} & \text{if } \mathfrak{n}(\Lambda_p(L)) = p^2\gamma\mathbb{Z}. \end{cases}$$

These λ_p maps are what we refer to as Watson's transformations.

The following is a minor adjustment of [4, Lemma 2.5].

Lemma 2.4. *Suppose that L is a ternary lattice. If p is an odd prime such that $p^2|dL$, then $d(\lambda_p(L)) = (\frac{1}{p^t})dL$ for some $t \in \{1, 2, 4\}$.*

Proof. Note first that by Lemma 2.2, $d(\Lambda_p(L)) = p^2 dL$ if M is unimodular of rank 1. Then $d(\lambda_p(L)) = (\frac{1}{p})dL$ or $(\frac{1}{p^4})dL$ depending on whether $\mathfrak{n}(\Lambda_p(L)) = p\gamma\mathbb{Z}$ or $p^2\gamma\mathbb{Z}$, respectively. If M is unimodular of rank 2 then $\mathfrak{n}(N) \subseteq p^2\mathbb{Z}_p$, by the assumption that $p^2|dL$; so $\mathfrak{n}(\Lambda_p(L)) = p^2\mathbb{Z}$, by Lemma 2.2. Therefore,

$$d(\lambda_p(L)) = (\frac{1}{p^2})^3 d(\Lambda_p L) = ((\frac{1}{p^6})(p^4 dL) = (\frac{1}{p^2})dL.$$

□

In Chapter 3, given a $\mathbb{Z}$-coset $L + \mathbf{v}$, we will be concerned with reducing prime power divisors of the discriminant of L only at odd primes away from the

conductor. Therefore, for the remainder of this section we only look at Watson's transformations at such primes. Let $L+\mathbf{v}$ be a primitive $\mathbb{Z}$-coset with conductor $\mathfrak{c}$. For any prime $p \nmid 2\mathfrak{c}$ we note that $\mathbf{v} \in L_p$ and hence $L_p + \mathbf{v} = L_p$. The primitivity of $L+\mathbf{v}$ guarantees that $\mathfrak{n}(L_p+\mathbf{v}) = \mathfrak{n}(L_p) = \mathfrak{s}(L_p) = \mathbb{Z}_p$. Therefore, if $\mathfrak{s}(L) = \gamma\mathbb{Z}$ then $\gcd(p, \gamma) = 1$ for all $p \nmid 2\mathfrak{c}$.

We begin with a technical lemma and then show that we can use Watson's transformations on $\mathbb{Z}$-cosets while preserving regularity, primitivity, and the conductor as well.

Lemma 2.5. *Let L and K be $\mathbb{Z}$-lattices on a quadratic space V and $\mathbf{w}, \mathbf{v} \in V$. If $L_p + \mathbf{v} \subseteq K_p + \mathbf{w}$ for all p then $L + \mathbf{v} \subseteq K + \mathbf{w}$. In particular, $L + \mathbf{v} = K + \mathbf{w}$ if and only if $L_p + \mathbf{v} = K_p + \mathbf{w}$ for all primes p.*

Proof. Suppose $L_p+\mathbf{v} \subseteq K_p+\mathbf{w}$ for all p and let $\mathbf{x}+\mathbf{v} \in L+\mathbf{v}$. Then $\mathbf{x}+\mathbf{v} \in L_p+\mathbf{v}$ so $\mathbf{x} + \mathbf{v} \in K_p + \mathbf{w}$ for all p. Therefore $\mathbf{x} + \mathbf{v} - \mathbf{w} \in K_p$ for all p and hence $\mathbf{x} + \mathbf{v} - \mathbf{w} \in K$. Therefore $\mathbf{x} + \mathbf{v} \in K + \mathbf{w}$. □

Lemma 2.6. *Let $L + \mathbf{v}$ be a primitive regular ternary $\mathbb{Z}$-coset with conductor $\mathfrak{c}$ on a quadratic space (V, Q). If p is an odd prime such that $p \nmid \mathfrak{c}$ and $L + \mathbf{v}$ does not behave well at p, then there exists $\mathbf{w} \in V$ such that $\lambda_p(L) + \mathbf{w}$ is a primitive regular $\mathbb{Z}$-coset of conductor $\mathfrak{c}$.*

Proof. Since $p \nmid \mathfrak{c}$, we have $L_p + \mathbf{v} = L_p$ and $\mathfrak{s}L_p = \mathbb{Z}_p$. As L does not behave well at p, Lemma 2.3 guarantees that $\Lambda_p(L) = \{\mathbf{x} \in L : Q(\mathbf{x}) \in p\mathbb{Z}\}$. Consider the coset $\Lambda_p(L) + p^j\mathbf{v}$, where $2 < j$ such that $p^j \equiv 1 \mod \mathfrak{c}$. We claim that at any prime q:

$$\Lambda_p(L)_q + p^j\mathbf{v} = \begin{cases} L_q + \mathbf{v} & \text{if } q|\mathfrak{c}, \\ \Lambda_p(L_p) & \text{if } p = q, \\ L_q & \text{if } q \nmid \mathfrak{c}p. \end{cases}$$

First suppose $p \neq q$. By Lemma 2.1, $\Lambda_p(L)_q = \Lambda_p(L_q) = L_q$. If $q|\mathfrak{c}$, then by our choice of j we have $p^j \equiv 1 \mod \mathfrak{c}$ and so $(p^j - 1)\mathbf{v} \in L$. Therefore $L + p^j\mathbf{v} = L + \mathbf{v}$, thus $\Lambda_p(L)_q + p^j\mathbf{v} = L_q + p^j\mathbf{v} = L_q + \mathbf{v}$. If $q \nmid \mathfrak{c}$ then $\mathbf{v} \in L_q$ and hence $\Lambda_p(L)_q + p^j\mathbf{v} = L_q + p^j\mathbf{v} = L_q$. Finally if $p = q$, then $\mathbf{v} \in L_p$ and by Lemma 2.3 we also have $p^j\mathbf{v} \in \Lambda_p(L_p)$ hence $\Lambda_p(L_p) + p^j\mathbf{v} = \Lambda_p(L_p)$.

Since $\Lambda_p(L_p) \subseteq L_p = L_p + \mathbf{v}$ it follows from our claim that $\Lambda_p(L)_q + p^j\mathbf{v} \subseteq L_q + \mathbf{v}$ for all primes q. Therefore, Lemma 2.5 gives $\Lambda_p(L) + p^j\mathbf{v} \subseteq L + \mathbf{v}$. We will now show that $\Lambda_p(L) + p^j\mathbf{v}$ is regular.

Suppose that a is a positive integer represented by $\Lambda_p(L)_q + p^j\mathbf{v}$ for all primes q. This means that a is represented by $L_q + \mathbf{v}$ for all primes q. The regularity of $L + \mathbf{v}$ then guarantees the existence of $\mathbf{x} \in L$ such that $Q(\mathbf{x} + \mathbf{v}) = a$. To show that $\mathbf{x} + \mathbf{v} \in \Lambda_p(L) + p^j\mathbf{v}$, Lemma 2.5 allows us to equivalently show that $\mathbf{x} + \mathbf{v} \in \Lambda_p(L)_q + p^j\mathbf{v}$ for every prime q. First suppose $p = q$. It has been assumed that a is represented by $\Lambda_p(L)_p + p^j\mathbf{v} = \Lambda_p(L_p)$ so there exists $\mathbf{y} \in \Lambda_p(L_p)$ such that $Q(\mathbf{y}) = a$. As previously noted, Lemma 2.3 shows that

$$\Lambda_p(L_p) = \{\mathbf{z} \in L_p : Q(\mathbf{z}) \in p\mathbb{Z}_p\}$$

and hence $p|a$. Therefore, $p|Q(\mathbf{x} + \mathbf{v})$ and since $\mathbf{v} \in L_p$ we have $\mathbf{x} + \mathbf{v} \in L_p$ with $Q(\mathbf{x} + \mathbf{v}) \in p\mathbb{Z}_p$ thus giving $\mathbf{x} + \mathbf{v} \in \Lambda_p(L_p)$. Now for all $q \neq p$, since $\mathbf{x} \in L$ we have $\mathbf{x} + \mathbf{v} \in L_q + \mathbf{v} = \Lambda_p(L)_q + p^j\mathbf{v}$. Thus $\mathbf{x} + \mathbf{v} \in \Lambda_p(L)_q + p^j\mathbf{v}$ for all primes q.

Since $p \nmid \mathfrak{c}$, it is clear that $\Lambda_p(L) + p^j\mathbf{v}$ must also have conductor $\mathfrak{c}$. The λ_p transformation sends L on the quadratic space (V, Q) to a new $\mathbb{Z}$-lattice $\lambda_p(L)$ on the quadratic space (V, Q') where $Q'(\mathbf{x}) = \frac{1}{p^i}Q(\mathbf{x})$ for $i \in \{1, 2\}$ depending on $\mathfrak{n}(\Lambda_p(L))$. Therefore, $\lambda_p(L) + p^j\mathbf{v}$ is regular and with conductor $\mathfrak{c}$, as regularity and conductors are invariant under the scaling of the quadratic space. Next, to show

$\lambda_p(L)+p^j\mathbf{v}$ is primitive, we first show that $\mathfrak{n}(\Lambda_p(L)+p^j\mathbf{v}) = p^k\mathbb{Z}$ for some $k \in \mathbb{N}$. Let $\mathfrak{n}(\Lambda_p(L), p^j\mathbf{v}) = \alpha\mathbb{Z}$. As $\mathfrak{n}(\Lambda_p(L) + p^j\mathbf{v})$ is generated by $\mathfrak{n}(\Lambda_p(L), p^j\mathbf{v})$ and the ideal generated by $Q(p^j\mathbf{v})$, it will suffice to show that $\gcd(\alpha, Q(p^j\mathbf{v})) = p^k$. Let $q \neq p$ be prime and suppose $q|\gcd(Q(\mathbf{v}), \alpha)$. Since $L + \mathbf{v}$ is primitive with $q|Q(\mathbf{v})$, we know that $\mathfrak{n}(L, \mathbf{v}) \not\subseteq q\mathbb{Z}$. Therefore, there exists $\mathbf{x} \in L$ such that $q \nmid Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x})$. This also guarantees that

$$q \nmid p^{2j}(Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x})) = Q(p^j\mathbf{x}) + 2B(p^j\mathbf{v}, p^j\mathbf{x}).$$

However, Lemma 2.3 shows that $p^j\mathbf{x} \in \Lambda_p(L)$ thus contradicting our assumption that $q|\alpha$. Therefore, $q \nmid \gcd(\alpha, Q(p^j\mathbf{v}))$.

Since

$$Q'(\mathbf{x}) + 2B'(\mathbf{x}, p^j\mathbf{v}) = \frac{1}{p^i}(Q(\mathbf{x}) + 2B(\mathbf{x}, p^j\mathbf{v})),$$

we see that $\mathfrak{n}(\lambda_p(L)+p^j\mathbf{v}) = \frac{1}{p^i}\mathfrak{n}(\Lambda_p(L)+p^j\mathbf{v}) = p^{k-i}\mathbb{Z}$. From the definition of λ_p and our choice of j, it is clear that $\lambda_p(L)+p^j\mathbf{v}$ is integral as $Q'(p^j\mathbf{v}) = p^{2j-i}Q(\mathbf{v}) \in p\mathbb{Z}$. Therefore, to show primitivity it suffices to show that $\mathfrak{n}(\lambda_p(L), p^j\mathbf{v}) \not\subseteq p\mathbb{Z}$. Let $\mathfrak{s}(L) = \gamma\mathbb{Z}$ and notice that $\mathfrak{s}(\Lambda_p(L)) = p^i\gamma\mathbb{Z}$ hence $\mathfrak{s}(\lambda_p(L)) = \gamma\mathbb{Z}$. The primitivity of $L+\mathbf{v}$ and Corollary 1.3 then guarantees that $p \nmid \gamma$. Suppose $\mathfrak{n}(\lambda_p(L), p^j\mathbf{v}) \subseteq p\mathbb{Z}$, then

$$p|(Q'(\mathbf{x}) + 2B'(p^j\mathbf{v}, \mathbf{x})) \text{ for all } \mathbf{x} \in \lambda_p(L). \tag{2.1}$$

However, since $j > i$ and $p \nmid \gamma$, we are guaranteed the existence of an $\mathbf{x} \in \lambda_p(L)$ with $p \nmid Q'(\mathbf{x})$ and $p|2B'(p^j\mathbf{v}, \mathbf{x})$. This contradicts (2.1) and hence we conclude $\mathfrak{n}(\lambda_p(L), p^j\mathbf{v}) \not\subseteq p\mathbb{Z}$. As $\mathfrak{n}(\lambda_p(L)+p^j\mathbf{v}) = p^{k-i}\mathbb{Z}$ is generated by $\mathfrak{n}(\lambda_p(L), p^j\mathbf{v})$ and the ideal generated by $Q(p^j\mathbf{v})$, we conclude that $\lambda_p(L) + p^j\mathbf{v}$ is primitive.

□

It is possible to begin with a primitive regular ternary coset and use Lemma 2.6 to descend down to a primitive regular ternary coset which behaves well at all odd primes outside of the conductor. We describe that process now.

Begin with a primitive regular ternary coset $L + \mathbf{v}$ of conductor $\mathfrak{c}$, and fix an odd prime $p \nmid \mathfrak{c}$. If $L + \mathbf{v}$ does not behave well at p then by applying Lemma 2.6 we obtain a new primitive regular ternary coset $\lambda_p(L) + \mathbf{v}'$. If $\lambda_p(L) + \mathbf{v}'$ does not behave well at p we can apply Lemma 2.6 again. Since Lemma 2.4 guarantees that the prime power of p dividing the discriminant of L decreases after each successive application of Lemma 2.6, we can eventually find $\ell \geq 0$ and a vector $\mathbf{w}$ in the $\mathbb{Q}$-space spanned by $\lambda_p^\ell(L)$ such that $\lambda_p^\ell(L) + \mathbf{w}$ is regular and behaves well at p. For such an ℓ we define the δ_p operation to be $\delta_p(L + \mathbf{v}) = \lambda_p^\ell(L) + \mathbf{w}$.

A given ternary $\mathbb{Z}$-coset $L + \mathbf{v}$ of conductor $\mathfrak{c}$ behaves well at all but finitely many primes. Let $\{p_1, p_2, \ldots, p_n\}$ be the set of these primes that also satisfy the property of being relatively prime to $2\mathfrak{c}$. Define the δ operation to be

$$\delta(L + \mathbf{v}) = (\delta_{p_1} \circ \ldots \circ \delta_{p_n})(L + \mathbf{v}).$$

The lattice $\delta(L + \mathbf{v})$ is then a regular primitive ternary $\mathbb{Z}$-coset with conductor $\mathfrak{c}$. If we let $\delta(L + \mathbf{v}) = N + \mathbf{w}$, then it follows from Lemma 2.4 that $dN | dL$.

2.2 Successive Minima

Let L be a $\mathbb{Z}$-lattice on the positive definite quadratic space (V, Q) over $\mathbb{Q}$ of dimension n. The following definition and lemma are from [7] and adapted from [3, Chapter 12].

For $1 \leq j \leq n$, the **jth minimum of** L is that positive integer μ_j such that

(i) $\dim(\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq \mu_j\}) \geq j$ and

(ii) $\dim(\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) < \mu_j\}) < j$.

The values $\mu_1, \ldots, \mu_n$ will be collectively referred to as the **successive minima** of L.

Lemma 2.7. *Suppose that for some $j \in \{2, \ldots, n\}$, there exist linearly independent vectors $\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}$ in L such that $Q(\mathbf{m}_i) = \mu_i$ for $i = 1, \ldots, j-1$. If $\mathbf{c} \in L$ satisfies $Q(\mathbf{c}) < \mu_j$, then $\mathbf{c} \in \text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$.*

Proof. If $\mathbf{c} = 0$ then $\mathbf{c} \in \text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$. Otherwise let $\mathbf{c} \neq 0$ and l be the smallest index such that $Q(\mathbf{c}) < \mu_l$. Then $2 \leq l \leq j$ and $\mu_{l-1} \leq Q(\mathbf{c}) < \mu_l$. If $\mathbf{c} \notin \text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$ then $\mathbf{c} \notin \text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{l-1}\}$ and hence $\dim(\text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{l-1}, \mathbf{c}\}) = l$. Therefore,

$$\dim(\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq Q(\mathbf{c})\}) \geq l.$$

Now, since $\mu_1, \ldots, \mu_{l-1} \leq Q(\mathbf{c}) < \mu_l$, we have

$$l \leq \dim(\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq Q(\mathbf{c})\}) \leq \dim(\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) < \mu_l\}) < l$$

where the last inequality is obtained from the definition of μ_l. This is a contradiction, which means $\mathbf{c} \in \text{span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$. □

Corollary 2.8. *There exists a set of linearly independent vectors $\{\mathbf{m}_1, \ldots, \mathbf{m}_n\}$ in L with $Q(\mathbf{m}_i) = \mu_i$ for all $1 \leq i \leq n$.*

Proof. If $n = 1$ then for any basis vector $\mathbf{e}_1$ of L, $Q(\mathbf{e}_1) = \mu_1$ so we are done. Now suppose $n > 1$. Let $\mathbf{m}_1 \in L$ such that $\mathbf{m}_1 \neq 0$ and $Q(\mathbf{m}_1) \leq Q(\mathbf{x})$ for all $\mathbf{x} \in L$.

Then it is clear from the definition of μ_1 that $Q(\mathbf{m}_1) = \mu_1$. Now suppose that for $1 < i \leq n$, there exist linearly independent vectors $\mathbf{m}_1, \ldots, \mathbf{m}_{i-1}$ such that $Q(\mathbf{m}_j) = \mu_j$ for all $j < i$. Consider the subset M of L where

$$M = \{\mathbf{x} \in L : \mathbf{x} \notin \text{ span}_{\mathbb{Q}}\{\mathbf{m}_1, \ldots, \mathbf{m}_{i-1}\}\}.$$

By the contrapositive to Lemma 2.7 we see that for all $\mathbf{x} \in M$, $Q(\mathbf{x}) \geq \mu_i$. By means of contradiction suppose that all of these $\mathbf{x}$ satisfy $Q(\mathbf{x}) > \mu_i$. Then it would be the case that

$$\text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq \mu_i\} = \text{span}_{\mathbb{Q}}\{\mathbf{x} \in L : Q(\mathbf{x}) < \mu_i\}$$

contradicting the definition of μ_i in L. Therefore, there must be some $\mathbf{x} \in L$ with $\mathbf{x}$ linearly independent from $\{\mathbf{m}_1, \ldots, \mathbf{m}_{i-1}\}$ such that $Q(\mathbf{x}) = \mathbf{m}_i$. We can now inductively complete this process to see that L must have n linearly independent vectors satisfying $Q(\mathbf{m}_i) = \mu_i$. □

In the case when $n = 3$, we can choose $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3$ such that they form a basis for L and satisfy $Q(\mathbf{m}_1) \leq Q(\mathbf{m}_2) \leq Q(\mathbf{m}_3)$ and $2|B(\mathbf{m}_i, \mathbf{m}_j)| \leq Q(\mathbf{m}_j)$ for all $i \neq j$ [3]. Such a basis is called a **Minkowski basis** for L. As was described in Chapter 1 and [6, Lemma 2.2], every positive ternary quadratic polynomial is equivalent to a Minkowski reduced ternary quadratic polynomial. This is equivalent to saying that a positive definite ternary $\mathbb{Z}$-coset $L + \mathbf{v}$ is isometric to one in canonical form with a Minkowski basis. When $L + \mathbf{v}$ is in canonical form, it also satisfies

$$Q(\mathbf{x} + \mathbf{v}) = Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x}) + Q(\mathbf{v}) \geq Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x}) \geq 0$$

for all $\mathbf{x} \in L$, thus giving $2|B(\mathbf{v}, \mathbf{m}_i)| \leq Q(\mathbf{m}_i)$ for all i. The following result is [7, Proposition 2.3] and will play an essential role in many of the proofs to come.

Proposition 2.9. *Let L be a lattice of discriminant D with successive minima $\mu_1, \ldots, \mu_n$. Then there exists a constant $C = C(n)$ such that*

$$D \leq \mu_1 \mu_2 \cdots \mu_n \leq CD.$$

2.3 Estimations of Character Sums

Throughout this section, notations are similar to those of [7, Section 3]. Let $\chi_1, \ldots, \chi_r$ be a set of quadratic Dirichlet characters modulo $k_1, \ldots, k_r$, respectively, and $\eta_1, \ldots, \eta_r$ be values from the set $\{\pm 1\}$. Let Γ be the least common multiple of $k_1, \ldots, k_r$, and fix an integer Δ which is relatively prime to Γ. An inequality of the form $A \ll B$ will mean that there exists a constant t such that $|A| \leq tB$. We may alternatively write $A = B + O(C)$ when $A - B \ll C$. A real valued function in several variables is said to be bounded if its absolute value is bounded above by a constant independent of the variables.

Let τ be a positive integer relatively prime to Δ. For any $s, H \in \mathbb{N}$, define $\mathscr{S}_s(H)$ to be the number of positive integers N in the interval $(s, s + H)$ which satisfy the conditions

$$\chi_i(N) = \eta_i, \text{ for } i = 1, \ldots, r \tag{2.2}$$

$$N \equiv \tau \mod \Delta. \tag{2.3}$$

Let $W = \{1, 2\}$. For any $\mathbf{e} = (e_1, \ldots, e_r) \in W^r$, let $\pi_{\mathbf{e}} := \prod_{i=1}^{r} (\eta_i \chi_i)^{e_i}$. When $\mathbf{e}_0 = (2, \ldots, 2)$, $\pi_{\mathbf{e}_0}$ is the principal character modulo Γ. We will say that $\chi_1, \ldots, \chi_r$ are independent if $\prod_{i=1}^{r} (\chi_i)^{e_i}$ is nonprincipal for all $(e_1, \ldots, e_r) \neq \mathbf{e}_0$.

Before we estimate $\mathscr{S}_s(H)$ we note that if we relax condition (2.3) to $\gcd(N, \Delta) = 1$ and define $S_s(H)$ to be the number of $N \in (s, s+H)$ satisfying this and (2.2), then the following proposition is a slight adjustment to [6, Proposition 3.6].

Proposition 2.10. *Suppose that $\chi_1, \ldots, \chi_r$ are independent. Let k be a fixed positive integer, $h = \min\{H : S_s(H) > k\}$, and $\omega(\Gamma)$ denote the number of distinct prime divisors of Γ. Then*

$$S_s(H) = 2^{-r}\frac{\phi(\Gamma\Delta)}{\Gamma\Delta}H + O(H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\epsilon}\Delta^{\epsilon}), \tag{2.4}$$

and if $r \leq \omega(\Gamma) + 1$, we have

$$h \ll \Gamma^{\frac{3}{8}+\epsilon}\Delta^{\epsilon}, \tag{2.5}$$

where ϕ is Euler's phi-function, the implied constant in (2.4) depends only on ϵ, and the implied constant in (2.5) depends only on ϵ and k.

Proof. As this proposition differs from [6, Proposition 3.6] only in the definition of h, (2.4) follows immediately. We then note that $S_s(H) > k$ whenever

$$\frac{\phi(\Gamma)}{2^r\Delta\Gamma}H + (1 - \frac{1}{2^r\phi(\Delta)})C(\Delta\Gamma)^{\frac{3}{16}+\epsilon}H^{\frac{1}{2}} - k > 0.$$

We may now proceed as in the proof of [6, Proposition 3.6], but notice that the resulting implied constant in (2.5) also depends on k. □

The main use of this next result will be to obtain an upper bound for the smallest positive integer h satisfying (2.2) and (2.3) in terms of the magnitude of Γ and given a fixed integer Δ. The initial bound for $\mathscr{S}_s(H)$ was obtained without fixing Δ so is written in generality.

Proposition 2.11. *If $\chi_1, \dots, \chi_r$ are independent, then*

$$\mathscr{S}_s(H) = 2^{-r}\frac{\phi(\Gamma)}{\Gamma\Delta}H + O(H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\epsilon}) \tag{2.6}$$

where ϕ denotes Euler's phi-function and the implied constant depends only on ϵ and Δ. Furthermore, let $\omega(\Gamma)$ be the number of distinct prime divisors of Γ and $h = \min\{H : \mathscr{S}_s(H) > k\}$ for any $k \in \mathbb{N}$. If Δ is a fixed positive integer, and $r \leq \omega(\Gamma) + 1$, then

$$h \ll \Gamma^{\frac{3}{8}+\epsilon}. \tag{2.7}$$

where the implied constant depends only on ϵ, Δ, and k.

Proof. Define a function Φ on $\mathbb{Z}$ by $\Phi(N) = \sum_{\mathbf{e}\in W^r} \pi_{\mathbf{e}}(N)$. Notice that if (2.2) holds for N, then $\pi_{\mathbf{e}}(N) = 1$ for all $\mathbf{e} \in W^r$. However, if (2.2) does not hold, then there exists some $1 \leq j \leq r$ for which either $\chi_j(N) = 0$, or $\eta_j\chi_j(N) = -1$. If there exists j with $\chi_j(N) = 0$, then $\pi_{\mathbf{e}}(N) = 0$ for all $\mathbf{e} \in W^r$. On the other hand if $\eta_j\chi_j(N) = -1$, without loss of generality we can assume $j = r$, then

$$\begin{aligned}\sum_{\mathbf{e}\in W^r} \pi_{\mathbf{e}}(N) &= \sum_{\mathbf{e}\in W^{r-1}} \pi_{\mathbf{e}}(N)(\eta_r\chi_r(N))^2 + \sum_{\mathbf{e}\in W^{r-1}} \pi_{\mathbf{e}}(N)(\eta_r\chi_r(N)) \\ &= \sum_{\mathbf{e}\in W^{r-1}} \pi_{\mathbf{e}}(N) \qquad\qquad - \sum_{\mathbf{e}\in W^{r-1}} \pi_{\mathbf{e}}(N) = 0.\end{aligned}$$

Therefore,

$$\Phi(N) = \begin{cases} 2^r & \text{if (2.2) holds for } N, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\widehat{G}_\Delta$ denote the group of all characters of $(\mathbb{Z}/\Delta\mathbb{Z})^\times$, and recall the following

identity:

$$\sum_{\psi \in \widehat{G}_\Delta} \psi(N) = \begin{cases} |\widehat{G}_\Delta| & \text{if } N \equiv 1 \mod \Delta, \\ 0 & \text{otherwise.} \end{cases}$$

Fix a positive integer t such that $t \cdot \tau \equiv 1 \mod \Delta$ and $t \equiv 1 \mod \Gamma$. Then $\chi_i(N) = \chi_i(tN)$ for all i and hence $\Phi(N) = \Phi(tN)$. Moreover, $N \equiv \tau \mod \Delta$ if and only if $tN \equiv 1 \mod \Delta$ and hence

$$\sum_{\psi \in \widehat{G}_\Delta} \psi(tN) = \begin{cases} |\widehat{G}_\Delta| & \text{if (2.3) holds for } N, \\ 0 & \text{otherwise.} \end{cases}$$

To prove (2.6) we will calculate

$$\sum_{N \in (s, s+H)} \sum_{\psi \in \widehat{G}_\Delta} (\psi \cdot \Phi)(tN)$$

in two different ways. First,

$$\begin{aligned} \sum_{N \in (s, s+H)} \sum_{\psi \in \widehat{G}_\Delta} (\psi \cdot \Phi)(tN) &= \sum_{N \in (s, s+H)} \Phi(tN) \cdot \left(\sum_{\psi \in \widehat{G}_\Delta} \psi(tN) \right) \\ &= \sum_{\substack{N \in (s, s+H) \\ N \equiv \tau \mod \Delta}} |\widehat{G}_\Delta| \Phi(tN) \\ &= \sum_{\substack{N \in (s, s+H) \\ N \equiv \tau \mod \Delta \\ \chi(N) = \eta}} 2^r \cdot |\widehat{G}_\Delta| \\ &= 2^r \cdot \phi(\Delta) \mathscr{S}_s(H). \end{aligned} \tag{2.8}$$

On the other hand, if we let ψ_0 be the principal character modulo Δ, we can

rewrite the sum on the left as

$$\sum_{N\in(s,s+H)}\sum_{\psi\in\widehat{G}_\Delta}(\psi\cdot\Phi)(tN)=\sum_{N\in(s,s+H)}\psi_0\cdot\pi_{\mathbf{e}_0}(tN)+\sum_{N\in(s,s+H)}\left(\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\psi\cdot\pi_{\mathbf{e}_0}(tN)\right)$$
$$+\sum_{N\in(s,s+H)}\left(\sum_{\psi\in\widehat{G}_\Delta}\sum_{\substack{\mathbf{e}\in W^r\\ \mathbf{e}\neq\mathbf{e}_0}}\psi\cdot\pi_{\mathbf{e}}(tN)\right).$$

Whenever $\psi\neq\psi_0$ or $\mathbf{e}\neq\mathbf{e}_0$, $\psi\cdot\prod_{i=1}^r(\chi_i)^{e_i}$ is a nonprincipal character modulo $\Gamma\Delta$. We also note that $\pi_{\mathbf{e}}:=\prod_{i=1}^r(\eta_i\chi_i)^{e_i}=\prod_{i=1}^r\eta_i^{e_i}\prod_{i=1}^r\chi_i^{e_i}$, and so $\pi_{\mathbf{e}}$ is not necessarily a character. However, it does differ from one by at most a negative sign and $|\pi_{\mathbf{e}}|=|\prod_{i=1}^r\chi_i^{e_i}|$. Furthermore, as $|\psi\cdot\pi_{\mathbf{e}_0}(t)|=1$, we obtain

$$\left|\sum_{N\in(s,s+H)}\left(\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\psi\cdot\pi_{\mathbf{e}_0}(tN)\right)\right|\leq\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\left|\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}_0}(tN)\right|$$
$$=\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\left|\psi(t)\pi_{\mathbf{e}_0}(t)\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}_0}(N)\right|$$
$$=\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\left|\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}_0}(N)\right|.$$

Therefore, as $\pi_{\mathbf{e}_0}$ is a character modulo Γ, we can apply Burgess's estimate for

character sums [2, Theorem 2] to $\left|\sum_{N\in(s,s+H)} \psi\cdot\pi_{\mathbf{e}_0}(N)\right|$ to obtain

$$\sum_{N\in(s,s+H)}\left(\sum_{\substack{\psi\in\widehat{G}_\Delta\\ \psi\neq\psi_0}}\psi\cdot\pi_{\mathbf{e}_0}(tN)\right)=(\phi(\Delta)-1)O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).$$

Similarly, we obtain

$$\left|\sum_{N\in(s,s+H)}\left(\sum_{\psi\in\widehat{G}_\Delta}\sum_{\substack{\mathbf{e}\in W^r\\ \mathbf{e}\neq\mathbf{e}_0}}\psi\cdot\pi_{\mathbf{e}}(tN)\right)\right|\leq\sum_{\psi\in\widehat{G}_\Delta}\sum_{\substack{\mathbf{e}\in W^r\\ \mathbf{e}\neq\mathbf{e}_0}}\left|\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}}(tN)\right|$$

where

$$\left|\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}}(tN)\right|=\left|\sum_{N\in(s,s+H)}\psi\cdot\pi_{\mathbf{e}}(N)\right|=\left|\sum_{N\in(s,s+H)}\psi\cdot\chi_i^{e_i}(N)\right|.$$

Therefore, we can again apply Burgess's estimate to obtain

$$\sum_{N\in(s,s+H)}\left(\sum_{\psi\in\widehat{G}_\Delta}\sum_{\substack{\mathbf{e}\in W^r\\ \mathbf{e}\neq\mathbf{e}_0}}\psi\cdot\pi_{\mathbf{e}}(tN)\right)=(2^r-1)\phi(\Delta)O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).$$

Hence

$$\sum_{N\in(s,s+H)}\sum_{\psi\in\widehat{G}_\Delta}(\psi\cdot\Phi(tN))=\sum_{N\in(s,s+H)}\psi_0\cdot\pi_{\mathbf{e}_0}(tN)+(2^r\phi(\Delta)-1)O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).$$

Furthermore, using the special case $r = 0$ in Proposition 2.10 we obtain

$$\begin{aligned}\sum_{N\in(s,s+H)} \psi_0 \cdot \pi_{\mathbf{e}_0}(tN) &= \sum_{\substack{N\in(s,s+H)\\ \gcd(N,\Gamma\Delta)=1}} 1 \\ &= \frac{\phi(\Gamma\Delta)}{\Gamma\Delta} H + O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).\end{aligned}$$

Hence

$$\sum_{N\in(s,s+H)} \sum_{\psi\in\widehat{G}_\Delta} (\psi \cdot \Phi(tN)) = \frac{\phi(\Gamma\Delta)}{\Gamma\Delta} H + (2^r\phi(\Delta))O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).$$

Therefore, combining this with (2.8) gives the desired result:

$$\mathscr{S}_s(H) = \frac{\phi(\Gamma)}{2^r\Gamma\Delta} H + O(H^{\frac{1}{2}}(\Gamma\Delta)^{\frac{3}{16}+\epsilon}).$$

If we assume that Δ is a fixed integer and set $\delta = \frac{\epsilon}{6}$, this equation now guarantees the existence of a positive constant C such that

$$\mathscr{S}_s(H) \geq \frac{\phi(\Gamma)}{2^r\Gamma\Delta} H - CH^{\frac{1}{2}}(\Gamma)^{\frac{3}{16}+\delta}$$

for all $H > 0$. It follows that $\mathscr{S}_s(H) > k$, whenever

$$\frac{\phi(\Gamma)}{2^r\Gamma\Delta} H - C(\Gamma)^{\frac{3}{16}+\delta} H^{\frac{1}{2}} - k > 0.$$

Hence $\mathscr{S}_s(H) > k$ whenever

$$\sqrt{H} > \frac{C(\Gamma)^{\frac{3}{16}+\delta} + \sqrt{(C(\Gamma)^{\frac{3}{16}+\delta})^2 + 4k\frac{\phi(\Gamma)}{2^r\Gamma\Delta}}}{\frac{2\phi(\Gamma)}{2^r\Gamma\Delta}}.$$

Observe that $\frac{\Gamma}{\phi(\Gamma)} \ll \Gamma^{\epsilon}$ (for example see [13]) and $2^r \ll 2^{\omega(\Gamma)} \leq \tau(\Gamma) \ll \Gamma^{\epsilon}$, see [1, pg. 296], where the implied constants depend only on ϵ, and $\tau(\Gamma)$ denotes the number of positive divisors of Γ. Therefore, using $\delta = \frac{\epsilon}{6}$ again, we obtain

$$
\begin{aligned}
&2^{r-1}\Delta\frac{\Gamma}{\phi(\Gamma)}\left(C(\Gamma)^{\frac{3}{16}+\delta} + \sqrt{(C(\Gamma)^{\frac{3}{16}+\delta})^2 + 4k\frac{\phi(\Gamma)}{2^r\Gamma\Delta}}\right) \\
&\quad \ll 2^{r-1}\Delta\frac{\Gamma}{\phi(\Gamma)}(\Gamma)^{\frac{3}{16}+\delta} + 2^{r-1}\Delta\frac{\Gamma}{\phi(\Gamma)}\sqrt{(C(\Gamma)^{\frac{3}{16}+\delta})^2} + \frac{2^{r-1}\Gamma\Delta}{\phi(\Gamma)}\sqrt{k\frac{\phi(\Gamma)}{2^{r-2}\Gamma\Delta}} \\
&\quad \ll \Gamma^{2\delta}(\Gamma)^{\frac{3}{16}+\delta} + \Gamma^{2\delta}(\Gamma)^{\frac{3}{16}+\delta} + \sqrt{k\frac{2^r\Gamma\Delta}{\phi(\Gamma)}} \\
&\quad \ll \Gamma^{\frac{3}{16}+3\delta} + \sqrt{k\Delta}\sqrt{\Gamma^{2\delta}} \\
&\quad \ll \Gamma^{\frac{3}{16}+\frac{\epsilon}{2}}.
\end{aligned}
$$

The last bound is achieved by noting that $\sqrt{k\Delta}$ is bounded, $\Gamma^{\delta} \leq \Gamma^{\frac{3}{16}+3\delta}$, and then substituting $\frac{\epsilon}{6}$ back in for δ. Therefore, $\sqrt{h} \ll \Gamma^{\frac{3}{16}+\frac{\epsilon}{2}}$ where the implied constant depends only on k, Δ, and ϵ. The desired result $h \ll \Gamma^{\frac{3}{8}+\epsilon}$ then follows.

□

Chapter 3

Primitive Regular Ternary $\mathbb{Z}$-cosets

Similar to the methods used in [16], [6], and [7], we will prove a finiteness result for primitive regular ternary $\mathbb{Z}$-cosets by showing that the discriminant of the corresponding lattice is bounded. We first establish in Section 3.1 some local results for primitive regular $\mathbb{Z}$-cosets. In Section 3.2 we will bound the discriminant of a $\mathbb{Z}$-coset which behaves well at all primes not dividing the conductor. We will then prove the main result in Section 3.3.

3.1 Local Representations of Primitive Regular Quadratic Polynomials

As the study of global representations of regular polynomials can be viewed as a local question, we begin with some local results for primitive quadratic polynomials.

Proposition 3.1. *Let $f(\mathbf{x})$ be a primitive quadratic polynomial with $f(0) = 0$. If p is an odd prime, then $f(\mathbf{x})$ represents all of the coset $p^k\mathbb{Z}_p + r$, for some $0 \leq k \leq 1$ and $r \in \{0, \ldots, p^k - 1\}$.*

Proof. Every quadratic form is diagonalizable over $\mathbb{Z}_p$ when p is an odd prime [3, Ch. 8 Theorem 3.1]. Therefore, we may assume that $f(\mathbf{x})$ is of the form

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \sum_{1 \leq i \leq n} a_i x_i^2 + b_i x_i.$$

The condition of primitivity guarantees that f is an integral quadratic polynomial and hence $\{a_i, b_i | 1 \leq i \leq n\} \subseteq \mathbb{Z}_p$. Furthermore, the primitivity of f guarantees the existence of an $i \leq n$ with either a_i or b_i a p-adic unit, since otherwise $\mathfrak{n}(f) \subseteq p\mathbb{Z}$. Therefore, it is enough to consider representations of a polynomial of the form $ax^2 + bx$ where either $a \in \mathbb{Z}_p^\times$ or $b \in \mathbb{Z}_p^\times$.

First, suppose that $a, b \in \mathbb{Z}_p^\times$. Then for any $\epsilon \in \mathbb{Z}_p$, $h(x) = ax^2 + bx - \epsilon$ has an integral solution when

$$x = \frac{-b \pm \sqrt{b^2 + 4a\epsilon}}{2a}$$

is in $\mathbb{Z}_p$. Our choice of a guarantees that $2a \in \mathbb{Z}_p^\times$ and so $h(x)$ has a solution over $\mathbb{Z}_p$ exactly when $b^2 + 4a\epsilon$ is a square in $\mathbb{Z}_p$. Since $b, a \in \mathbb{Z}_p^\times$, whenever $\epsilon \in p\mathbb{Z}_p$ the local square theorem [15, 63.1] guarantees that $b^2 + 4a\epsilon$ is in fact a square in $\mathbb{Z}_p$. Therefore, $ax^2 + bx$ represents all of $p\mathbb{Z}_p$ whenever $a, b \in \mathbb{Z}_p^\times$.

Next, suppose that $b \in \mathbb{Z}_p^\times$ and $p|a$. Let $\epsilon \in \mathbb{Z}_p$ and $\gamma \in \mathbb{Z}_p$ be such that $\gamma = b^{-1}\epsilon$. Consider the polynomial $h(x) = ax^2 + bx - \epsilon$. Then $h(\gamma) = a\gamma^2 + b\gamma - \epsilon \equiv b\gamma - \epsilon \equiv 0 \mod p$ and $h'(\gamma) = 2a\gamma + b \equiv b \not\equiv 0 \mod p$; hence Hensel's lemma guarantees the existence of $\alpha \in \mathbb{Z}_p$ such that $h(\alpha) = 0$. Thus, when $b \in \mathbb{Z}_p^\times$ and $p|a$, $ax^2 + bx$ represents all of $\mathbb{Z}_p$.

Finally, suppose that $p|b$ and $a \in \mathbb{Z}_p^\times$. Then as above, since $a \in \mathbb{Z}_p^\times$, $h(x) = ax^2 + bx - \epsilon$ has a solution over $\mathbb{Z}_p$ exactly when $b^2 + 4a\epsilon$ is a square. If $\epsilon \equiv a \mod p$ then $4a\epsilon \equiv 4a^2 \mod p$ and so $4a\epsilon = l^2$ for some $l \in \mathbb{Z}_p^\times$. As $p|b^2$, the local square theorem guarantees that $b^2 + 4a\epsilon$ is a square. Therefore, $ax^2 + bx$ will represent all of the coset $a + p\mathbb{Z}_p$, or equivalently $r + p\mathbb{Z}_p$ where $r \in \{0, \ldots, p-1\}$ such that $r \equiv a \mod p$.

This exhausts all possibilities for a and b, therefore $ax^2 + bx$ and hence $f(x)$ is either $\mathbb{Z}_p$-universal, represents all of $p\mathbb{Z}_p$, or represents a coset $p\mathbb{Z}_p + r$ with $r \in \{0, \ldots, p-1\}$. □

Proposition 3.2. *Let $f(\mathbf{x})$ be a primitive quadratic polynomial such that $f(0) = 0$. Over $\mathbb{Z}_2$, $f(\mathbf{x})$ represents all of the coset $2^k\mathbb{Z}_2 + r$, for some $0 \leq k \leq 5$ and $r \in \{0, \ldots, 2^k - 1\}$.*

Proof. Let

$$f(\mathbf{x}) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j + \sum_{1 \leq i \leq n} b_i x_i.$$

The primitivity of f guarantees that it is an integral quadratic polynomial and hence $\{a_{ij}, b_j | 1 \leq i \leq j \leq n\} \subseteq \frac{1}{2}\mathbb{Z}$. Fix $1 \leq i \leq n$, and consider the polynomial $a_{ii}x^2 + b_i x$. Suppose that $\mathrm{ord}_2(b_i) = -1$. Then as f is integral, it must also be the case that $\mathrm{ord}_2(a_{ii}) = -1$. Therefore, $a_{ii}x^2 + b_i x = \frac{ax^2+bx}{2}$ where a and b are odd integers. Let $\epsilon \in \mathbb{Z}_2$ and consider the equation $ax^2 + bx = 2\epsilon$. By completing the square this equation becomes $(2ax + b)^2 = 8a\epsilon + b^2$. Since $b \in \mathbb{Z}_2^\times$, this is equivalent to $(2axb^{-1} + 1)^2 = 8ab^{-2}\epsilon + 1$ which, by the local square theorem [15, Theorem 63.1], always has a solution $x \in \mathbb{Z}_2$ when $a, b \in \mathbb{Z}_2^\times$. Therefore if there exists i with $\mathrm{ord}_2(b_i) = -1$ and $\mathrm{ord}_2(a_{ii}) = -1$, then f is universal over $\mathbb{Z}_2$.

We may henceforth assume that $b_i, a_{ii} \in \mathbb{Z}$ for all i. So, let us consider the polynomial $ax^2 + bx$ with $a, b \in \mathbb{Z}$. If $\mathrm{ord}_2(b) = 0$, then for any $\epsilon \in 2\mathbb{Z}_2$, the

equation $ax^2 + bx = \epsilon$ is always solvable in $\mathbb{Z}_2$ by the local square theorem. In this case, f represents all of $2\mathbb{Z}_2$.

Next we consider the case when $b \in 2\mathbb{Z}$ and a is an odd integer. The roots of the polynomial the polynomial $ax^2 + bx - \epsilon$ are

$$\frac{-b \pm \sqrt{b^2 + 4a\epsilon}}{2a}.$$

Since $a \in \mathbb{Z}_2^\times$ and $2|b$, these elements are in $\mathbb{Z}_2$ whenever $\sqrt{b^2 + 4a\epsilon} \in 2\mathbb{Z}_2$ or equivalently whenever $b^2 + 4a\epsilon$ is a square in $4\mathbb{Z}_2$. We now consider some cases based on the 2-adic order of b. If $2||b$, then $\sqrt{b^2 + 4a\epsilon} = 2\sqrt{d^2 + a\epsilon}$ where $d \in \mathbb{Z}_2^\times$. The local square theorem then guarantees that $d^2 + a\epsilon$ is a square in $\mathbb{Z}_2$ whenever $\epsilon \in 2^3\mathbb{Z}_2$. Now if $4||b$, then by the local square theorem $\sqrt{b^2 + 4a\epsilon} = 4\sqrt{d^2 + 2^{-2}a\epsilon}$ has a solution whenever $\epsilon \in 2^5\mathbb{Z}_2$. Finally, if $8|b$ then $\sqrt{b^2 + 4a\epsilon} = 2\sqrt{16d^2 + a\epsilon}$ where $d \in \mathbb{Z}_2$. By choosing ϵ so that $\epsilon \equiv a \mod 8$ we see that

$$16d^2 + a\epsilon = 16d^2 + a(a + 8\epsilon') = 8(2d^2 + \epsilon') + a^2$$

where $a \in \mathbb{Z}_2^\times$. Therefore the local square theorem will guarantee that this is a square and hence if $8|b$, $ax^2 + bx$ represents all of the coset $a + 2^3\mathbb{Z}_2$. By choosing a proper representative $r \equiv a \mod 8$, f represents all of $r + 2^3\mathbb{Z}_2$. Therefore, in this case f must represent all of a coset $r + 2^k\mathbb{Z}_2$ where $r \in \{0, \ldots, 2^k - 1\}$ and $k \leq 5$.

Finally we assume that for all i, $a_{ii}, b_i \in 2\mathbb{Z}$. Then, by the primitivity of f, there exists $i \neq j$ with $a_{ij} \in \frac{1}{2}\mathbb{Z}_2^\times$. Let $L = \mathbb{Z}^n$ be the lattice imposed with the quadratic form $Q(\mathbf{x}) = \sum_{1 \leq i,j \leq n} a_{ij}x_ix_j$. Then $\mathfrak{s}(L) = \frac{1}{2}\mathbb{Z}$ and $\mathfrak{n}(L) = \mathbb{Z}$. Therefore, there exists $\mathbf{w} \in L_2$ such that $Q(\mathbf{w}) = a$ for some $a \in \mathbb{Z}_2^\times$. Let $\mathbf{v} \in \mathbb{Q}^n$

be the vector such that $2B(\mathbf{v},\mathbf{x}) = \sum_{1\le i\le n} b_i x_i$ for all $\mathbf{x} \in \mathbb{Q}^n$. Then, since $b_i \in 2\mathbb{Z}$, $B(\mathbf{v},\mathbf{x}) \in \mathbb{Z}$ for all $\mathbf{x} \in L$. In particular, $B(\mathbf{v},\mathbf{w}) =: d \in \mathbb{Z}_2$, and so

$$f(\lambda\mathbf{w}) = a\lambda^2 + 2d\lambda, \text{ for all } \lambda \in \mathbb{Z}_2.$$

As is covered in the previous paragraph, this polynomial, and hence f, represents all of a coset $r + 2^k\mathbb{Z}_2$, for some $r \in \{0,\dots,2^k-1\}$ and $k \le 5$.

This exhausts all possibilities for the coefficients of f and hence we get the desired result. □

Corollary 3.3. *Let $L+\mathbf{v}$ be a primitive $\mathbb{Z}$-coset of conductor $\mathfrak{c}$. If p is a prime such that $p|2\mathfrak{c}$, then $L_p+\mathbf{v}$ represents $p^{k_p}\mathbb{Z}_p + r_p$ for some $0 \le k_p \le 7+ord_p(\mathfrak{c})$ and $r_p \in \{0,1,\dots,p^{k_p}-1\}$.*

Proof. As a primitive $\mathbb{Z}$-coset of conductor $\mathfrak{c}$, $L+\mathbf{v}$ can be associated with a primitive complete quadratic polynomial $f(\mathbf{x})+Q(\mathbf{v})$ where $f(\mathbf{x}) = Q(\mathbf{x}) + 2B(\mathbf{v},\mathbf{x})$ and $\mathfrak{n}(f) = \alpha\mathbb{Z} \supseteq 4\mathfrak{c}\mathbb{Z}$. Therefore, $\frac{f(\mathbf{x})}{\alpha}$ is a primitive quadratic polynomial and so by Propositions 3.1 and 3.2 over $\mathbb{Z}_p$, $\frac{f}{\alpha}$ represents all of a coset of the form $p^k\mathbb{Z}_p + r$, where $0 \le k \le 5$, and $0 \le r \le p^k-1$. Since $\alpha|4\mathfrak{c}$ over $\mathbb{Z}_p$, f represents all of a coset of the form $p^{k_p}\mathbb{Z}_p + s_p$ where $0 \le k_p \le 7+\mathrm{ord}_p(\mathfrak{c})$ and $s_p \in \{0,1,\dots,p^{k_p}-1\}$. Therefore, over $\mathbb{Z}_p$ $f(\mathbf{x})+Q(\mathbf{v})$ represents all of $p^{k_p}\mathbb{Z}_p+r_p$ where $r_p \in \{0,1,\dots,p^{k_p}-1\}$ such that $r_p \equiv s_p + Q(\mathbf{v}) \mod p^{k_p}$. Since $L_p+\mathbf{v}$ represents a if and only if $f(\mathbf{x})+Q(\mathbf{v})$ represents a over $\mathbb{Z}_p$, we have the desired result. □

3.2 Bounding Prime Divisors of the Discriminant of a $\mathbb{Z}$-coset

In this section we bound the prime divisors of the discriminant of a primitive regular $\mathbb{Z}$-coset with a fixed conductor. Recall that a positive ternary quadratic polynomial is called *Minkowski reduced*, or just *reduced*, if its quadratic part is Minkowski reduced and it attains its minimum at the zero vector. When we say a quadratic form is reduced we mean it is Minkowski reduced as described in [3, Chapter 12]. We begin by citing a few technical lemmas before stating the main proposition of this section. The following two results are Lemma 2.3 and Lemma 3.4, respectively, from [6].

Lemma 3.4. *Let $Q(\mathbf{x})$ be a positive definite reduced ternary quadratic form. Then for any $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$,*

$$Q(\mathbf{x}) \geq \frac{1}{6}(Q(\mathbf{e}_1)x_1^2 + Q(\mathbf{e}_2)x_2^2 + Q(\mathbf{e}_3)x_3^2).$$

Lemma 3.5. *Let T be a finite set of primes and a be an integer not divisible by any prime in T. For any integer d, the number of integers in the set $\{d, a + d, \ldots, (n-1)a + d\}$ that are not divisible by any prime in T is at least*

$$n\frac{\tilde{p} - 1}{\tilde{p} + t - 1} - 2^t + 1,$$

where $t = |T|$ and $\tilde{p}$ is the smallest prime in T.

Lemma 3.6. *Let $L + \mathbf{v}$ be a primitive ternary $\mathbb{Z}$-coset on a quadratic space (V, Q). Fix a Minkowski basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ for L and let $\{\mu_1, \mu_2, \mu_3\}$ be the successive minima of L. Given $\mathbf{x} \in L$ we write $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3$ where $(x_1, x_2, x_3) \in \mathbb{Z}^3$.*

1. *If* $|x_3| \geq 9$, *we have* $Q(\mathbf{x}+\mathbf{v}) \geq \frac{3}{2}\mu_3$.

2. *If* $|x_3| \leq 8$ *and* $|x_2| \geq 22$, *then* $Q(\mathbf{x}+\mathbf{v}) \geq \frac{7}{2}\mu_2$.

3. *If* $|x_3| \leq 8$ *and* $|x_2| \leq 21$, *then* $Q(\mathbf{x}+\mathbf{v}) \geq x_1^2 - 30|x_1|$.

4. *If* $|x_3| \leq 8$, $|x_2| \leq 21$, *and* $|x_1| \geq 31$, *then* $Q(\mathbf{x}+\mathbf{v}) \geq 31\mu_1$.

Proof. By Lemma 3.4 and the facts that $2|B(\mathbf{v},\mathbf{e}_i)| \leq Q(\mathbf{e}_i)$ and $Q(\mathbf{x}+\mathbf{v}) \geq Q(\mathbf{x}) + 2B(\mathbf{v},\mathbf{x})$, we have

$$\begin{aligned} Q(\mathbf{x}+\mathbf{v}) &\geq \sum_{i=1}^{3}(\frac{1}{6}\mu_i x_i^2 - 2w_i x_i) \\ &\geq \sum_{i=1}^{3}\mu_i(\frac{1}{6}x_i^2 - |x_i|). \end{aligned}$$

So if $|x_3| \geq 9$, then

$$Q(\mathbf{x}+\mathbf{v}) \geq -\frac{3}{2}\mu_1 - \frac{3}{2}\mu_2 + \frac{9}{2}\mu_3 \geq \frac{3}{2}\mu_3.$$

Suppose now that $|x_3| \leq 8$. Since $2|a_{12}| \leq \mu_1 \leq \mu_2$, one obtains $4a_{12} - \mu_1\mu_2 \leq 0$ and hence

$$\frac{\mu_1}{2}x_1^2 + 2a_{12}x_1x_2 + \frac{\mu_2}{2}x_2^2 \geq 0$$

for all $(x_1, x_2) \in \mathbb{Z}^2$. So, if $|x_2| \geq 22$, then

$$\begin{aligned} Q(\mathbf{x}+\mathbf{v}) \geq & Q(x_1\mathbf{e}_1 + x_2\mathbf{e}_2) + Q(x_3\mathbf{e}_3 + \mathbf{v}) - \frac{\mu_1}{2}x_1^2 + 2a_{12}x_1x_2 + \frac{\mu_2}{2}x_2^2 \\ \geq & \frac{\mu_1}{2}x_1^2 + 2(a_{13}x_3 + w_1)x_1 + \frac{\mu_2}{2}x_2^2 + 2(a_{23}x_3 + w_2)x_2 + Q(x_3\mathbf{e}_3 + \mathbf{v}) \\ \geq & -\frac{81}{2}\mu_1 + 44\mu_2 \\ \geq & \frac{7}{2}\mu_2. \end{aligned}$$

Now let us assume further that $|x_2| \leq 21$. Then

$$\begin{aligned} Q(\mathbf{x}+\mathbf{v}) =& \mu_1 x_1^2 + 2(a_{12}x_2 + a_{13}x_3 + w_1)x_1 + Q(x_2\mathbf{e}_2 + x_3\mathbf{e}_3 + \mathbf{v}) \\ \geq& \mu_1(x_1^2 - 30|x_1|) \\ \geq& x_1^2 - 30|x_1|. \end{aligned}$$

If in addition we let $|x_1| \geq 31$, then

$$\begin{aligned} Q(\mathbf{x}+\mathbf{v}) \geq& \mu_1(x_1^2 - 30|x_1|) \\ \geq& 31\mu_1. \end{aligned}$$

□

Therefore,

$$Q(\mathbf{x}+\mathbf{v}) \geq \min\left\{\frac{3}{2}\mu_3, \frac{7}{2}\mu_2, 31\mu_1\right\}$$

unless $|x_1| \leq 30$, $|x_2| \leq 21$, and $|x_3| \leq 8$.

Corollary 3.7. *There are at most* 44591 *elements* $\mathbf{x} \in L$ *such that*

$$Q(\mathbf{x}+\mathbf{v}) < \min\left\{\frac{3}{2}\mu_3, \frac{7}{2}\mu_2, 31\mu_1\right\}.$$

It is now convenient to introduce the following notation. Fix a primitive regular ternary $\mathbb{Z}$-coset $L+\mathbf{v}$ of conductor $\mathfrak{c}$. At every prime $p|2\mathfrak{c}$, Lemma 3.3 guarantees that $L_p+\mathbf{v}$ represents all of a coset $p^{k_p}\mathbb{Z}_p+r_p$ where k_p and r_p are integers bounded by a constant depending only on $\mathfrak{c}$. Let r be the smallest non-negative integer such that $r \equiv r_p \mod p^{k_p}$ for all $p|2\mathfrak{c}$, and also set $a := \prod_{p|2\mathfrak{c}} p^{k_p}$. Then, a and r are both positive integers which are bounded by a constant only depending on $\mathfrak{c}$.

Proposition 3.8. *Let* $L+\mathbf{v}$ *be a primitive regular ternary* $\mathbb{Z}$*-coset with conductor*

$\mathfrak{c}$. *There exists a constant C, depending only on $\mathfrak{c}$, such that if $L+\mathbf{v}$ behaves well at all primes $p \nmid 2\mathfrak{c}$ then $dL \leq C$.*

Proof. Fix a Minkowski basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ for L. Let T be the set of odd primes p such that $p \nmid \mathfrak{c}$ and L_p is not split by $\mathbb{H}$. Then T is a finite set. Let $t = |T|$, $\tilde{p}$ be the smallest prime in T, and $\mathfrak{T}$ be the product of primes in T. Note that since $\tilde{p} > 2$, we have

$$\omega := \frac{\tilde{p}+t-1}{\tilde{p}-1} \leq t+1.$$

Also, for convenience we set $Q(\mathbf{e}_i) = \mu_i$, $B(\mathbf{v}, \mathbf{e}_i) = w_i$, and $B(\mathbf{e}_i, \mathbf{e}_j) = a_{ij}$ for $i \neq j$. Let (x_1, x_2, x_3) denote a vector in $\mathbb{Z}^3$ and $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3$. Finally we let $\gamma(L+\mathbf{v}) := \min\left\{\frac{3}{2}\mu_3, \frac{7}{2}\mu_2, 31\mu_1\right\}$ and notice that Corollary 3.7 states that there are at most 44591 elements $\mathbf{x}$ of L with $Q(\mathbf{x}+\mathbf{v}) < \gamma(L+\mathbf{v})$.

Consider the positive integers $ak+r$, where $k \in \mathbb{N}$. If $p|2\mathfrak{c}$ then by Lemma 3.3 and our choice of a and r, $L_p + \mathbf{v}$ represents $ak+r$. If $p \nmid 2\mathfrak{c}$ then as $L+\mathbf{v}$ behaves well at such a prime, either L_p is split by $\mathbb{H}$ or $p \in T$. If L_p is split by $\mathbb{H}$ then $L_p + \mathbf{v} = L_p$ is universal and represents $ak+r$. Otherwise, if $p \in T$ then since L behaves well at p, L_p represents those $ak+r$ which are relatively prime to p [15, Corollary 92.1b]. Therefore, the regularity of $L+\mathbf{v}$ guarantees that it will represent all integers $ak+r$ with $k \in \mathbb{N}$ that are relatively prime to $\mathfrak{T}$.

In order to bound dL, we first bound each of the successive minima of L starting with μ_1. Let $n = (t+1)(44591+2^t)$. Since $t+1 \geq \omega$,

$$n \geq \omega(44591+2^t) = \frac{\tilde{p}+t-1}{\tilde{p}-1}(44591+2^t).$$

By Lemma 3.5, the set $\{r, a+r, \ldots, a(n-1)+r\}$ contains at least

$$n\frac{\tilde{p}-1}{\tilde{p}+t-1} - 2^t + 1 > 44591$$

elements represented by $L+\mathbf{v}$. Therefore, there exists $k_1 \in \mathbb{N}$ with $n > k_1 \geq 0$ such that ak_1+r is represented by $L+\mathbf{v}$ and $ak_1+r \geq \gamma(L+\mathbf{v})$. Then, as $a > r$,

$$\begin{aligned}\mu_1 \leq \gamma(L+\mathbf{v}) \leq ak_1+r &< a(t+1)(44591+2^t)+r \\ &\ll (t+1)(44591+2^t) \\ &\ll t2^t,\end{aligned}$$

where the implied constant depends only on a.

Next, we bound μ_2. Let η be the smallest positive integer such that

$$\eta > [43 \cdot 17 \cdot (2(15+\sqrt{225+a\eta+r})+1)+2^t-1]\omega. \tag{3.1}$$

By means of contradiction, let us suppose $\frac{3}{2}\mu_2 > a\eta+r$. Then for any positive integer $s \leq a\eta+r$, Proposition 3.6 states that if $Q(\mathbf{x}+\mathbf{v})=s$, then $|x_2| \leq 21$, $|x_3| \leq 8$, and $Q(\mathbf{x}+\mathbf{v}) \geq \mu_1(x_1^2-30|x_1|) \geq x_1^2-30|x_1|$. Therefore, if

$$|x_1| > 15+\sqrt{225+a\eta+r}$$

then $Q(\mathbf{x}+\mathbf{v}) > a\eta+r$. This shows that the number of integers smaller than $a\eta+r$ which are represented by $L+\mathbf{v}$ is at most

$$43 \cdot 17 \cdot (2(15+\sqrt{225+a\eta+r})+1).$$

With $n = \eta$ in Lemma 3.5, we notice that the number of elements in the set $\{r, a+r, \ldots, a(\eta-1)+r\}$ which are represented by $L+\mathbf{v}$ is at least $\eta\frac{\tilde{p}-1}{\tilde{p}+t-1} - 2^t + 1$. However, from (3.1) we see that

$$\eta\frac{\tilde{p}-1}{\tilde{p}+t-1} - 2^t + 1 > 43 \cdot 17 \cdot (2(15 + \sqrt{225 + a\eta + r}) + 1).$$

Therefore, the number of positive integers smaller than $a\eta+r$ that are represented by $L+\mathbf{v}$ is strictly greater than $43\cdot17\cdot(2(15+\sqrt{225 + a\eta + r})+1)$. This contradicts our earlier claim. Therefore we must have

$$\mu_2 \leq \frac{2}{3}(a\eta + r).$$

Now let us estimate the size of η. Recall that $\omega \leq t + 1$ and then observe that

$$\sqrt{225 + a\eta + r} \leq 15 + \sqrt{a\eta + r}.$$

Now if $a = 1$ then $r = 0$ and so $\sqrt{225 + a\eta + r} \leq 15 + \sqrt{\eta}$; otherwise $a > 1$ and so $\sqrt{a\eta + r} \leq \sqrt{a\eta + a} \leq a\sqrt{\eta}$. Either way we have

$$\sqrt{225 + a\eta + r} \leq 15 + a\sqrt{\eta}.$$

Let η' be the smallest positive integer which satisfies

$$\eta' > [43 \cdot 17 \cdot (2(30 + a\sqrt{\eta'}) + 1) + 2^t - 1](t + 1).$$

Then by comparing this to the definition of η we see that $\eta' \geq \eta$. Therefore it

suffices to bound η' instead. To do so we consider the inequality

$$\eta' - 1462(t+1)a\sqrt{\eta'} - (44590 + 2^t)(t+1) > 0.$$

Then η' is the smallest integer such that

$$\sqrt{\eta'} > \frac{1462a(t+1) + \sqrt{(1462a(t+1))^2 + 4(44590 + 2^t)(t+1)}}{2}.$$

Now,

$$\frac{1462a(t+1) + \sqrt{(1462a(t+1))^2 + 4(44590 + 2^t)(t+1)}}{2} \ll \sqrt{t2^t}.$$

Therefore, we conclude that $\sqrt{\eta'} \ll \sqrt{t2^t}$ and hence

$$\mu_2 \leq \frac{2}{3}(a\eta + r) \ll \eta < \eta' \ll t2^t,$$

where the implied constant depends only on a.

Finally, we will bound μ_3. Recall from Proposition 3.6 that if $|x_3| \geq 9$, then $Q(\mathbf{x} + \mathbf{v}) \geq \frac{3}{2}\mu_3$. Let M be a sublattice of L defined by $M :=\text{span}_{\mathbb{Z}}\{\mathbf{e}_1, \mathbf{e}_2\}$ and $\mathfrak{A}$ be the product of those primes in T that do not divide dM. The successive minima of the binary lattice M are μ_1 and μ_2. So by Proposition 2.9 we have $dM \leq \mu_1\mu_2$. Let $q_1 < \cdots < q_{17}$ be the smallest 17 distinct primes such that $\left(\frac{-dM}{q_i}\right) = -1$, $\gcd(q_i, a) = 1$, and $q_i \notin T$ for all i. Set $\mathfrak{M} = \prod_{1 \leq i \leq 17} q_i$.

In order to estimate the size of each of these primes we will repeatedly use Proposition 2.10 to show that $q_i \ll dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}q_i^{i\epsilon}$, where the implied constant depends only on a and ϵ. To bound q_1 we use Proposition 2.10 with $k = 0$, the character modulo $8dM$ defined by the Jacobi symbol $\left(\frac{-dM}{*}\right) = -1$, $\Delta = \mathfrak{A}a$, and

$\Gamma = dM$, to obtain

$$q_1 \ll dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon} \leq dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}q_1^{\epsilon}.$$

We next bound q_i for any $2 \leq i \leq 17$ by using Proposition 2.10 with $k = 0$, the character modulo $8dM$ defined by the Jacobi symbol $\left(\frac{-dM}{*}\right) = -1$, $\Delta = \mathfrak{A}aq_1 \cdots q_{i-1}$, and $\Gamma = dM$. This gives

$$\begin{aligned} q_i \ll & dM^{\frac{3}{8}+\epsilon}(\mathfrak{A}aq_1 \cdots q_{i-1})^{\epsilon} \\ \ll & dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}(q_1 \cdots q_{i-1})^{\epsilon} \\ \leq & dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}((q_{i-1})^{i-1})^{\epsilon} \\ < & dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}(q_i)^{i\epsilon}. \end{aligned}$$

Fix $\epsilon > 0$ and let $\delta = \frac{\epsilon}{17}$ be used in the above bound for the q_i. Then

$$\begin{aligned} \mathfrak{M} = q_1 \cdots q_{17} \ll & dM^{17(\frac{3}{8}+\delta)}\mathfrak{A}^{17\delta}q_1^{\delta} \cdots q_{17}^{17\delta} \\ \leq & dM^{(\frac{51}{8}+17\delta)}\mathfrak{A}^{17\delta}q_1^{17\delta} \cdots q_{17}^{17\delta} \\ = & dM^{(\frac{51}{8}+\epsilon)}\mathfrak{A}^{\epsilon}\mathfrak{M}^{\epsilon}. \end{aligned}$$

Therefore $\mathfrak{M}^{1-\epsilon} \ll dM^{(\frac{51}{8}+\epsilon)}\mathfrak{A}^{\epsilon}$ and hence

$$\mathfrak{M} \ll dM^{\frac{51}{8(1-\epsilon)}+\frac{\epsilon}{1-\epsilon}}\mathfrak{A}^{\frac{\epsilon}{1-\epsilon}}.$$

Now, we let $\epsilon = \frac{1}{4}$. Since $\mathfrak{A} \leq \mathfrak{T}$, we see that

$$\mathfrak{M} \ll dM^{\frac{51}{6}+\frac{1}{3}}\mathfrak{A}^{\frac{1}{3}} \ll (t2^t)^{\frac{53}{6}}\mathfrak{T}^{\frac{1}{3}}.$$

By fixing ϵ, Proposition 2.10 guarantees the implied constant now only depends

on a.

For each integer $1 \leq i \leq 17$, $Q(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + (i-9)\mathbf{e}_3 + \mathbf{v})$ is a positive integral quadratic polynomial $\tilde{h}_i(x_1, x_2) = q(\boldsymbol{x}) + 2b(\boldsymbol{w}_i, \boldsymbol{x}) + c_i$ where q is the positive definite binary quadratic form that is associated to the binary lattice M, b is the bilinear form associated with q, and $\boldsymbol{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2$. For each $1 \leq i \leq 17$, M_{q_i} is anisotropic $\mathbb{Z}_{q_i}$-unimodular. In particular, $q(\boldsymbol{x}) \in \mathbb{Z}_{q_i}$, and hence $2b(\boldsymbol{w}_i, \boldsymbol{x}) \in \mathbb{Z}_{q_i}$ for all $\boldsymbol{x} \in M_{q_i}$ as well. This implies that $\boldsymbol{w}_i \in M_{q_i}$ and so $q(\boldsymbol{w}_i) \in \mathbb{Z}_{q_i}$. Now by the Chinese Remainder Theorem there exists $m \leq \mathfrak{M}^2$ such that

$$am \equiv q_i + c_i - q(\boldsymbol{w}_i) - r \mod q_i^2, \text{ for } 1 \leq i \leq 17.$$

Then for every $1 \leq i \leq 17$, we have $\mathrm{ord}_{q_i}((am + r) + q(\boldsymbol{w}_i) - c_i) = 1$ and so $(am + r) + q(\boldsymbol{w}_i) - c_i$ is not represented by $q(\boldsymbol{x} + \boldsymbol{w_i})$ over $\mathbb{Z}_{q_i}$. Thus $am + r$ is not represented by $h_i(\boldsymbol{x})$. Furthermore, for any integer λ, $a(m + \lambda\mathfrak{M}^2) + r$ is not represented by $h_i(\boldsymbol{x})$. However, by Lemma 3.5, there must be a positive integer $k_3 \leq (t+1)2^t$ such that $a\mathfrak{M}^2k_3 + am + r$ is relatively prime to $\mathfrak{T}$. Then $a(m + k_3\mathfrak{M}^2) + r$ is represented by $Q(\mathbf{x} + \mathbf{v})$ but not by $h_i(x_1, x_2)$ for any i and hence $|x_3| \geq 9$. Therefore

$$\mu_3 \leq \frac{2}{3}(a\mathfrak{M}^2k_3 + am + r) \ll (t2^t)^{\frac{53}{3}}\mathfrak{T}^{\frac{2}{3}}.$$

As a result,

$$\mathfrak{T} \leq dL \leq \mu_1\mu_2\mu_3 \ll (t2^t)^{\frac{59}{3}}\mathfrak{T}^{\frac{2}{3}}.$$

Since $\mathfrak{T}$ is a product of t distinct primes, it grows at least as fast as $t!$. Therefore the above inequality shows that t, and hence $\mathfrak{T}$, must be bounded. Since a is bounded by our choice of $\mathfrak{c}$, we conclude dL is bounded above by a constant

which depends only on $\mathfrak{c}$. $\square$

As previously noted in Section 2.1, given a primitive regular ternary coset $L+\mathbf{v}$ of conductor $\mathfrak{c}$, $\delta(L+\mathbf{v})$ is a primitive regular ternary $\mathbb{Z}$-coset with conductor $\mathfrak{c}$, which behaves well at all primes $p \nmid 2\mathfrak{c}$. Let $\delta(L+\mathbf{v}) = L' + \mathbf{v}'$. Then $dL'|dL$ and Proposition 3.8 gives a bound on dL'. Let ℓ be an odd prime dividing the discriminant of L. If $\ell|dL'$ then ℓ is bounded. We assume now that $\ell \nmid dL'$.

At every prime $p \nmid 2\mathfrak{c}\ell$, if $L+\mathbf{v}$ does not behave well at p, then we may apply δ_p to $L+\mathbf{v}$ to obtain a $\mathbb{Z}$-coset that does behave well at p. Therefore we can assume without loss of generality that $L+\mathbf{v}$ behaves well at all primes not dividing $p \nmid 2\mathfrak{c}\ell$. Next, since $\ell|dL$ but $\ell \nmid dL'$, we can repeatedly use Lemma 2.6 to transform $L+\mathbf{v}$ into a $\mathbb{Z}$-coset $\tilde{L}+\tilde{\mathbf{v}}$ with $\tilde{L}_\ell \cong \langle \alpha, \ell^2\beta, \ell^2\gamma\rangle$. Therefore, we assume $\tilde{L}+\tilde{\mathbf{v}}$ behaves well at all primes $p \nmid \mathfrak{c}\ell$ and $\tilde{L}_\ell \cong \langle \alpha, \ell^2\beta, \ell^2\gamma\rangle$.

Let $\tilde{T}$ be the set of odd prime divisors of $d\tilde{L}$ that do not divide $2\mathfrak{c}\ell$ and let $\tilde{\mathfrak{T}}$ denote the product of these primes. Then, by a method similar to the one used earlier in this section, one can show that $\tilde{L}+\tilde{\mathbf{v}}$ represents every positive integer $am+r$ which is relatively prime to $\tilde{\mathfrak{T}}$ and which satisfies the additional constraint that $(am+r)\alpha$ is a quadratic residue mod ℓ. We now bound ℓ.

Proposition 3.9. *The prime ℓ is bounded.*

Proof. Let $\tilde{\mu_1} \leq \tilde{\mu_2}$ be the first two successive minima of $\tilde{L}$ and fix a reduced basis $\{\tilde{\mathbf{e}}_1, \tilde{\mathbf{e}}_2, \tilde{\mathbf{e}}_3\}$ of $\tilde{L}$ such that $Q(\tilde{\mathbf{e}}_i) = \tilde{\mu_i}$. Let $\gcd(a,r) = b$. We apply Proposition 2.11 using the following conditions: $s=0$, $r=1$ and χ_1 is given by the quadratic residue character modulo ℓ, $\eta = \left(\frac{b\alpha}{l}\right)$, $\Delta = \frac{a}{b}\tilde{\mathfrak{T}}$, $\tau \in \mathbb{N}$ such that $b\tau \equiv 1 \mod \tilde{\mathfrak{T}}$ and $\tau \equiv \frac{r}{b} \mod \frac{a}{b}$, $k = 44592$, and $\epsilon = \frac{1}{8}$. This will give a positive $h \ll \ell^{\frac{1}{2}}$ such that there are 44592 positive integers $n \leq h$ with the additional properties that $bn \equiv 1 \mod \tilde{\mathfrak{T}}$, bn is in the same square class as α over $\mathbb{Z}_\ell$, and $bn = am + r$

for some positive integer m. These properties then guarantee that each of these integers is represented by $\tilde{L} + \tilde{\mathbf{v}}$. However, since there are more than 44591 such integers, Corollary 3.7 guarantees the existence of $n' \leq h$ such that bn' is represented by $\tilde{L}+\tilde{\mathbf{v}}$ with $31\tilde{\mu}_1 \leq bn'$. Consequently we have $\tilde{\mu}_1 \leq bn' \leq bh \ll \ell^{\frac{1}{2}}$, where the implied constant depends only on a and $\tilde{\mathfrak{T}}$.

Next, we will bound $\tilde{\mu}_2$. Using the same conditions as those provided above for Proposition 2.11 we see that for any positive integer n, the number of integers between 0 and n which are represented by $\tilde{L} + \tilde{\mathbf{v}}$ is at least

$$\frac{\phi(\ell)}{2a\tilde{\mathfrak{T}}\ell} n + O(n^{\frac{1}{2}}\ell^{\frac{3}{16}+\epsilon}).$$

On the other hand, Proposition 2.9 shows that for any $n < \tilde{\mu}_2$, if $Q(\mathbf{x} + \tilde{\mathbf{v}}) \leq n$ then $|x_3| \leq 8$, $|x_2| \leq 21$, and $Q(\mathbf{x} + \tilde{\mathbf{v}}) \geq \tilde{\mu}_1(x_1^2 - 30|x_1|) \geq x_1^2 - 30|x_1|$. Therefore, if $|x_1| > 15 + \sqrt{225 + n}$ then $Q(\mathbf{x} + \tilde{\mathbf{v}}) \geq x_1^2 - 30|x_1| > n$, and hence the number of integers represented by $\tilde{L} + \tilde{\mathbf{v}}$ which are smaller than n is at most $43 \cdot 17 \cdot (2(15 + \sqrt{225 + n}) + 1)$. So, given any positive integer $n < \tilde{\mu}_2$

$$\begin{aligned}\frac{\phi(\ell)}{2a\tilde{\mathfrak{T}}\ell} n - C_1(n^{\frac{1}{2}}\ell^{\frac{3}{16}+\epsilon}) &\leq 43 \cdot 17 \cdot (2(15 + \sqrt{225 + n}) + 1) \\ &\leq C_2\sqrt{n}\end{aligned}$$

for some positive constants C_1 and C_2 depending only on a, $\tilde{\mathfrak{T}}$, and μ_1. Since $\ell > 1$, we have

$$\begin{aligned}n \leq& \frac{2a\tilde{\mathfrak{T}}\ell}{\phi(\ell)}(C_2 n^{\frac{1}{2}} + C_1\sqrt{n}\ell^{\frac{3}{16}+\epsilon}) \\ \leq& \frac{2a\tilde{\mathfrak{T}}\ell}{\phi(\ell)}(C_2 + C_1)n^{\frac{1}{2}}\ell^{\frac{3}{16}+\epsilon}.\end{aligned}$$

Recall from the proof of Proposition 2.11 that $\frac{\ell}{\phi(\ell)} \ll \ell^{\epsilon}$. Therefore, $n \ll n^{\frac{1}{2}}\ell^{\frac{3}{16}+2\epsilon}$. Set $\epsilon = \frac{1}{32}$ to get $\sqrt{n} \ll \ell^{\frac{1}{4}}$, and hence $n \ll \ell^{\frac{1}{2}}$ where the implied constant depends only on a, $\tilde{\mathfrak{T}}$, and $\tilde{\mu_1}$. Since this must be true for any integer smaller than $\tilde{\mu_2}$, it is true for $\tilde{\mu_2} - 1$. Therefore, we can conclude $\tilde{\mu_2} \ll \ell^{\frac{1}{2}} + 1 \ll \ell^{\frac{1}{2}}$. Since $\tilde{L}_\ell \cong \langle \alpha, \ell^2\beta, \ell^2\gamma \rangle$, we conclude that $\ell^2 \leq \tilde{\mu_1}\tilde{\mu_2} \ll \ell$, and hence ℓ is bounded. $\square$

3.3 Main Result

We are now ready to prove the main theorem.

Theorem 3.10. *Fix a positive integer $\mathfrak{c}$. There are only finitely many isometry classes of primitive regular ternary $\mathbb{Z}$-cosets with conductor $\mathfrak{c}$.*

Proof. Let $L + \mathbf{v}$ be a primitive regular ternary $\mathbb{Z}$-coset in canonical form. Let μ_1, μ_2, μ_3 be the successive minima for L and fix a reduced basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ of L such that $Q(\mathbf{e}_i) = \mu_i$. It suffices to show that these successive minima are bounded.

Let T denote the set of prime divisors of dL which do not divide $2\mathfrak{c}$. Set $\mathfrak{T}$ to be the product of these primes, and $t = |T|$. Propositions 3.9 and 3.8 guarantee that $\mathfrak{T}$ is bounded. For any $p \in T$, the primitivity of $L + \mathbf{v}$ guarantees that $\mathfrak{n}(L_p + \mathbf{v}) = \mathbb{Z}_p$. Furthermore, since $p \nmid 2\mathfrak{c}$, we in fact have $\mathfrak{n}(L_p + \mathbf{v}) = \mathfrak{n}(L_p) = \mathbb{Z}_p$. Therefore, for every $p \in T$, L_p represents some p-adic unit α_p. Let $b = \gcd(a, r)$ and apply Proposition 2.11 using the following conditions:

- Let $s = 0$, $\Delta = \frac{a}{b}$, $k = 44592$, $\epsilon = \frac{1}{8}$, $\tau \in \mathbb{N}$ be such that $\tau \equiv \frac{r}{b} \mod \frac{a}{b}$,
- for each $p \in T$ let χ_p be the quadratic residue character modulo p, thus giving $\Gamma = \mathfrak{T}$, and

- for each quadratic character modulo p set $\eta_p = \left(\frac{b\alpha_p}{p}\right)$.

With these conditions, Proposition 2.11 gives a positive $h \ll \mathfrak{T}^{\frac{1}{2}}$ such that there are 44592 positive integers $n \leq h$ with the property that bn is in the same square class as α_p over $\mathbb{Z}_p$ for all $p \in T$ and $bn = am + r$ for some positive integer m. This guarantees that each bn is represented by $L + \mathbf{v}$. Since there are 44592 such integers, there exists n' with $bn' \leq bh \ll \mathfrak{T}^{\frac{1}{2}}$ such that $Q(\mathbf{x} + \mathbf{v}) = bn'$ with $|x_1| > 30$, $|x_2| > 21$, and $|x_3| > 8$. Corollary 3.7 then guarantees that $\mu_1 \leq bn' \ll \mathfrak{T}^{\frac{1}{2}}$. Then since $\mathfrak{T}$ is bounded, so is μ_1.

In order to bound μ_2 we apply the same conditions as listed above to Proposition 2.11 to see that the number of integers between 0 and n represented by $L+\mathbf{v}$ is at least

$$\frac{\phi(\mathfrak{T})}{2^t \mathfrak{T} a} n + O(n^{\frac{1}{2}} \mathfrak{T}^{\frac{3}{16}+\epsilon}).$$

However, by Proposition 2.9 we also have that for any $n < \mu_2$ the number of integers represented by $L + \mathbf{v}$ which are smaller than n is at most

$$43 \cdot 17 \cdot (2(15 + \sqrt{225 + n}) + 1).$$

Thus for any positive $n < \mu_2$ there exists positive constants C_1 and C_2 such that

$$\frac{\phi(\mathfrak{T})}{2^t \mathfrak{T} a} n - C_1(n^{\frac{1}{2}} \mathfrak{T}^{\frac{3}{16}+\epsilon}) \leq C_2 n^{\frac{1}{2}},$$

or equivalently

$$\begin{aligned} n \leq & (C_2 n^{\frac{1}{2}} + C_1 n^{\frac{1}{2}} \mathfrak{T}^{\frac{3}{16}+\epsilon}) 2^t a \frac{\mathfrak{T}}{\phi(\mathfrak{T})} \\ \leq & (C_2 + C_1) n^{\frac{1}{2}} \mathfrak{T}^{\frac{3}{16}+\epsilon} 2^t a \frac{\mathfrak{T}}{\phi(\mathfrak{T})}. \end{aligned}$$

We recall from the proof of Proposition 2.11 that $\frac{\mathfrak{T}}{\phi(\mathfrak{T})} \ll \mathfrak{T}^{\epsilon}$ and $2^t \ll \mathfrak{T}^{\epsilon}$ where the implied constants depend only on ϵ. Therefore,

$$n \ll n^{\frac{1}{2}}\mathfrak{T}^{\frac{3}{16}+\epsilon}\mathfrak{T}^{2\epsilon} = n^{\frac{1}{2}}\mathfrak{T}^{\frac{3}{16}+3\epsilon}.$$

By letting $\epsilon = \frac{1}{48}$ we then get $n^{\frac{1}{2}} \ll \mathfrak{T}^{\frac{1}{4}}$ and hence $n \ll \mathfrak{T}^{\frac{1}{2}}$. As this is true for any positive integer $n < \mu_2$, it is true for $\mu_2 - 1$ and hence $\mu_2 \ll \mathfrak{T}^{\frac{1}{2}}$ with the implied constant depending only on a and μ_1. Since $\mathfrak{T}$ is bounded, μ_2 is bounded.

Finally to bound μ_3, we recall that if $|x_3| \geq 9$, then $Q(\mathbf{x}+\mathbf{v}) \geq \frac{3}{2}\mu_3$. Let $M :=\text{span}_{\mathbb{Z}}\{\mathbf{e}_1, \mathbf{e}_2\}$, and $\mathfrak{A}$ be the product of primes in T that do not divide dM. The successive minima of the binary lattice M are μ_1 and μ_2 so by Proposition 2.9 we have $dM \leq \mu_1\mu_2$. Let $q_1 < \cdots < q_{17}$ be the smallest distinct primes such that $\left(\frac{-dM}{q_i}\right) = -1$, $\gcd(q_i, a) = 1$, and $q_i \notin T$ for all i. Set $\mathfrak{M} = \prod_{1\leq i\leq 17} q_i$. As in the proof of Proposition 3.8 we can bound each of these primes so that $q_i \ll dM^{\frac{3}{8}+\epsilon}\mathfrak{A}^{\epsilon}(q_i)^{i\epsilon}$, giving

$$\mathfrak{M} \ll dM^{\frac{51}{8(1-\epsilon)}+\frac{\epsilon}{1-\epsilon}}\mathfrak{A}^{\frac{\epsilon}{1-\epsilon}}.$$

Take $\epsilon = \frac{1}{4}$. Since $\mathfrak{A} \leq \mathfrak{T}$, we have

$$\mathfrak{M} \ll dM^{\frac{51}{6}+\frac{1}{3}}\mathfrak{A}^{\frac{1}{3}} \leq dM^{\frac{53}{6}}\mathfrak{T}^{\frac{1}{3}}.$$

As $\mathfrak{T}$ and dM are bounded, so is $\mathfrak{M}$. Now, for each $1 \leq i \leq 17$, $Q(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + (i-9)\mathbf{e}_3 + \mathbf{v})$ is a positive integral quadratic polynomial

$$h_i(x_1, x_2) = q(\boldsymbol{x}) + 2b(\boldsymbol{w}_i, \boldsymbol{x}) + c_i$$

where q is a positive definite binary quadratic form that is associated to the binary lattice M and $\boldsymbol{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2$. For each $1 \leq i \leq 17$, M_{q_i} is anisotropic $\mathbb{Z}_{q_i}$-unimodular. In particular, $q(\boldsymbol{x}) \in \mathbb{Z}_{q_i}$, and hence $2b(\boldsymbol{w}_i, \boldsymbol{x}) \in \mathbb{Z}_{q_i}$ as well, for all $\boldsymbol{x} \in M_{q_i}$. This implies that $\boldsymbol{w}_i \in M_{q_i}$ and so $q(\boldsymbol{w}_i) \in \mathbb{Z}_{q_i}$. Now by the Chinese Remainder Theorem there exists $m \leq \mathfrak{M}^2$ such that

$$am \equiv q_i + c_i - q(\boldsymbol{w}_i) - r \mod q_i^2, \text{ for } i = 1, \ldots, 17.$$

Then for every i, $\mathrm{ord}_{q_i}((am+r) + q(\boldsymbol{w}_i) - c_i) = 1$ and so $(am+r) + q(\boldsymbol{w}_i) - c_i$ is not represented by $q(\boldsymbol{x} + \boldsymbol{w_i})$ over $\mathbb{Z}_{q_i}$. Thus $am + r$ is not represented by $h_i(\boldsymbol{x})$. Furthermore, for any integer λ, $a(m + \lambda\mathfrak{M}^2) + r$ is not represented by $h_i(\boldsymbol{x})$. By Proposition 2.11, there exists an element of this form which is still represented by $L + \mathbf{v}$. Let $b' = \gcd(a\mathfrak{M}^2, am + r)$. Set $s = 0$, $\Delta = \frac{a\mathfrak{M}^2}{b'}$, $k = 0$, $\epsilon = \frac{1}{8}$, and for each $p \in T$ we use the quadratic residue character modulo p thus giving $\Gamma = \mathfrak{T}$. Then for each quadratic character modulo p we use $\eta_p = \left(\frac{b\alpha_p}{p}\right)$. Finally, we use $\tau \in \mathbb{N}$ such that $\tau \equiv \frac{am+r}{b'} \mod \frac{a\mathfrak{M}^2}{b'}$. Then Proposition 2.4 guarantees the existence of an $h \ll \mathfrak{T}^{\frac{1}{2}}$ where bh is in the same square class as α_p for all $p \in T$, and $bh = a(m + \mathfrak{M}^2 h) + r$ is represented by $Q(\mathbf{x} + \mathbf{v})$ but not represented by $h_i(x_1, x_2)$ for any i. Therefore, $\mu_3 \leq bh \ll \mathfrak{T}^{\frac{1}{2}}$, where the implied constant depends on a and $\mathfrak{M}$. Since a, $\mathfrak{T}$, and $\mathfrak{M}$ are bounded, so is μ_3. $\square$

Chapter 4

Regular Quadratic Forms and m-gonal Forms

In this chapter, we discuss some consequences and in particular show Theorem 1.1 implies the results of Watson [16] and Chan and Oh [6]. Further, we apply these results to an interesting family of quadratic polynomials called m-gonal forms.

As any integral quadratic lattice L may be viewed as a $\mathbb{Z}$-coset $L + \mathbf{v}$ with $\mathbf{v} \in L$, quadratic lattices and hence quadratic forms have conductor 1. Furthermore, quadratic forms are complete quadratic polynomials and so Proposition 1.4 shows that two primitive quadratic forms are semi-equivalent if and only if they are equivalent. Therefore, Theorem 1.1 implies Watson's result [16, 17] which states that up to equivalence there are only finitely many primitive positive definite regular integral quadratic forms in three variables.

For any $m \geq 3$ a generalized m**-gonal number**, sometimes referred to as a generalized polygonal number, is defined to be a number of the form

$$P_m(x) = \frac{(m-2)x^2 - (m-4)x}{2}, \; x \in \mathbb{Z}.$$

Geometrically, an m-gonal number $P_m(x)$ with $x > 0$ represents the number of equally spaced points that form a regular polygon with m sides of length x. Triangular numbers are then 3-gonal numbers that represent the number of equally spaced points in an equilateral triangle. Similarly the case $m = 4$ corresponds to the perfect squares. As is the case with triangular forms, we can generalize this further to create a family of quadratic polynomials.

Fix $m \geq 3$. Given any positive integers $a_1, \ldots, a_n$, we call the following polynomial

$$\mathcal{P}_m(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i \left(\frac{(m-2)x_i^2 - (m-4)x_i}{2} \right)$$

an m-**gonal form**. An m-gonal form is said to be primitive if $\gcd(a_1, \ldots, a_n) = 1$.

We will use this specific form to run through an example of how we can calculate the conductor of a quadratic polynomial. By completing the squares we see that a ternary m-gonal form $\mathcal{P}_m(a_1, a_2, a_3)$ represents an integer ℓ if and only if the equation

$$\begin{aligned} 8(m-2)\ell + (m-4)^2(a_1+a_2+a_3) =& a_1(2(m-2)x_1 - (m-4))^2 + \\ & a_2(2(m-2)x_2 - (m-4))^2 + \\ & a_3(2(m-2)x_3 - (m-4))^2 \end{aligned}$$

is soluble in $\mathbb{Z}$.

Let N be the $\mathbb{Z}$-lattice with quadratic map Q and orthogonal basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ such that $N \cong \langle 4(m-2)^2 a_1, 4(m-2)^2 a_2, 4(m-2)^2 a_3 \rangle$. Then the above equation is soluble in $\mathbb{Z}$ if and only if $8(m-2)\ell + (m-4)^2(a_1+a_2+a_3)$ is represented by the coset $N + \mathbf{v}$ where $\mathbf{v} = \frac{-(m-4)}{2(m-2)}(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$, i.e. if there exists a vector $\mathbf{x} \in N$ such that $Q(\mathbf{x} + \mathbf{v}) = 8(m-2)\ell + (m-4)^2(a_1+a_2+a_3)$.

Given positive integers $a_1, \ldots, a_n$ we can in fact calculate $\mathfrak{c}$, $\mathbf{v}$, and N for any $\mathcal{P}_m(a_1, \ldots, a_n)$ with $m \geq 3$: From the definition of $\mathbf{v}$, we can see that the conductor of an m-gonal form $\mathcal{P}_m$ is either $\mathfrak{c} = 2(m-2)$ if m is odd, $\mathfrak{c} = m-2$ if $ord_2(m) = 1$, or $\mathfrak{c} = \frac{m-2}{2}$ if $ord_2(m) > 1$. We then set $N \cong \langle \mathfrak{c}a_1 \frac{m-2}{4}, \ldots, \mathfrak{c}a_n \frac{m-2}{4} \rangle$ and $v = -\frac{m-4}{2(m-2)}(\mathbf{e}_1 + \cdots + \mathbf{e}_n) = -\frac{d}{\mathfrak{c}}(\mathbf{e}_1 + \cdots + \mathbf{e}_n)$ where $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ is an orthogonal basis for N and $d = (m-4)/\gcd((m-4), 2(m-2))$. Therefore, $\mathcal{P}_m(\mathbf{x}) = \ell$ if and only if

$$N + \mathbf{v} \text{ represents } \begin{cases} 4\mathfrak{c}\ell + Q(\mathbf{v}) \text{ if } \mathfrak{c} = 2(m-2), \\ 2\mathfrak{c}\ell + Q(\mathbf{v}) \text{ if } \mathfrak{c} = (m-2), \\ \mathfrak{c}\ell + Q(\mathbf{v}) \text{ if } \mathfrak{c} = \frac{(m-2)}{2}, \end{cases}$$

where Q is the quadratic form associated to N. Therefore, we see that the conductor of any m-gonal form $\mathcal{P}_m$ is completely determined by our choice of m.

Lemma 4.1. *If $\mathcal{P}_m$ and $\mathcal{P}'_m$ are semi-equivalent primitive m-gonal forms, then up to a rearranging of terms $\mathcal{P}_m = \mathcal{P}'_m$.*

Proof. Fix $m \geq 3$ and suppose $\mathcal{P}_m$ and $\mathcal{P}'_m$ are primitive m-gonal forms. First we will show that the condition of equivalence implies equality for m-gonal forms and then use this to show that semi-equivalence implies equality for primitive m-gonal forms. Suppose that $\mathcal{P}_m$ and $\mathcal{P}'_m$ are equivalent and let Q and Q' be their respective quadratic parts. The equivalence of $\mathcal{P}_m$ and $\mathcal{P}'_m$ in particular guarantees that Q and Q' are isometric as quadratic forms. Therefore, Q and Q' must have the same successive minima. Furthermore, as the quadratic parts of m-gonal forms, Q and Q' are both diagonalizable. Then as equivalent diagonal quadratic forms with the same successive minima, we must have that, up to a reordering of terms, the coefficients of the quadratic parts of $\mathcal{P}_m$ and $\mathcal{P}'_m$ are

equal. However, any m-gonal form is completely determined by the coefficients on its quadratic part and so we conclude that $\mathcal{P}_m$ and $\mathcal{P}'_m$ must in fact be equal.

Now suppose there exists $\alpha, \beta, \gamma \in \mathbb{Z}$ such that $\alpha\mathcal{P}_m(\mathbf{x}) = \beta\mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0) + \gamma$ with $\gcd(\alpha, \beta, \gamma) = 1$. As an m-gonal form $\mathcal{P}_m(\mathbf{0}) = 0$ and so $\beta\mathcal{P}'_m(\mathbf{x}_0) + \gamma = 0$. Therefore, we have $\beta|\gamma$. However, the primitivity of $\mathcal{P}_m$ implies that this only happens when either $\beta = 0$ or $\beta = 1$. It can be easily seen that $\beta \neq 0$, as otherwise $\mathcal{P}_m(\mathbf{x})$ would be constant. We therefore have $\beta = 1$ with $\gamma = -\mathcal{P}'_m(\mathbf{x}_0)$ and hence $\alpha\mathcal{P}_m(\mathbf{x}) = \mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0) - \mathcal{P}'_m(\mathbf{x}_0)$. Note that $T \in \mathrm{GL}_n(\mathbb{Z})$ implies that there exists $\mathbf{y}_0 \in \mathbb{Z}^n$ such that $\mathbf{y}_0 T = -\mathbf{x}_0$. Evaluating at $\mathbf{y}_0$ then gives $\alpha\mathcal{P}_m(\mathbf{y}_0) = \mathcal{P}'_m(\mathbf{0}) - \mathcal{P}'_m(\mathbf{x}_0) = -\mathcal{P}'_m(\mathbf{x}_0)$ and so $\alpha|\mathcal{P}'_m(\mathbf{x}_0)$. This would imply that $\alpha|\mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0)$ for all $\mathbf{x} \in \mathbb{Z}^n$. However, since $\mathcal{P}'_m$ is primitive, so is $\mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0)$ and hence $\alpha = 1$. Therefore, we can conclude that $\mathcal{P}_m(\mathbf{x}) = \mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0) - \mathcal{P}'_m(\mathbf{x}_0)$. As an m-gonal form $\mathcal{P}'_m$ and $\mathcal{P}_m$ are both non-negative functions that reach their minimum at the zero vector. By evaluating at $\mathbf{y}_0$ again we see that $\mathcal{P}_m(\mathbf{y}_0) = -\mathcal{P}'_m(\mathbf{x}_0)$ which can only happen if $\mathcal{P}_m(\mathbf{y}_0) = \mathcal{P}'_m(\mathbf{x}_0) = 0$ and hence $\mathcal{P}_m(\mathbf{x}) = \mathcal{P}'_m(\mathbf{x}T + \mathbf{x}_0)$. The result from the previous paragraph now guarantees that $\mathcal{P}_m(\mathbf{x}) = \mathcal{P}'_m(\mathbf{x})$. □

Since we have now shown that the conductor of an m-gonal form is fixed and every semi-equivalence class contains a unique primitive m-gonal form, we get the following corollary to Theorem 1.1:

Corollary 4.2. *For each $m \geq 3$, there are only finitely many primitive regular m-gonal forms in three variables.*

The case $m = 3$ recovers the finiteness results for triangular forms shown by Chan and Oh in [6]. One can see that the condition of semi-equivalence is required for any hope of a finiteness result on quadratic polynomials, but the condition of

requiring a fixed conductor extends the previously known finiteness results to include a much wider range of quadratic polynomials.

Bibliography

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976, Undergraduate Texts in Mathematics. MR 0434929 (55 #7892)

[2] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR 0148626 (26 #6133)

[3] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978. MR 522835 (80m:10019)

[4] W. K. Chan and A. G. Earnest, *Discriminant bounds for spinor regular ternary quadratic lattices*, J. London Math. Soc. (2) **69** (2004), no. 3, 545–561. MR 2048511 (2005b:11042)

[5] W. K. Chan, A. G. Earnest, and B.-K. Oh, *Regularity properties of positive definite integral quadratic forms*, Algebraic and arithmetic theory of quadratic forms, Contemp. Math., vol. 344, Amer. Math. Soc., Providence, RI, 2004, pp. 59–71. MR 2058667 (2005c:11043)

[6] W. K. Chan and B.-K. Oh, *Representations of integral quadratic polynomials*, Diophantine methods, lattices, and arithmetic theory of quadratic forms,

Contemp. Math., vol. 587, Amer. Math. Soc., Providence, RI, 2013, pp. 31–46. MR 3074801

[7] A. G. Earnest, *The representation of binary quadratic forms by positive definite quaternary quadratic forms*, Trans. Amer. Math. Soc. **345** (1994), no. 2, 853–863. MR 1264145 (95a:11034)

[8] ———, *An application of character sum inequalities to quadratic forms*, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 155–158. MR 1353928 (96j:11044)

[9] L. J. Gerstein, *Basic quadratic forms*, Graduate Studies in Mathematics, vol. 90, American Mathematical Society, Providence, RI, 2008. MR 2396246 (2009e:11064)

[10] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.*, J. Reine Angew. Math. **153** (1924), 113–130 (German).

[11] D. Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479. MR 1557926

[12] W. C. Jagy, I. Kaplansky, and A. Schiemann, *There are 913 regular ternary forms*, Mathematika **44** (1997), no. 2, 332–341. MR 1600553 (99a:11046)

[13] W. J. LeVeque, *Fundamentals of number theory*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977. MR 0480290 (58 #465)

[14] B.-K. Oh, *Regular positive ternary quadratic forms*, Acta Arith. **147** (2011), no. 3, 233–243. MR 2773202 (2012c:11087)

[15] O. T. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition. MR 1754311 (2000m:11032)

[16] G. L. Watson, *Some problems in the theory of numbers*, Ph.D. thesis, University College, London, 1953.

[17] ———, *Regular positive ternary quadratic forms*, J. London Math. Soc. (2) **13** (1976), no. 1, 97–102. MR 0414489 (54 #2590)