Upper Bounds for the Number of Integral Points on Quadratic Curves and Surfaces.

by

Veronika Shelestunova

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2010

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We are interested in investigating the number of integral points on quadrics.

First, we consider non-degenerate plane conic curves defined over $\mathbb{Z}$. In particular we look at two types of conic sections: hyperbolas with two rational points at infinity, and ellipses. We give upper bounds for the number of integral points on such curves which depends on the number of divisors of the determinant of a given conic.

Next we consider quadratic surfaces of the form $q(x, y, z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbb{Z}$. We give an upper bound for the number of integral points (x, y, z) with bounded height.

Acknowledgments

I want to say a special thank you to my supervisor Professor David McKinnon. I am very grateful to him for his excellent academic guidance and constant moral support. Thank you for giving me confidence and awakening new ideas in me.

I also want to thank Professor Cameron Stewart for all his valuable help.

I want to thank Professors Kevin Hare (University of Waterloo), Wentang Kuo (University of Waterloo), Alfred Menezes (University of Waterloo), and Tom Tucker (University of Rochester) for their comments and for their time spent on reading this thesis.

Thanks also go to Administrative Coordinator Shonn Martin, Administrative Assistant Lis D'Alessio, and Administrative Coordinator Nancy Maloney for all their help and moral support.

Dedication

This thesis is dedicated to my wonderful parents who always support me.

Contents

Chapter 1

Introduction

The study of integral points on affine curves has always drawn attention of many mathematicians. But only recently, Silverman [Sil00] gave the conditions determining whether a given irreducible affine curve defined over $\mathbb{Z}$ has finite or infinite set of integral points. It was proven earlier by Siegel [Sie29] that a geometrically irreducible affine curve has only finitely many integral points unless it has geometric genus 0 and at most two points at infinity. Silverman gave a necessary and sufficient condition for a curve of that type to possess a finite number of integral points. There was a small mistake in his statement that was later corrected by Poulakis [Pou02].

Knowing that a given curve has finitely many integral points leads to the next questions: "How many integral points does the curve have?" and "How to find those points?". An explicit bound for the number of integer solutions for curves of genus 0 with at least 3 points at infinity was obtained by Poulakis [Pou93]. Such

a bound also follows from Bilu [Bil93]. The bounds were too large to provide a good method to find the actual points, so later on, Poulakis and Voskos [PV00] gave a practical general method for finding integral points on curves of genus 0 with at least three points at infinity. Two years later they gave a practical method for finding integral points on curves of genus 0 with at most two points at infinity [PV02]. Other mathematicians also worked on answering the above questions. One remarkable example is due to Corvaja and Zannier [CZ03].

Consider irreducible conic curves defined over $\mathbb{Z}$. We can divide such curves into four types: (i) parabolas; (ii) ellipses; (iii) hyperbolas with two rational points at infinity; (iv) hyperbolas with two points at infinity that are conjugates over a real quadratic field. It follows from [Sil00] that there are either none or an infinite number of integral points on curves of types (i) and (iv). Same conclusion also follows from the work of Niven [Niv42]. Explicit algorithms for finding a complete set of integral points on those curves can be found in [Nag64], [Dic71]. Thus, we narrow our focus to hyperbolas with rational points at infinity, and ellipses.

Using the method described in our proof, one can compute effectively all the integer solutions, but there are other algorithms to solve the above type of equations, see [MA], [Nag64], [Dic71]. Moreover, in the hyperbola case, "Mathematica" implements an algorithm, which is different from ours, that can also be used to get the same maximum number of integer solutions. However, an explicit bound is not given in the above sources.

After examining integral points on quadratic curves we can ask similar questions in a higher dimensional case. So we are interested in upper bounds for the number

of integral points of bounded height on quadratic surfaces. Such questions were also studied before. For example, Scourfield [Sco61] looked at a particular quadratic surface, defined by the equation $x^2+y^2-z^2=1$, and found an asymptotic estimate for the number of integral points of height bounded by B to be $CB\log B$ (where C is a constant that does not depend on B). Duke, Rudnik and Sarnak [DRS93] proved results for more general cases (at the same time, Eskin and McMullen [EM93] also worked on similar questions) using techniques from harmonic analysis. In the case of quadratic forms they claim that the following asymptotics can be deduced: CB or $CB\log B$. However in their paper they omit the details, including stating precisely when the asymptotic formula is CB and when it is $CB\log B$. We obtain our estimates for the number of integral points with bounded height for a general smooth quadratic surface with infinitely many integral points, using a completely different approach that involves a geometric argument. Our techniques are much more elementary.

The thesis is organized as follows. In Chapter 2 (Background) we will give background which will be helpful in understanding and proving the main theorems. Due to the nature of the problems we are interested in this thesis, we will not need too much background, but few definitions will still be essential. In particular, we will talk about projective n-space, quadratic forms and conic sections.

Chapter 3 (Main Theorems) consists of Section 3.1 (Integral Points on Quadratic Curves) and Section 3.2 (Integral Points on Quadratic Surfaces). In the first section of Chapter 3 we will investigate integral points on non-degenerate quadratic curves defined over $\mathbb{Z}$ of two types: hyperbolas with two rational points at infinity, and

ellipses. We will give upper bounds for the number of integral points on such curves that depend on the number of divisors of the determinant of a given curve.

In particular, hyperbolas with two rational points at infinity can be defined as follows:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \text{ with } D = b^2 - 4ac = m^2$$

for some non-zero integer m, and the determinant $\Delta = \frac{4acf+bde-ae^2-b^2f-cd^2}{4} \neq 0$. We will show that the number of integral points on hyperbolas with two rational points at infinity is bounded from above by $4\mathbf{d}(4\Delta)$, where (4Δ) is the determinant of a given curve and $\mathbf{d}(4\Delta)$ denotes the number of positive divisors of 4Δ.

Next we will consider ellipses:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \text{ with } D = b^2 - 4ac < 0.$$

As before we define the determinant of the curve denoted by Δ to be $\frac{4acf+bde-ae^2-b^2f-cd^2}{4}$ and we assume it is nonzero. A trivial upper bound for the number of integral points on ellipses is $\left(\left\lfloor \frac{8\sqrt{-a(4\Delta)}}{-D} \right\rfloor + 2\right)$, but we are interested in an upper bound that depends on the number of divisors of the determinant. We will show that the number of integral points is not greater than $24\mathbf{d}(-16a(4\Delta))$, where $\mathbf{d}(-16a(4\Delta))$ denotes the number of positive divisors of $-16a(4\Delta)$. Note that our bound also depends on the coefficient in front of x^2. It is easy to adjust our argument to get an upper bound $24\mathbf{d}(-16c(4\Delta))$, and in particular this latter bound can be used if $|a| > |c|$.

In the second section of Chapter 3 we will give an upper bound for the num-

ber of integral points with bounded height on non-degenerate quadratic surfaces. Let $q(x, y, z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbb{Z}$. We will show that an upper bound for the number of integral solutions (x, y, z) with $|x|, |y|, |z| \leq B$ is $KB \log B$ with an exception that in some cases it is $KB(\log B)^2$, where K is a constant that depends on the coefficients of the original polynomial but not on B. We will be using bounds obtained in Section 3.1 to get our estimates. The idea in the proofs is to transform a given surface to a surface that we can slice with planes $z = C'$ (as C' varies) where each slice is a hyperbola with two rational points at infinity (so the surface can be expressed as a family of hyperbolas) or an ellipse (so the surface can be expressed as a family of ellipses). There will be only finitely many integral points on each slice. Then we will sum up integral points on those slices to get our bounds.

Chapter 4 contains the conclusion.

Chapter 2

Background

2.1 Projective n-space

Definition 1. *Let K be a field. We define* **projective n-space** *over K, denoted by $\mathbf{P}^n$ or $\mathbf{P}^n(K)$, to be the set of equivalence classes of $(n+1)$-tuples $[a_1 : \ldots : a_{n+1}]$ of elements of K, not all zero, under the equivalence relation given by*

$$[a_1 : \ldots : a_{n+1}] \sim [\lambda a_1 : \ldots : \lambda a_{n+1}]$$

for all $\lambda \in K, \lambda \neq 0$ (see Section I.2 of [Har77]).

An element of $\mathbf{P}^n(K)$ is called a point in $\mathbf{P}^n(K)$.

Points at **infinity** in $\mathbf{P}^n$ are points with the last coordinate zero, i.e. points of the form $[a_1 : \ldots : a_n : 0]$.

A point $[a_1 : \ldots : a_{n+1}]$ of $\mathbf{P}^n(\mathbb{Q})$ is in **reduced form** if $a_1, \ldots, a_{n+1}$ are integers and $\gcd(a_1, \ldots, a_{n+1}) = 1$.

The **height** of $[a_1 : \ldots : a_{n+1}]$ (in reduced form) is defined to be

$$H([a_1 : \ldots : a_{n+1}]) = \max(|a_1|, \ldots, |a_{n+1}|).$$

2.2 Quadratic Forms

Quadratic forms are homogeneous quadratic polynomials in n variables. Using homogeneous coordinates, a non-zero quadratic form in n variables defines an $(n-2)$-dimensional quadric in $(n-1)$-dimensional projective space.

Any $n \times n$ real symmetric matrix S determines a quadratic form. Conversely, given a quadratic form in n variables, its coefficients can be arranged into an $n \times n$ symmetric matrix. For example, if we are given a ternary quadratic form

$$q(x, y, z) = ax^2 + bxy + cy^2 + dxz + eyz + fz^2$$

we associate the following matrix S with it:

$$S = \begin{bmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{bmatrix}.$$

If none of the eigenvalues of matrix S are zero (or equivalently if $\det S \neq 0$)

then the corresponding quadratic form is called **non-degenerate**. This includes positive definite, negative definite, and indefinite quadratic forms. Throughout the thesis we will be considering non-degenerate quadratic forms. A quadratic form $q(x_1, x_2, \ldots, x_n)$ is called

-**positive definite**, if $q(x_1, x_2, \ldots, x_n) > 0$ for all $(x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0)$

-**negative definite**, if $q(x_1, x_2, \ldots, x_n) < 0$ for all $(x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0)$

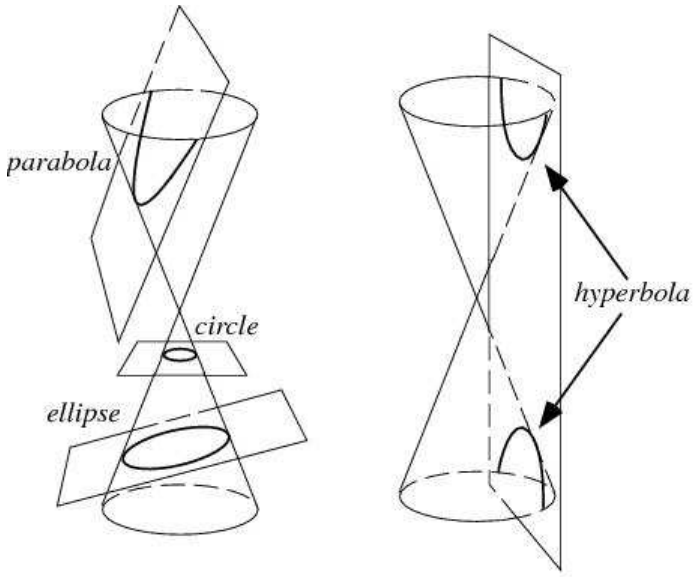
-**indefinite**, otherwise.

We can determine what type of form we have by looking at the eigenvalues of the corresponding matrix S. Thus, if all the eigenvalues of S are positive, we have a positive definite quadratic form, if all the eigenvalues are negative, we get a negative definite quadratic form, and if a matrix S has both positive and negative eigenvalues, the corresponding form is indefinite.

We define the **signature** of a non-degenerate quadratic form to be a pair (s_p, s_n), where s_p is the number of positive eigenvalues of S and s_n is the number of negative eigenvalues of S.

2.3 Conic Sections

Conic sections are curves generated by the intersections of a plane with one or two nappes of a cone. The image below is taken from Wolfram MathWorld web page [MW].



Consider irreducible (non-degenerate) conic curves defined over $\mathbb{Z}$. We can divide such curves into four types:

(i) **parabola** (one rational point at infinity);

(ii) **ellipse** (two imaginary points at infinity);

(iii) **hyperbola** (two rational points at infinity);

(iv) **hyperbola** (two points at infinity that are conjugates over a real quadratic field).

It follows from [Sil00] that there are either none or an infinite number of integral points on curves of types (i) and (iv). Explicit algorithms for finding a complete set of integral points on those curves can be found in [Nag64], [Dic71]. In this thesis we will look closer at the curves of types (ii) and (iii) which are known to have only finitely many integral points.

Let $\mathcal{C}$ be a non-degenerate plane conic curve defined over $\mathbb{Z}$. In particular, we are given a bivariate quadratic equation

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f, \in \mathbb{Z}$, $\gcd(a, b, c, d, e, f) = 1$, and a, b, c are not all zero.

The **discriminant** of the curve is defined to be $D = b^2 - 4ac$.

Let $\mathcal{C}_h : ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$ be the corresponding curve in the projective plane. Then (X, Y) is a solution of $\mathcal{C}$ if and only if $[X : Y : 1]$ is a solution of $\mathcal{C}_h$.

Points at infinity that lie on $\mathcal{C}_h$ are points with $z = 0$, i.e. they have to satisfy the equation $ax^2 + bxy + cy^2 = 0$.

Assuming that there are two distinct rational points at infinity on $\mathcal{C}_h$ is the same as assuming that $D = b^2 - 4ac = m^2$ for some non-zero integer m. Such curves are hyperbolas with two rational points at infinity and are known to have finitely many integral points.

If $D < 0$, i.e. there are two imaginary points at infinity on a given curve, then the curve is an ellipse.

Let

$$S = \begin{bmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{bmatrix}.$$

Then S is a symmetric matrix associated to $\mathcal{C}_h$; i.e.

$$\mathcal{C}_h : \begin{bmatrix} x & y & z \end{bmatrix} S \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

We define the **determinant**, denoted by Δ, of the curve $\mathcal{C}$ to be the determinant of this matrix S.

$$\Delta = \det(S) = \begin{vmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{vmatrix} = \frac{4acf + bde - ae^2 - fb^2 - cd^2}{4}.$$

Chapter 3

Main Theorems

3.1 Integral Points on Quadratic Curves

In this section we will consider non-degenerate quadratic curves of two types; in particular we will look at hyperbolas with two rational points at infinity and ellipses. We will give upper bounds for the number of integral points on such curves.

3.1.1 Hyperbolas with Two Rational Points at Infinity

Let $\mathcal{C}$ be a non-degenerate plane conic curve defined over $\mathbb{Z}$, with the property of having two distinct rational points at infinity in the projective plane. We give an upper bound for the number of integer points on $\mathcal{C}$. The bound depends only on the determinant of the conic.

In particular, we are given a bivariate quadratic equation

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f, \in \mathbb{Z}$, $\gcd(a, b, c, d, e, f) = 1$, $b^2 - 4ac = m^2$ for some non-zero integer m, and $\frac{4acf+bde-ae^2-b^2f-cd^2}{4} \neq 0$. The last quantity also defines the determinant of the curve denoted by Δ. We show that the the number of integer solutions to this quadratic equation does not exceed $4\mathbf{d}(4\Delta)$, where $\mathbf{d}(4\Delta)$ is the number of positive divisors of 4Δ.

The proof involves solving the above equation to determine what conditions are necessary in order for the solution to be integral. We apply some of those restrictions to get an upper bound for the number of integer solutions. Observing that the bound depends only on the determinant of the curve if the equation has coefficients $a \neq 0$ and $c = 0$, we show that we can always find a linear transformation that sends the original curve to a curve in the required form (i.e. $a \neq 0$ and $c = 0$), satisfying all the initial assumptions, and having the same number of integer points and the same determinant as the original curve.

Theorem 1. *Let $\mathcal{C}$ be a non-degenerate curve in $\mathbf{A}^2$, defined by a bivariate quadratic equation with integer coefficients. Let C_h denote the corresponding homogenized curve $\mathcal{C}$ in $\mathbf{P}^2$ and assume that C_h has two distinct rational points at infinity. Let $\Delta \neq 0$ denote the determinant of the quadratic curve. Then the number of integer points on $\mathcal{C}$ is not greater than $4\mathbf{d}(4\Delta)$, where $\mathbf{d}(4\Delta)$ is the number of positive divisors of 4Δ.*

Note: It should be noted that $\Delta \neq 0$ is immediate from the fact that we are

restricting our attention to non-degenerate curves.

Proof: Given the following quadratic curve

$$\mathcal{C} : ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

with $a, b, c, d, e, f, \in \mathbb{Z}$, $\gcd(a, b, c, d, e, f) = 1$ and a, b, c are not all zero. By homogenizing the above equation we get the corresponding curve in the projective plane

$$\mathcal{C}_h : ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0.$$

First we will show that, without loss of generality, we can assume that $a \neq 0$ and $c = 0$.

Let $M \in SL_3(\mathbb{Z})$ be in the form $\begin{bmatrix} u & g & 0 \\ v & h & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Then the linear transformation defined by M sends the curve $\mathcal{C}_h$ to a curve $\mathcal{C}'_h$ with the property that $\mathcal{C}$ and $\mathcal{C}'$ have the same number of integer solutions. To see that, first observe that the inverse of M is given by $\begin{bmatrix} h & -g & 0 \\ -v & u & 0 \\ 0 & 0 & 1 \end{bmatrix}$. So we have

$$M \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} ux + gy \\ vx + hy \\ 1 \end{bmatrix} \text{ and } M^{-1} \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} hx' - gy' \\ -vx' + uy' \\ 1 \end{bmatrix}.$$

Hence, the above transformation gives us a one to one correspondence between the points on $\mathcal{C}_h$ in the form $[x : y : 1]$ with $x, y \in \mathbb{Z}$ and the points on $\mathcal{C}'_h$ in the form $[x' : y' : 1]$ with $x', y' \in \mathbb{Z}$.

It is easy to see that since $\mathcal{C}_h$ has two distinct rational points at infinity, $\mathcal{C}'_h$ will also have two distinct rational points at infinity. The property that $\mathcal{C}'$ is non-degenerate will follow from the fact that this linear transformation preserves the determinant of the curve. To prove that, consider the symmetric matrix S associated with $\mathcal{C}_h$, that we described in Section 2.3. Then

$$\mathcal{C}'_h : \begin{bmatrix} x & y & z \end{bmatrix} (M^{-1})^T S M^{-1} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

Consequently, a symmetric matrix that represents $\mathcal{C}'_h$ is $(M^{-1})^T S M^{-1}$ and since $\det(M) = 1$, then $\Delta' = \Delta$.

So, such a matrix M preserves the determinant, the number of integer points, and the property that it has two rational points at infinity. It remains to show that we can pick M such that $a' \neq 0$ and $c' = 0$. This would imply that we can continue our argument assuming that $a \neq 0$ and $c = 0$.

Observe that $\mathcal{C}'_h$ satisfies the required property - the coefficient in front of x^2 is non-zero and the coefficient in front of y^2 is zero - if and only if the two points at infinity on $\mathcal{C}'_h$ are $[0 : Z : 0]$ and $[X : Y : 0]$ with $X, Y, Z \neq 0$. Hence, to show that we can find the required linear transformation we need to show that we can find M in the form described above that sends two points at infinity of $\mathcal{C}_h$ to rational

points $[0 : Z : 0]$ and $[X : Y : 0]$ with $X, Y, Z \neq 0$.

We can have the following four possibilities for the coefficients a and c in the original curve $\mathcal{C}_h$:

i) $a \neq 0$ and $c = 0$;

ii) $a = 0$ and $c = 0$;

iii) $a = 0$ and $c \neq 0$;

iv) $a \neq 0$ and $c \neq 0$.

Clearly, in the first case we already have the curve in the required form. By symmetry in x and y, case iii) is the same as case i).

For the second case, the two points at infinity on $\mathcal{C}_h$ are $P = [1 : 0 : 0]$ and $Q = [0 : 1 : 0]$, then we let $M = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. We see that

$$MP = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \text{ and } MQ = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$$

giving two points at infinity of the the required form.

In the final case, the points at infinity are

$$P = [p : r : 0] \text{ and } Q = [q : r : 0],$$

$$\text{where } p = -b + \sqrt{b^2 - 4ac},\ q = -b - \sqrt{b^2 - 4ac} \text{ and } r = 2a.$$

Note that by our assumptions, p, q, and r are all integers, but they may not be coprime.

We will find M with $\det(M) = 1$ such that

$$MP = \begin{bmatrix} u & g & 0 \\ v & h & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p \\ r \\ 0 \end{bmatrix} = \begin{bmatrix} up + gr \\ vp + hr \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \gcd(p, r) \\ 0 \end{bmatrix}$$

and

$$MQ = \begin{bmatrix} u & g & 0 \\ v & h & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} q \\ r \\ 0 \end{bmatrix} = \begin{bmatrix} uq + gr \\ vq + hr \\ 0 \end{bmatrix}$$

with $(uq + gr)(vq + hr) \neq 0$. Note also that $\gcd(p, r) \neq 0$, since $P = [p : r : 0]$. Let $u = \frac{r}{\gcd(p,r)}$ and $g = -\frac{p}{\gcd(p,r)}$. Then $up + gr = 0$ and $uq + gr = -2u\sqrt{b^2 - 4ac} \neq 0$. Next, we want to find integers v and h such that $vp+hr = \gcd(p, r)$ and $vq+hr \neq 0$. The first condition also implies that $uh - gv = 1$, i.e. the determinant of M is one. Clearly, there are infinitely many solutions to $vp+hr = \gcd(p, r)$, so suppose (v, h) is one of them. Then the equation $vq + hr = \gcd(p, r) - 2v\sqrt{b^2 - 4ac} = 0$ has at most one integer solution for v. Since there are many possibilities for choosing (v, h) we can always find the pair such that $vq + hr \neq 0$, and thus we can always get the required matrix M.

Therefore, we can always find a linear transformation that sends a given curve to a curve that satisfies all the original assumptions, has the same number of integer points, and, moreover, has the property that the coefficient in front of x^2 is non-zero

and the coefficient in front of y^2 is zero. For that reason, without loss of generality, we can assume that we are given a curve $\mathcal{C} : ax^2 + bxy + cy^2 + dx + ey + f = 0$, where $a \neq 0$ and $c = 0$. Note that the determinant becomes $\Delta = \frac{bde - ae^2 - fb^2}{4}$ and $b^2 - 4ac > 0$ implies that $b \neq 0$.

So we have the equation

$$ax^2 + bxy + dx + ey + f = 0.$$

By fixing y and thinking about the equation in terms of x we get

$$ax^2 + (by + d)x + (ey + f) = 0.$$

We can use the quadratic formula to get

$$x = \frac{-(by + d) \pm \sqrt{(by + d)^2 - 4a(ey + f)}}{2a}.$$

In order for x to be an integer we need to find $y \in \mathbb{Z}$, such that

1) $(by + d)^2 - 4a(ey + f) = A^2$ for some integer A;

2) $2a$ divides $-(by + d) \pm A$.

Let us look at equation 1). By rearranging the terms in that equation, we get

$$b^2y^2 + (2bd - 4ae)y + (d^2 - 4af - A^2) = 0.$$

Again, we can use the quadratic formula to get

$$y = \frac{-(2bd - 4ae) \pm \sqrt{(2bd - 4ae)^2 - 4b^2(d^2 - 4af - A^2)}}{2b^2}.$$

Since we want y to be an integer, we need the following two conditions satisfied:

1) $(2bd - 4ae)^2 - 4b^2(d^2 - 4af - A^2) = B^2$ for some integer B;

2) $2b^2$ divides $-(2bd - 4ae) \pm B$.

The first condition gives us the following equation in terms of A and B :

$$B^2 - 4b^2A^2 = (2bd - 4ae)^2 - 4b^2(d^2 - 4af)$$

$$\implies B^2 - 2^2b^2A^2 = -16a(4\Delta)$$

$$\implies (B - 2bA)(B + 2bA) = -16a(4\Delta).$$

So we write

$$B - 2bA = h$$

$$B + 2bA = n$$

then

$$B = \tfrac{h+n}{2}$$

$$A = \tfrac{n-h}{4b}$$

where $hn = -16a(4\Delta)$.

In order for B to be an integer, h and n have to be both even or both odd. Since their product is even and thus they cannot be both odd, h and n are both even.

In order for A to be an integer, $n \equiv h \bmod 4$. If $h \equiv 2 \bmod 4$, then $h = 2k_1$ where k_1 is odd, and therefore $n = -8k_2 \equiv 0 \bmod 4$ and $h \not\equiv n \bmod 4$. For that reason, we want both h and n be divisible by four. So, let $h = 4\alpha$, and $n = 4\beta$.

$$(A, B) = \left(\frac{(\beta - \alpha)}{b}, 2\alpha + 2\beta \right), \text{ where } \alpha\beta = -a(4\Delta).$$

The next step is to go back and express x and y in terms of α and β. For each (A, B) we have four solutions:

$$S_1 = \begin{cases} y = \frac{-(2bd-4ae)+B}{2b^2} = \frac{-(bd-2ae)+(\alpha+\beta)}{b^2} \\ x = \frac{-(by+d)+A}{2a} = \frac{-2ae+(\alpha+\beta)+(\beta-\alpha)}{2ab} \end{cases}$$

$$S_2 = \begin{cases} y = \frac{-(2bd-4ae)+B}{2b^2} = \frac{-(bd-2ae)+(\alpha+\beta)}{b^2} \\ x = \frac{-(by+d)-A}{2a} = \frac{-2ae+(\alpha+\beta)-(\beta-\alpha)}{2ab} \end{cases}$$

$$S_3 = \begin{cases} y = \frac{-(2bd-4ae)-B}{2b^2} = \frac{-(bd-2ae)-(\alpha+\beta)}{b^2} \\ x = \frac{-(by+d)+A}{2a} = \frac{-2ae-(\alpha+\beta)+(\beta-\alpha)}{2ab} \end{cases}$$

$$S_4 = \begin{cases} y = \frac{-(2bd-4ae)-B}{2b^2} = \frac{-(bd-2ae)-(\alpha+\beta)}{b^2} \\ x = \frac{-(by+d)-A}{2a} = \frac{-2ae-(\alpha+\beta)-(\beta-\alpha)}{2ab} \end{cases}$$

Observe that due to the obvious symmetry pairs (α, β), (β, α), $(-\alpha, -\beta)$ and $(-\beta, -\alpha)$ give rise to the same set of solutions. Thus the first thing we notice from the above argument is that to count pairs (α, β) that produce distinct sets of solutions we can consider only positive divisors of $a(4\Delta)$.

Next, for each pair (α, β) we have the following four possibilities for x:

$$(i) : x = \frac{-ae + \beta}{ab} \Longrightarrow a \text{ divides } \beta$$

$$(ii) : x = \frac{-ae + \alpha}{ab} \Longrightarrow a \text{ divides } \alpha$$

$$(iii) : x = \frac{-ae - \alpha}{ab} \Longrightarrow a \text{ divides } \alpha$$

$$(iv) : x = \frac{-ae - \beta}{ab} \Longrightarrow a \text{ divides } \beta.$$

Consequently, in order for x to be an integer in at least one of the above four cases, a has to divide at least one of β or α, thus we can exclude the pairs (α, β), where both α and β are not divisible by a. Since $\alpha\beta = -a(4\Delta)$, and we showed earlier that (α, β) and (β, α) give the same set of solutions, without loss of generality, we can let $\alpha = a\alpha'$, and we count the pairs $(a\alpha', \beta)$, where $\alpha'\beta = -4\Delta$. Let $\mathbf{d}(4\Delta)$ denote the number of positive divisors of (4Δ). Then, using the above argument, we can conclude that the bound for the number of integer solutions on $\mathcal{C}$ is not greater then $4\mathbf{d}(4\Delta)$.

This completes the proof.

3.1.2 Ellipses

In this section we will give an upper bound for the number of integer points on an ellipse which depends on the number of divisors of the determinant of the conic.

In particular, we are given a bivariate quadratic equation

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f, \in \mathbb{Z}$, $\gcd(a, b, c, d, e, f) = 1$, and $D = b^2 - 4ac < 0$. As before we define the determinant of the curve, denoted by Δ, to be $\frac{4acf+bde-ae^2-b^2f-cd^2}{4}$ and we assume it is nonzero.

The proof in this thesis involves solving the above equation to determine what conditions are necessary in order for the solution to be integer. We apply some of those restrictions to show that the number of integral points on a given ellipse is bounded by the number of solutions of the corresponding equation $X^2 - DY^2 = -16a(4\Delta)$. We will show that the number of integral solutions on this latter equation is not more than $\mathbf{d}(-16a(4\Delta))$.

Theorem 2. *Let $\mathcal{C}$ be a non-degenerate curve in $\mathbf{A}^2$, defined by a bivariate quadratic equation with integer coefficients. Let $\Delta \neq 0$ denote the determinant of the quadratic curve. Let $D = b^2 - 4ac < 0$. Then the number of integer points on $\mathcal{C}$ is not greater than $24\mathbf{d}(-16a(4\Delta))$, where $\mathbf{d}(-16a(4\Delta))$ is the number of positive divisors of $-16a(4\Delta)$.*

Note: The fact that C is non-degenerate implies that $\Delta \neq 0$. The fact that $D < 0$ implies that we are looking at an ellipse.

Proof: Let

$$C : ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f, \in \mathbb{Z}$, $\gcd(a, b, c, d, e, f) = 1$ and a, b, c are not all zero.

By fixing y and thinking about the equation in terms of x we get

$$ax^2 + (by + d)x + (cy^2 + ey + f) = 0.$$

We can use the quadratic formula to get

$$x = \frac{-(by + d) \pm \sqrt{(by + d)^2 - 4a(cy^2 + ey + f)}}{2a}.$$

In order for x to be an integer we need to find $y \in \mathbb{Z}$ such that

1) $(by + d)^2 - 4a(cy^2 + ey + f) = A^2$ for some integer A;

2) $2a$ divides $-(by + d) \pm A$.

Let us look at equation 1). By rearranging the terms in that equation, we get

$$(b^2 - 4ac)y^2 + (2bd - 4ae)y + (d^2 - 4af - A^2) = 0.$$

Again, we can use the quadratic formula to get

$$y = \frac{-(2bd - 4ae) \pm \sqrt{(2bd - 4ae)^2 - 4(b^2 - 4ac)(d^2 - 4af - A^2)}}{2(b^2 - 4ac)}.$$

Since we want y to be an integer, we need the following two conditions satisfied:

1) $(2bd - 4ae)^2 - 4(b^2 - 4ac)(d^2 - 4af - A^2) = B^2$ for some integer B;

2) $2(b^2 - 4ac)$ divides $-(2bd - 4ae) \pm B$.

The first condition gives us the following equation in terms of A and B :

$$B^2 - 4(b^2 - 4ac)A^2 = (2bd - 4ae)^2 - 4(b^2 - 4ac)(d^2 - 4af)$$

$$\implies B^2 - 4(b^2 - 4ac)A^2 = -16a(4acf + bde - ae^2 - cd^2 - fb^2)$$

$$\implies B^2 - 4DA^2 = -16a(4\Delta).$$

Thus we see that a necessary condition for (x, y) to be an integer solution is the existence of the corresponding solution on the curve $X^2 - 4DY^2 = -16a(4\Delta)$. Note that not every integral solution on this new curve will correspond to and an integral solution on the original curve. Since we only look for an upper bound, we will examine integral solutions of $X^2 - DY^2 = -16a(4\Delta)$.

Remark. Since we assumed that $D < 0$, there are no integral solutions if $-16a(4\Delta) < 0$.

We can write the above expression in the following form

$$(X - \sqrt{D}Y)(X + \sqrt{D}Y) = -16a(4\Delta).$$

Let $\mathbf{d_1}(\alpha)$ be the number of ways to factor an integer α as $\alpha = (X - \sqrt{D}Y)(X + \sqrt{D}Y)$ for integers X and Y. We will show that

$$\mathbf{d_1}(\alpha) \leq 6\mathbf{d}(\alpha)$$

where $\mathbf{d}(\alpha)$ is the number of positive divisors of α.

Let $\mathbf{d_2}(\alpha)$ denote the number of ways to factor an ideal (α) as $(\alpha) = I\overline{I}$ for an ideal I of the ring of integers of $\mathbb{Q}(\sqrt{D})$.

Claim 1. $\mathbf{d_1}(\alpha) \leq 6\mathbf{d_2}(\alpha)$

Each factorization of α as $\alpha = (X - \sqrt{D}Y)(X + \sqrt{D}Y)$ will give an ideal factorization $(\alpha) = (X - \sqrt{D}Y)(X + \sqrt{D}Y)$ up to multiplication by units. Since $D < 0$, there can be at most 6 units in the ring of integers of $\mathbb{Q}(\sqrt{D})$ (see p.230 of [DF04]) so we get $\mathbf{d_1}(\alpha) \leq 6\mathbf{d_2}(\alpha)$.

Claim 2. $\mathbf{d_2}(\alpha) \leq \mathbf{d}(\alpha)$

First, let us show that $\mathbf{d_2}(\alpha)$ is multiplicative. Let α and β be integers such that $\gcd(\alpha, \beta) = 1$. We will show that there is a one-to-one correspondence between factorizations $(\alpha\beta) = I\overline{I}$ of $(\alpha\beta)$ and pairs of factorizations $(\alpha) = U\overline{U}$ and $(\beta) = V\overline{V}$.

Let $(\alpha\beta) = I\overline{I}$. Set $U = (\alpha) + I$ and $V = (\beta) + I$. Then

$$U\overline{U} = ((\alpha) + I)((\alpha) + \overline{I}) = (\alpha^2) + \alpha I + \alpha\overline{I} + I\overline{I} = (\alpha^2) + \alpha I + \alpha\overline{I} + (\alpha\beta) = (\alpha)$$

since $\gcd(\alpha, \beta) = 1$. Similarly we can see that $V\overline{V} = (\beta)$. So we get the following map Φ

$$(\alpha\beta) = I\overline{I} \xrightarrow{\Phi} \begin{cases} (\alpha) = ((\alpha) + I)((\alpha) + \overline{I}) = U\overline{U} \\ (\beta) = ((\beta) + I)((\beta) + \overline{I}) = V\overline{V} \end{cases}$$

To define a map going in the other direction - call this map Ψ - assume $(\alpha) = U\overline{U}$

and $(\beta) = V\overline{V}$. Let $I = UV$ then $I\overline{I} = (UV)(\overline{UV}) = (\alpha\beta)$.

$$\begin{cases} (\alpha) = U\overline{U} \\ (\beta) = V\overline{V} \end{cases} \xrightarrow{\Psi} (\alpha\beta) = (UV)(\overline{UV}) = I\overline{I}.$$

We still need to show that the above maps give us a bijection, i.e

$$\Psi \circ \Phi = \Phi \circ \Psi = \text{ identity.}$$

We start with $(\alpha\beta) = I\overline{I}$.

$$(\alpha\beta) = I\overline{I} \xrightarrow{\Phi} \begin{cases} (\alpha) = ((\alpha) + I)((\alpha) + \overline{I}) \\ (\beta) = ((\beta) + I)((\beta) + \overline{I}) \end{cases}$$

$$\xrightarrow{\Psi} (\alpha\beta) = (((\alpha) + I)((\beta) + I))(((\alpha) + \overline{I})((\beta) + \overline{I})$$

So we want to show $((\alpha) + I)((\beta) + I) = I$.

$$((\alpha)+I)((\beta)+I) = (\alpha\beta)+(\beta)I+(\alpha)I+I^2 = I\overline{I}+I((\alpha)+(\beta))+I^2 = I(\overline{I}+(1)+I) = I.$$

On the other hand, let $(\alpha) = U\overline{U}$ and $(\beta) = V\overline{V}$.

$$\begin{cases} (\alpha) = U\overline{U} \\ (\beta) = V\overline{V} \end{cases} \xrightarrow{\Psi} (\alpha\beta) = (UV)(\overline{UV}) \xrightarrow{\Phi} \begin{cases} (\alpha) = ((\alpha) + UV)((\alpha) + \overline{UV}) \\ (\beta) = ((\beta) + UV)((\beta) + \overline{UV}) \end{cases}$$

So we need to show that $((\alpha) + UV) = U$ and $((\beta) + UV) = V$.

$$((\alpha) + UV) = U\overline{U} + UV = U(\overline{U} + V) = U.$$

The last equality holds since $\alpha \in \overline{U}$ and $\beta \in V$ and $\gcd(\alpha, \beta) = 1$ implying that $1 \in (\overline{U} + V)$. Similarly

$$((\beta) + UV) = V\overline{V} + UV = V(\overline{V} + U) = V.$$

We have just shown that $\mathbf{d_2}(\alpha)$ is multiplicative. Let $\alpha = p^\gamma$, where p is a prime in $\mathbb{Z}$.

A prime ideal (p) of $\mathbb{Z}$ when viewed as an ideal of the ring of the integers of $\mathbb{Q}(\sqrt{D})$ can behave in the following three ways.

1) (p) remains a prime ideal

2) $(p) = L^2$

3) $(p) = L\overline{L}$.

In the first case, the only ideal factorization can be $(p^\gamma) = (p^{\frac{\gamma}{2}})(p^{\frac{\gamma}{2}})$ and it is only possible if γ is even. In the second case we get the unique ideal factorization $(p^\gamma) = (L^\gamma)(L^\gamma)$. In the last case $(p^\gamma) = (L^n\overline{L^m})(L^m\overline{L^n})$, where $m + n = \gamma$. Thus the number of such ideal factorizations are $\gamma + 1$, i.e. is equal to $\mathbf{d}(p^\gamma)$. Combining all three cases together we see that $\mathbf{d_2}(p^\gamma) \leq \mathbf{d}(p^\gamma)$.

Since both $\mathbf{d_2}(\alpha)$ and $\mathbf{d}(\alpha)$ are multiplicative we conclude the following

$$\mathbf{d_2}(\alpha) \leq \mathbf{d}(\alpha).$$

This implies that

$$\mathbf{d_1}(\alpha) \leq 6\mathbf{d_2}(\alpha) \leq 6\mathbf{d}(\alpha)$$

and the number of integral solutions of $X^2 - DY^2 = -16a(4\Delta)$ is at most $6\mathbf{d}(-16a(4\Delta))$. For each pair of solutions of $X^2 - DY^2 = -16a(4\Delta)$ we can get at most 4 corresponding integral solutions on the original curve. Thus the number of integral points on an ellipse is bounded from above by $24\mathbf{d}(-16a(4\Delta))$.

This completes the proof.

3.2 Integral Points on Quadratic Surfaces

In this section we are considering the following question. Let $q(x, y, z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbb{Z}$. If q is a definite form, then the real points of $q(x, y, z) = k$ form an ellipsoid (if there are any real points at all), and there are finitely many integral points (possibly zero). We will not consider that case. We will assume that the above form q is not definite. So, by multiplying both sides of the equation by (-1) if necessary, without loss of generality we may assume that $q(x, y, z)$ has signature $(1, 2)$; i.e. the matrix representation for the quadratic form has one positive and two negative eigenvalues. We are interested in estimating an upper bound for the number of integral solutions (x, y, z) with $|x|, |y|, |z| \leq B$.

In other words, we are given the following quadratic equation:

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = k$$

where $a, b, c, d, e, f, \in \mathbb{Z}$, and $\gcd(a, b, c, d, e, f) = 1$. The determinant of the quadratic form is given by $\Delta = \frac{4acf+bde-ae^2-b^2f-cd^2}{4}$. Note that $\Delta > 0$ since we assumed that the signature is $(1, 2)$.

We will look at two cases. In Theorem 3 we assume that there is a rational point at infinity on the closure of this surface in $\mathbf{P}^3$, and in Theorem 4 we consider the general case. Even though the bounds in both theorems and the main idea are the same, we use slightly different techniques which makes both theorems worth stating. The idea in the proofs is to transform a given surface to a surface that we

can slice with planes $z = C'$ (as C' varies) and each slice is a hyperbola with two rational points at infinity (Theorem 3) or an ellipse (Theorem 4). There will be only finitely many integral points on each slice. Then we will sum up the number of integral points on those slices to get our estimates.

3.2.1 Hyperbola Case

Theorem 3. *Let $q(x, y, z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbb{Z}$ with signature $(1, 2)$. Moreover, we assume that there is a rational point at infinity. For any $B > 0$, an upper bound for the number of integral solutions (x, y, z) with $|x|, |y|, |z| \leq B$ is $KB \log B$ if $\sqrt{\frac{-k}{4\Delta}}$ is not in $\mathbb{Q}$, and $KB(\log B)^2$ otherwise, where K is a constant that depends only on the coefficients of the original polynomial, and not on B.*

Proof: Assume that there is a rational point $[X : Y : Z : 0]$ that lies on the following variety in $\mathbf{P}^3$

$$V : ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = kw^2.$$

Then we can find a linear map M with $\det(M) = 1$, such that $M(V)$ contains the point $[0 : 1 : 0 : 0]$ and M induces a bijection between integral points on V and on $M(V)$. Furthermore, there exists a constant C such that for all $\bar{x} \in V$

$$\frac{1}{C} H(M(\bar{x})) \leq H(\bar{x}) \leq C H(M(\bar{x})).$$

To see that such $M \in SL_4(\mathbb{Z})$ exists, consider the following argument. We assume that a rational point at infinity $[X : Y : Z : 0]$ is in reduced form, i.e. $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Y, Z) = 1$. If $[X : Y : Z : 0] = [0 : 1 : 0 : 0]$, then we simply let M be the identity matrix, otherwise let M be as follows:

$$M = \begin{bmatrix} a_{11} & \gcd(X,Z) & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 0 \\ \frac{Z}{\gcd(X,Z)} & 0 & \frac{-X}{\gcd(X,Z)} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where $a_{11}, a_{13}, a_{21}, a_{22}, a_{23}$ are integers that satisfy

$$a_{21}X + a_{22}Y + a_{23}Z = 1$$

$$a_{11}\frac{X}{\gcd(X,Z)} + a_{13}\frac{Z}{\gcd(X,Z)} = -Y.$$

Then $\det(M) = 1$ and M sends $[X : Y : Z : 0]$ to $[0 : 1 : 0 : 0]$. So M gives us the required change of coordinates map. Moreover, this transformation preserves the determinant of the original quadratic form.

Thus, without loss of generality, we may assume that $[0 : 1 : 0 : 0] \in V$, implying that $c = 0$. We may also assume that $b \neq 0$, since if b happens to be zero, we can use an additional change of variables to get a surface with $b \neq 0$.

So we have the following equation:

$$ax^2 + bxy + dxz + eyz + fz^2 = k.$$

By keeping $z \in \mathbb{Z}$ fixed, we get the following conic section:

$$ax^2 + bxy + (dz)x + (ez)y + (fz^2 - k) = 0.$$

We can count the number of solutions (x, y) to the above equation. This is a hyperbola with two rational points at infinity, unless it is degenerate, and in that case it is a union of two lines.

The matrix representation for the conic section is

$$A_z = \begin{bmatrix} a & \frac{1}{2}b & \frac{1}{2}dz \\ \frac{1}{2}b & 0 & \frac{1}{2}ez \\ \frac{1}{2}dz & \frac{1}{2}ez & fz^2 - k \end{bmatrix}.$$

The determinant is given by

$$\Delta_{A_z} = \det(A_z) = \frac{(4\Delta)z^2 + kb^2}{4}.$$

The conic section is degenerate if $\Delta_{A_z} = 0$. This happens if $z = \pm\sqrt{\frac{-kb^2}{4\Delta}}$.

First we will assume that $\sqrt{\frac{-k}{4\Delta}}$ is not in $\mathbb{Q}$. In that case the conic section is not degenerate for all $-B \leq z \leq B$. Moreover, if we consider $4\Delta_{A_z} = (4\Delta)z^2 + kb^2$ as a polynomial in z we can conclude that it is irreducible over $\mathbb{Z}$.

Using Theorem 1, we know that an upper bound for the number of integer solutions to $ax^2 + bxy + (dz)x + (ez)y + (fz^2 - k) = 0$ for fixed z is $4\mathbf{d}(4\Delta_{A_z})$ where $\mathbf{d}(\mu)$ denotes the number of positive divisors of μ. Thus as z varies from $-B$ to B

an upper bound for the number of integer solutions on the surface is given by

$$\sum_{z=-B}^{B} 4\mathbf{d}(4\Delta_{A_z}) = 4\mathbf{d}(4\Delta_{A_0}) + 2\sum_{z=1}^{B} 4\mathbf{d}(4\Delta_{A_z})) =$$

$$4\mathbf{d}(2b^2) + 2\sum_{z=1}^{B} 4\mathbf{d}(4\Delta z^2 + kb^2).$$

Erdős [Erd52] proves an upper bound for the sum of the divisors of a quadratic function $f(z)$, assuming that the given polynomial is irreducible. We already saw that $4\Delta_{A_z} = 4\Delta z^2 + kb^2$ (considered as a polynomial in z) is irreducible over $\mathbb{Z}$, so we may apply Erdős' result to it:

$$4\mathbf{d}(kb^2) + 2\sum_{z=1}^{B} 4\mathbf{d}(4\Delta z^2 + kb^2)$$

$$\leq c_0 + 2c_1 B\log(B) \leq KB\log B$$

where K is a constant that depends on the coefficients of the original polynomial, but not on B.

Now consider the case when $\sqrt{\frac{-k}{4\Delta}}$ is in $\mathbb{Q}$. In that case there might be two $z \in \mathbb{Z}$ such that the corresponding conic section becomes degenerate, i.e the union of two lines. There are at most $8B$ points on those conic sections, so we may neglect them. What is more important in that case, is that if $\sqrt{\frac{-k}{4\Delta}} \in \mathbb{Q}$, then $4\Delta_{A_z} = (4\Delta)z^2 + kb^2$ when considered as a polynomial in z is reducible. We will use results of Ennola [Enn68] for the sums of divisors of reducible polynomials to get the following upper bound for the number of integer solutions on the surface.

$$\sum_{z=-B}^{B} 4\mathbf{d}(4\Delta_{A_z}) = 4\mathbf{d}(4\Delta_{A_0}) + 2\sum_{z=1}^{B} 4\mathbf{d}(4\Delta_{A_z}))$$

$$= 4\mathbf{d}(2b^2) + 2\sum_{z=1}^{B} 4\mathbf{d}(4\Delta z^2 + kb^2) \leq KB(\log B)^2$$

where K is a constant that depends on the coefficients of the original polynomial, but not on B.

This finishes the proof of Theorem 3.

3.2.2 Ellipse Case

Theorem 4. *Consider $q(x, y, z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbb{Z}$ with signature $(1, 2)$. For any $B > 0$, an upper bound for the number of integral solutions (x, y, z) with $|x|, |y|, |z| \leq B$ is $KB \log B$ if $\sqrt{\frac{-kD}{4\Delta}}$ is not in $\mathbb{Q}$, and is $KB(\log B)^2$ if $\sqrt{\frac{-kD}{4\Delta}} \in \mathbb{Q}$, where K, D are constants that depend on the coefficients of the original polynomial, and Δ is the determinant of q.*

Proof: We first reduce to the case that $D = b^2 - 4ac < 0$.

Let

$$\ell := \begin{cases} A_1 x + A_2 y + A_3 z = 0 \\ w = 0 \end{cases}$$

be defined over $\mathbb{Q}$ and such that $V \cap \ell$ consists of two points conjugate over an

imaginary quadratic field. We can find a matrix $M_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 0 \\ A_1 & A_2 & A_3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ with $\det(M_3) = 1$ and integer entries that induces a bijection between integral points on V and on $M_3(V)$. There exists a constant C such that for all $\bar{x} \in V$

$$\frac{1}{C} H(M(\bar{x})) \leq H(\bar{x}) \leq C H(M(\bar{x})).$$

Thus , in particular, if we prove Theorem 4 for $M_3(V)$, we will have proven Theorem 4 for V. We therefore lose no generality by assuming $V = M_3(V)$. Since $M_3(\ell)$ is the line $z = w = 0$, the family of planes $z = C'$, as C' varies, expresses the surface V as a family of ellipses. In other words, V can be expressed as

$$a'x^2 + b'xy + c'y^2 + d'xz + e'yz + f'z^2 = k \text{ with } b'^2 - 4a'c' < 0.$$

By letting z vary from $-B$ to B, at each step the type of conic section that we get by keeping z fixed is an ellipse. To find an upper bound for the number of integer solutions (in a given range) to the above equation, we will count solutions on each of those ellipses as z varies from $-B$ to B and then take the sum.

By keeping z fixed, the above equation describes an ellipse in $\mathbb{R}^2$ with determinant $\Delta_{A_z} = \frac{4\Delta z^2 + kD}{4}$. There are only finitely many integer points on an ellipse. Using results from Theorem 2, the number of integral points is bounded by $24\mathbf{d}(-16a(4\Delta_{A_z}))$.

Note that in order for the above bound to make sense we require

$$-16a((4\Delta)z^2 + kD) \geq 0.$$

Thus we will have the following cases according to the values of k and a.

If $a < 0$ and $k \leq 0$, then since $D < 0$ and $\Delta > 0$, the above inequality holds for all z. Then an upper bound for the number of integer solutions of $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = k$ with $|z| \leq B$ is given by

$$\sum_{z=-B}^{B} 24\mathbf{d}(-16a(4\Delta_{A_z})).$$

Note in this case $-16a(4\Delta_{A_z}) = -16a((4\Delta)z^2 + kD)$ when considered as a polynomial in z is irreducible over $\mathbb{Z}$ and using similar argument as in Theorem 3 we get an upper bound $KB\log B$, where K is a constant that does not depend on B.

If $a < 0$ and $k > 0$, then $-16a((4\Delta)z^2 + kD) \geq 0$ for $|z| \geq \sqrt{\frac{-kD}{4\Delta}}$, meaning that for $|z| < \sqrt{\frac{-kD}{4\Delta}}$ there are no solutions. Thus an upper bound for the number of integer solutions of $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = k$ with $|z| \leq B$ is given by

$$2\sum_{z=\lceil\sqrt{\frac{-kD}{4\Delta}}\rceil}^{B} 24\mathbf{d}(-16a(4\Delta_{A_z})).$$

If $\sqrt{\frac{-kD}{4\Delta}}$ is not in $\mathbb{Q}$, then $-16a(4\Delta_{A_z}) = -16a((4\Delta)z^2 + kD)$ when considered

as a polynomial in z is irreducible and using a result of Erdős [Erd52], we obtain an upper bound of $KB \log B$. If $\sqrt{\frac{-kD}{4\Delta}} \in \mathbb{Q}$, then $-16a(4\Delta_{A_z}) = -16a((4\Delta)z^2 + kD)$ when considered as a polynomial in z is reducible. We use results of Ennola [Enn68] for the sums of divisors of reducible polynomials to get $KB(\log B)^2$ for an upper bound for the number of integer solutions on the surface. In both cases K is a constant that depends on the coefficients of the polynomial but not on B.

The following argument shows that under our assumptions on the surface, the case $a > 0$ never happens.

For a contradiction we will assume that there exists a surface $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = k$ with $a > 0$, $b^2 - 4ac < 0$, and thus $c > 0$. The corresponding quadratic form has $\Delta = \frac{4acf + bde - ae^2 - b^2 f - cd^2}{4} > 0$ and signature (1, 2).

The condition that $\Delta > 0$ gives us the following inequality:

$$ae^2 - bde + cd^2 + f(b^2 - 4ac) < 0.$$

It is easy to see that the quadratic form $ae^2 - bde + cd^2$ in variables d and e is positive definite implying that $ae^2 - bde + cd^2 \geq 0$ for any integers d and e. We can rewrite the above inequality as

$$f > \frac{ae^2 - bde + cd^2}{-(b^2 - 4ac)}.$$

Thus we can conclude that $f > 0$.

The characteristic polynomial of the quadratic form is given by

$$char(\lambda) = -\lambda^3 + (a+c+f)\lambda^2 + (\frac{e^2+b^2+d^2-4ac-4af-4fc}{4})\lambda + \Delta.$$

Using the assumption that the signature is (1,2), we know that the above polynomial has two negative and one positive roots. By taking the derivative of $char(\lambda)$ we can analyze the local maxima and minima.

$$char'(\lambda) = -3\lambda^2 + 2(a+c+f)\lambda + (\frac{e^2+b^2+d^2-4ac-4af-4fc}{4}).$$

Critical values occur at $\lambda_{1,2} = \frac{2(a+c+f)\pm\sqrt{4(a+c+f)^2+3(e^2+b^2+d^2-4ac-4af-4fc)}}{6}$. Since $(a+c+f) > 0$, the only way we can get two negative and one positive roots of $char(\lambda)$ is when $(e^2+b^2+d^2-4ac-4af-4fc) > 0$, i.e.

$$f < \frac{e^2+d^2+b^2-4ac}{4(a+c)}.$$

Now, combining both inequalities involving f we get the following

$$\frac{ae^2-bde+cd^2}{-(b^2-4ac)} < \frac{e^2+d^2+b^2-4ac}{4(a+c)}.$$

This is true if and only if

$$4(a+c)(ae^2-bde+cd^2) + (b^2-4ac)(e^2+d^2+b^2-4ac) < 0$$

$$(4a^2+b^2)e^2 + (4c^2+b^2)d^2 - (4ab+4cb)ed < -(b^2-4ac)^2.$$

The quadratic form in variables e and d on the LHS of the above inequality is positive definite. This gives us the desired contradiction since the value of the RHS is always negative. Thus $a \leq 0$. Since $b^2 - 4ac < 0$ implies that $a \neq 0$, we can conclude that $a < 0$.

In particular, $a > 0$ is only possible when the surface is ellipsoid.

This completes the proof.

Chapter 4

Conclusion

In this thesis we have found upper bounds for the number of integral points on quadratic curves and the number of integral points with bounded height on quadratic surfaces.

Quadratic Curves.

We considered non-degenerate quadratic curves defined over $\mathbb{Z}$ of two types.

Hyperbolas with two rational points at infinity:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \text{ with } b^2 - 4ac = m^2$$

for some non-zero integer m, and determinant $\Delta = \frac{4acf+bde-ae^2-b^2f-cd^2}{4} \neq 0$. We have shown that the number of integral points is bounded from above by $4\mathbf{d}(4\Delta)$, where $\mathbf{d}(4\Delta)$ denotes the number of positive divisors of 4Δ.

Ellipses:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \text{ with } b^2 - 4ac < 0$$

and determinant $\Delta = \frac{4acf+bde-ae^2-b^2f-cd^2}{4} \neq 0$. We have shown that the number of integral points is not greater than $24\mathbf{d}(-16a(4\Delta))$, where $\mathbf{d}(-16a(4\Delta))$ denotes the number of positive divisors of $-16a(4\Delta)$.

Remark. In the hyperbola case the bound only depends on the determinant of a given curve, while in the case with ellipses, our bound also depends on the coefficient in front of x^2. Note that it is easy to adjust our argument to get an upper bound $24\mathbf{d}(-16c(4\Delta))$, and in particular this latter bound can be used if $|a| > |c|$.

Quadratic Surfaces.

Next we considered quadrics in higher dimension; in particular we looked at non-degenerate quadratic surfaces defined over $\mathbb{Z}$ of the following type:

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = k.$$

We have shown that an upper bound for the number of integral points with height bounded by B is given by $KB \log B$ with an exception that in some cases it is $KB(\log B)^2$, where in both cases K is a constant that depends on the coefficients of the original polynomial but not on B.

Bibliography

[Bil93] Y. Bilu. Effective analysis of integral points on algebraic curves. *Thesis. Beer Sheva*, page 17, 1993.

[CZ03] P. Corvaja and U. Zannier. On the number of integral points on algebraic curves. *J. Reine Angew. Math.*, 565:27–42, 2003.

[DF04] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 2004.

[Dic71] L. E. Dickson. *History of the Theory of Numbers, Volume 2 (Chapter XIII)*. Chelsea Publishing Company, New York, 1971.

[DRS93] W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.*, 1:143–179, 1993.

[EM93] A. Eskin and C. McMullen. Mixing, counting, and equidistribution in lie groups. *Duke Math. J.*, 1:181–209, 1993.

[Enn68] V. Ennola. A note on a divisor problem. *Ann. Univ. Turku. Ser. A I*, 118, 1968.

[Erd52] P. Erdos. On the sum $\sum_{k=1}^{x} d(f(k))$. *J. London Mathematical Society*, 27:7–15, 1952.

[Har77] R. Hartshorne. *Algebraic Geometry. Graduate Texts in Mathematics, 52.* Springer-Verlag, New York, 1977.

[MA] http://documents.wolfram.com/mathematica/functions /advanceddocumentationdiophantinepolynomialsystems.

[MW] Weisstein, eric w. conic section. from mathworld–a wolfram web resource. http://mathworld.wolfram.com/conicsection.html.

[Nag64] T. Nagell. *Introduction to Number Theory (Chapter VI).* Chelsea Publishing Company, New York, 1964.

[Niv42] I. Niven. Quadratic diophantine equations in the rational and quadratic fields. *Transactions of the American Mathematical Society*, 52. No 1:1–11, 1942.

[Pou93] D. Poulakis. Points entiers sur les courbes de genre 0. *Colloq. Math.*, LXVI. 1:1–7, 1993.

[Pou02] D. Poulakis. Affine curves with infinitely many integral points. *Proceedings of the American Mathematical Society*, 131:1357–1359, 2002.

[PV00] D. Poulakis and E. Voskos. On the practical solution of genus zero diophantine equations. *J. Symbolic Computation*, 30:573–582, 2000.

[PV02] D. Poulakis and E. Voskos. Solving genus zero diophantine equations with at most two infinite valuations. *J. Symbolic Computation*, 33:479–491, 2002.

[Sco61] E. J. Scourfield. The divisors of a quadratic polynomial. *Proc. Glasgow Math. Assoc.*, 5:8–20, 1961.

[Sie29] C. L. Siegel. Uber einige anwendungen diophantischer approximationen. *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.*, 1, 1929.

[Sil00] J. H. Silverman. On the distribution of integer points on curves of genus zero. *Theoretical Computer Science*, 235:163–170, 2000.