A Bound On the Average Rank of j-Invariant Zero Elliptic Curves

Samuel Ruth

A Dissertation
Presented to the Faculty of Princeton University in Candidacy for the Degree of Doctor of Philosophy

Recommended for Acceptance by the Department of Mathematics Adviser: Manjul Bhargava

November 2013
Abstract

In this thesis, we prove that the average rank of $j$-invariant 0 elliptic curves, when ordered by discriminant, is bounded above by 3. This work follows from work of Bhargava and Shankar relating elements of the 2-Selmer groups of elliptic curves with equivalence classes of certain binary quartic forms. We also count the number of equivalence classes of these binary quartic forms. This step involves counting the number of points on a quadric in a homogenously expanding non-compact region. To count the number of points on this quadric, we use a modified version of the circle method. This work also has an application to the statistics of the class group of certain pure cubic fields.
Acknowledgements

I was fortunate enough to have many kind, talented fellow students as colleagues during my time at Princeton. I am thankful to all of them for their contributions to the general atmosphere of Fine Hall. Special thanks are owed to Arul Shankar and Kevin Hughes for many helpful conversations about the subject matter of this thesis. I would also like to thank my adviser, Manjul Bhargava, for suggesting my thesis problem, and I thank Manjul and my other reader, Chris Skinner, for advice on making the ideas contained herein as clear as possible.
To my parents, who started me on this path. To my brother, my first scientific colleague. To Rachel, my best friend and leading source of my happiness.
Contents

Abstract ................................................................. iii
Acknowledgements ...................................................... iv

1 Introduction ......................................................... 1
  1.1 Statement of Theorems ......................................... 1
  1.2 Elliptic Curves .................................................. 4
  1.3 2-Torsion in the Class Groups of Monogenic Cubic Fields .. 5

2 Binary Quartic Forms ............................................. 8
  2.1 Reduction Theory .............................................. 8
  2.2 Writing the Count as an Integral ............................ 10
  2.3 Counting Integer Points ....................................... 13
  2.4 The Constants .................................................. 14
    2.4.1 The Infinite Place ........................................ 14
    2.4.2 The Finite Places, \( p \neq 2, 3 \) ........................... 15
    2.4.3 \( p = 2 \) .................................................. 16
    2.4.4 \( p = 3 \) .................................................. 18

3 The Circle Method ............................................... 20
  3.1 The Work of Heath-Brown .................................... 20
    3.1.1 The Singular Integral .................................... 23
    3.1.2 Bounds on \( H_q(\bar{c}) \) .................................. 23
3.1.3 The Singular Series ............................................. 24
3.1.4 Final Analysis ...................................................... 25
3.2 Necessary Modifications .......................................... 27
3.3 A Modified Circle Method ......................................... 28
3.4 The Error Terms for \( t^2 < \eta \) ........................................ 29
3.5 The Error Terms for \( t^2 > \eta \) ........................................ 29
3.5.1 The Expression 3.14 ............................................... 30
3.5.2 The Expression 3.15 ............................................... 31
3.5.3 Proof of Lemma 3.5.1 ............................................. 34

4 The Mean Number of 2-Torsion Elements in the Class Groups of
Pure Monogenic Cubic Fields ........................................... 38
4.1 Computation of \( p \)-adic Densities for Purely Monogenic Cubic Fields . 39
4.1.1 Binary Quartic Forms with \( p^2 \nmid J, p \neq 2,3 \) ....................... 40
4.1.2 Binary Quartic Forms with \( 4 \nmid J \) .................................. 42
4.1.3 Binary Quartic Forms with \( J/27 \not\equiv 0,1,8 \pmod{9} \) ............. 42
4.2 The Bound on The Average Size of 2-Torsion In Pure Monogenic Cubic
Fields ................................................................. 42
4.3 Proof of Lemma 2.2.3 ............................................... 45

5 The Selmer Group ....................................................... 47
5.1 Connection with Binary Quartic Forms ........................... 47
5.2 The Counting Measure ............................................... 48
5.3 Y as a Homogenous Space for the Orthogonal Group .......... 48
5.3.1 \( p \neq 2,3 \) ..................................................... 51
5.3.2 \( p = 2 \) or \( p = 3 \) ............................................. 51
5.4 Comparing Measures ................................................ 52
5.5 Local Densities ..................................................... 53
Chapter 1

Introduction

1.1 Statement of Theorems

In this thesis we prove the following theorem.

**Theorem 1.1.1.** When elliptic curves over $\mathbb{Q}$ with $j$-invariant 0 are ordered by discriminant, the average rank of their Mordell-Weil groups is bounded above by 1.5.

This theorem is a consequence of a stronger result.

**Theorem 1.1.2.** When elliptic curves over $\mathbb{Q}$ with $j$-invariant 0 are ordered by discriminant, the average size of their 2-Selmer groups is bounded above by 3.

We conjecture that this inequality is in fact an equality.

**Conjecture 1.1.3.** When elliptic curves over $\mathbb{Q}$ with $j$-invariant 0 are ordered by discriminant, the average size of their 2-Selmer groups is 3.

The gap between Theorem 1.1.2 and Conjecture 1.1.3 is a uniformity estimate; this point will be discussed in more detail in Chapter 4.

An elliptic curve over $\mathbb{Q}$ can be written in the form $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. For a curve written in this form, we can compute the $j$-invariant by...
\( j = \frac{4A^3}{4A^3 + 27B^2} \). Furthermore, for a given elliptic curve there is a unique representation that satisfies the condition \( p^6 \nmid B \) for all \( p \) with \( p^4 \mid A \). The curves with \( j \)-invariant 0 are then exactly those of the form \( y^2 = x^3 + B \), with \( B \) sixth-power free. These elliptic curves are also the elliptic curves which have CM by \( \mathbb{Q}(\sqrt{-3}) \).

Since any two curves in this family have the same \( j \)-invariant, they are isomorphic over \( \mathbb{C} \). There has been much interest recently in the Selmer groups of quadratic twists of curves. Some results include the following.

- The average size of the 2-Selmer group for the family of elliptic curves \( y^2 = x^3 - D^2x \), where \( D \) varies, is 12 [HB1]. In fact, all the moments of the 2-Selmer groups for these curves have been computed [HB2].

- For \( E \) an elliptic curve with complete 2-torsion over \( \mathbb{Q} \) and no rational 4-torsion, the asymptotic distribution of the ranks of the quadratic twists of \( E \) have been computed [Swin],[Kan].

- Sufficient conditions have been found such that an elliptic curve has twists of arbitrary 2-Selmer rank. If \( E \) is an elliptic curve with no rational 2-torsion, then for any \( r \) such that \( E \) has one quadratic twist of Selmer rank \( r \), a proportion greater than some constant times \( X/\log(X) \) of quadratic twists of \( E \) with conductor less than \( X \) have Selmer rank \( r \) [MazRub].

- If \( E \) is an elliptic curve over a number field \( K \), the proportion of quadratic twists of \( E \) such that the 2-Selmer group modulo the 2-torsion points has odd dimension over \( \mathbb{F}_2 \) is a ratio of local factors. The distribution of Selmer ranks for certain quadratic twists are worked out for elliptic curves with \( \text{Gal}(K(E[2])/K) = S_3 \), when the twists are ordered a certain way [KMR].

- If \( E \) is an elliptic curve with a single non-trivial two-torsion point and no cyclic 4-isogeny defined over \( \mathbb{Q}(E[2]) \), then the distribution of the Selmer rank of all
quadratic twists with absolute discriminant less than $X$, divided by $\sqrt{\log \log X}$, converges weakly to a normal distribution [Kla].

- A possible explanation for the average size of 2-Selmer is given by modeling the 2-Selmer group as an intersection of two random maximal isotropic subspaces [PR].

- For the elliptic curves $E_k : y^2 = x^3 + k$, we have $\sum_{0 < k < X} C^{rk(E_k)} \ll C \cdot X$, for $C \in (1, \sqrt{3}]$ [Fou].

In their recent paper [BhaSha], Bhargava and Shankar prove the analogs of Theorem 1.1.1 and Conjecture 1.1.3 when averaging over all elliptic curves. It should be noted that they order their curves by an invariant called height. In general, ordering by height is not the same as ordering by discriminant, but it is in the case of $j$-invariant 0 elliptic curves.

Bhargava and Shankar use a map between 2-Selmer groups and certain equivalence classes of binary quartic forms. Let $V$ be the real vector space of binary quartic forms over $\mathbb{R}$; we write an element $f \in V$ as $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$. Then $GL_2(\mathbb{Z})$ acts on $V$ by linear change of variable, that is, for $g \in GL_2(\mathbb{Z})$, $(g.f)(x, y) = f((x, y)g)$. The ring of polynomial invariants of this action is freely generated over $\mathbb{R}$ by two polynomials, traditionally denoted $I$ and $J$. For $f$ as above, we have the following formulae:

$$I(f) = 12ae - 3bd + c^2$$

and

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

From the reduction theory of Bhargava-Shankar and a modification of the circle method of Heath-Brown [HB], we prove the following theorem.
Theorem 1.1.4. The number of $GL_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms with $I = 0$, $0 < |J| < X$, and no linear factor is

$$\frac{4\zeta(2)X}{75} \prod_{p \text{ prime}} \left(1 + \frac{1}{p^3 + p^2 + p}\right) + O_\varepsilon(X^{5/6+\varepsilon}).$$

As in Bhargava-Shankar, this count has an application to the class groups of monogenic cubic fields. A cubic field is a field of degree 3 over $\mathbb{Q}$. A number field $K$ is called monogenic if its ring of integers can be written in the form $\mathbb{Z}[x]$ for some $x \in K$. We say a field $\mathbb{Q}(\sqrt[3]{d})$ is purely monogenic if $\mathbb{Z}[\sqrt[3]{d}]$ is its ring of integers.

Theorem 1.1.5. When purely monogenic cubic fields of the form $\mathbb{Q}(\sqrt[3]{d})$ are ordered by discriminant, the average size of the 2-torsion subgroups of their class groups is bounded above by 2.

We detail now the relationship between binary quartic forms, elliptic curves, and the class group of cubic fields.

1.2 Elliptic Curves

The invariants $I$ and $J$ of a binary quartic form are relative invariants for the action of $GL_2(\mathbb{R})$, that is, for $g \in GL_2(\mathbb{R})$, we have $I(g.f) = (\det g)^4 I(f)$ and $J(g.f) = (\det g)^6 J(f)$, where $\det g$ is the determinant of $g$. If we define a $GL_2(\mathbb{R})$ action by $g.f(x, y) = \frac{1}{(\det g)^2} f((x, y)g)$, this $GL_2(\mathbb{R})$ action descends to $PGL_2(\mathbb{R})$ and preserves $I$ and $J$. A binary quartic form $f(x, y)$ over $\mathbb{Q}$ is called locally soluble if $x^2 = f(x, 1)$ has a solution over $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime $p$. We have the following bijection.

Proposition 1.2.1 ([BirSwi, BhaSha]). Let $E$ be the elliptic curve $y^2 = x^3 + Ax + B$. Then there is a 1-to-1 correspondence between elements of the 2-Selmer group of $E$ and $PGL_2(\mathbb{Q})$-equivalence classes of locally soluble integral binary quartic forms with invariants equal to $-3 \cdot 2^4 A$ and $-27 \cdot 2^6 B$. Furthermore, the set of integral
binary quartic forms that have a rational linear factor and fixed invariants $3 \cdot 2^4 A$ and $-27 \cdot 2^6 B$ lie in one $\text{PGL}_2(\mathbb{Q})$-equivalence class, and this class corresponds to the identity element in the 2-Selmer group of $E$.

Therefore, to count the total number of 2-Selmer elements for elliptic curves with $j$-invariant 0 and $|J| < X$, we start by counting the number of $\text{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms with $I = 0$ and $0 < |J| < X$. Then we count the number of distinct $\text{GL}_2(\mathbb{Z})$-orbits inside each $\text{PGL}_2(\mathbb{Q})$-orbit. We then impose congruence conditions to count only the locally soluble binary quartic forms. An improvement in this step would allow us to prove Conjecture 1.1.3.

To get a bound on the average Mordell-Weil rank of the curves, we use the exact sequence:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \text{Sel}_2(E) \to \text{III}_E[2] \to 0,$$

where $\text{III}_E[2]$ is the 2-torsion in the Tate-Shafarevich group $\text{III}_E$ of $E$. The group $\text{Sel}_2(E)$ is an elementary abelian 2-group; its order is thus $2^s$ for some integer $s$, called the 2-Selmer rank of $E$. From the above exact sequence we see that the 2-Selmer rank bounds the Mordell-Weil rank of the elliptic curve. Theorem 1.1.2 implies that the 2-Selmer rank is bounded by 1.5, which implies Theorem 1.1.1.

### 1.3 2-Torsion in the Class Groups of Monogenic Cubic Fields

We begin with some definitions. A cubic field over $\mathbb{Q}$ is a degree 3 extension of $\mathbb{Q}$. A pure cubic field $K$ is one that can be written $K = \mathbb{Q}(\sqrt[3]{d})$ for some $d \in \mathbb{Z}$. If $R$ is a ring and $A$ is an algebra over $R$, then $A$ is called monogenic over $R$ if there exists some $x \in A$ such that $A = R[x]$ as an $R$-algebra. For $K$ a number field, let $\mathcal{O}_K$ be
the ring of integers of $K$. Then $K$ is called monogenic if $\mathcal{O}_K$ is monogenic over $\mathbb{Z}$. If $K$ is of the form $\mathbb{Q}(\sqrt[n]{\alpha})$ for some $n$-th power-free $\alpha \in \mathbb{Z}$, we call $K$ purely monogenic if $\mathbb{Z}[\sqrt[n]{\alpha}]$ is the ring of integers of $K$.

A result of Dedekind [Ded] says that $\mathbb{Z}[\sqrt{d}]$ is a maximal order if and only if $d$ is square-free and $d \not\equiv 1, 8 \pmod{9}$. So Theorem 1.1.5 is about the 2-torsion in the class groups of these fields. We need the following theorem.

**Theorem 1.3.1** ([Woo, Bha3]). Suppose $\mathbb{Z}[\sqrt{d}]$ is a maximal cubic order. Then there is a bijection between $GL_2(\mathbb{Z})$-equivalence classes of binary quartic forms with $I$-invariant 0 and $J$-invariant $27d$ and elements of the 2-torsion subgroup of the class group of $\mathbb{Q}(\sqrt{d})$.

We will start by bounding above the number of $GL_2(\mathbb{Z})$-equivalence classes of binary quartic forms of bounded $J$-invariant that give maximal rings under this bijection. We then divide this number by the number of purely maximal cubic fields. This will give us the average size of the 2-torsion subgroup of the class group over purely monogenic cubic fields.

The organization of this thesis is as follows. In Chapter 2, we compute the number of $GL_2(\mathbb{Z})$-equivalence classes of binary quartic forms with $I = 0$ and bounded non-zero $J$-invariant. As in Bhargava-Shankar, this problem is reduced to counting the number of certain integral points in a non-compact region. We wish to count the number of points in this region that lie on a quadric, and the circle method is a natural tool for doing so. However, the cusps of this region prevents us from being able to simply use one of the theorems of [HB], and we instead have to make some modifications. These difficulties and modifications are discussed in Chapter 3. To get a one-to-one correspondence with elements of the 2-Selmer group, we need to take $PGL_2(\mathbb{Q})$-equivalence classes. The conversion from $GL_2(\mathbb{Z})$-equivalence to $PGL_2(\mathbb{Q})$-equivalence takes place in Chapter 5, and we are then able to bound the average size.
of the 2-Selmer group of elliptic curves with $I = 0$ when ordered by discriminant. In Chapter 4, we compute a bound on the average size of the 2-torsion subgroup of the class groups of purely monogenic cubic fields, as well as proving some auxiliary lemmas.
Chapter 2

Binary Quartic Forms

Let $V$ denote the real vector space of binary quartic forms over $\mathbb{R}$. We denote a generic element $f \in V$ as $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$. If the coefficients are all in $\mathbb{Z}$, we say $f$ is integral. The set of integral forms we denote by $V_\mathbb{Z}$. Let $G = \text{GL}_2(\mathbb{R})$ and let $\text{GL}_2^\pm(\mathbb{R})$ denote the subgroup of $G$ with determinant $\pm 1$. The group $\text{GL}_2^\pm(\mathbb{R})$ acts on the left on the vector space $V$ by change of variables on the right, that is, if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $(g.f)(x, y) = f(ax + cy, bx + dy)$. The ring of polynomial invariants of this action is freely generated over $\mathbb{R}$ by two elements,

$$I = 12ae - 3bd + c^2 \quad \text{and} \quad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$ 

The discriminant of $f$ is then equal to $(4I^3 - J^2)/27$. These two invariants $I$ and $J$ are also relative invariants for the action of $G$. For $g \in G$, we have $I(g.f) = (\det g)^4I(f)$ and $J(g.f) = (\det g)^6J(f)$.

2.1 Reduction Theory

We aim here to count the number of $\text{GL}_2(\mathbb{Z})$-equivalence classes of binary quartic forms with $I$-invariant equal to 0 and bounded non-zero $J$-invariant. We have the
following fact from Cremona [Crem].

**Proposition 2.1.1.** If $4I^3 - J^2 < 0$, then the set of binary quartic forms having fixed invariants $I$ and $J$ consists of one $G$-orbit.

We also have, for $g \in G$ and $f \in V$, that $J(g.f) = (\det g)^6 J(f)$. So all $f \in V$ such that $I(f) = 0$ and $J(f) > 0$ are $G$-equivalent, and the same is true for negative $J$. Let $v_0 = x^3y + 2x^2y^2$. This point has $I(v_0) = 0$ and $J(v_0) = -2$. For $F$ a subset of $G$, let $Fv_0 = \{ gv_0 | g \in F \}$. We regard $Fv_0$ as a multiset, where the multiplicity of a point $v$ in $Fv_0$ is equal to the number of $g \in F$ with $gv_0 = v$.

We have the following lemma from [BhaSha]:

**Lemma 2.1.2.** A binary quartic form with $I = 0$ and $J$ non-zero has $G$-stabilizer of size 4.

Note that two of these elements are the identity matrix and its additive inverse. For this reason, if we take a fundamental domain $F$ for the left action of $GL_2(\mathbb{Z})$ on $G$ and consider the multiset $Fv_0 \subset V$, the resulting multiset would contain every $GL_2(\mathbb{Z})$-equivalence class of binary quartic form with $I = 0$ and $J < 0$ exactly twice, except for the points whose $G$-stabilizers lie entirely in $GL_2(\mathbb{Z})$. These points are relatively rare, a fact which we will state formally in Lemma 2.2.3. With this caveat in mind, the total number of $GL_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms with $I = 0$ and $0 < |J| < X$ is equal to the number of such points in the single orbit $Fv_0$, as we divide by 2 to account for multiplicity, and multiply by 2 to account for positive and negative $J$. Now for the sake of the circle method, it is easier to replace the single point $v_0$ by a line where $J$ is a non-zero constant and where there is exactly one point $v$ with $I(v) = 0$. We will use the line

$$L = \{ x^3y - \frac{s}{3}xy^3 + \frac{2}{27}y^4 | -1 \leq s \leq 1 \}.$$
Note that \( I(x^3y - \frac{2}{3}xy^3 + \frac{2}{27}y^4) = s \). It is still the case that every \( \text{GL}_2(\mathbb{Z}) \)-equivalence class with \( I = 0 \) and \( J < 0 \) will appear exactly twice in \( \mathcal{F}L \) (except for those whose \( G \)-stabilizer lies entirely in \( \text{GL}_2(\mathbb{Z}) \)) and so counting the number of integral \( \text{GL}_2(\mathbb{Z}) \)-orbits with \( I = 0 \) and \( 0 < |J| < X \) is reduced to counting the number of integral points with \( I = 0 \) and \( 0 < |J| < X \) in \( \mathcal{F}L \).

Now let \( \mathcal{F} \) denote Gauss’s fundamental domain for \( \text{GL}_2(\mathbb{Z}) \backslash G \), which we then Iwasa decompose as \( \mathcal{F} = \Lambda \text{NAK} \), where

\[
N = \left\{ \begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix}, u \in \nu(\alpha) \right\}, \quad A = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}, t \geq \frac{\sqrt{3}}{2} \right\},
\]

\( K = \text{SO}(2), \nu(\alpha) \) is the union of one or two subintervals of \( [-\frac{1}{2}, \frac{1}{2}] \) depending on the value of \( \alpha \in A \), and

\[
\Lambda = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}, \lambda > 0 \right\}.
\]

We will use \( a_t \) to denote an element of \( A \) with parameter \( t \), \( k \) for an element of \( K \) and \( n \) for an element of \( N \). The notation \( \lambda \) will mean both a real number and the \( 2 \times 2 \) matrix \( \lambda I_2 \), where \( I_2 \) is the \( 2 \times 2 \) identity matrix.

### 2.2 Writing the Count as an Integral

We begin with the same steps as in Bhargava-Shankar, which allow us to write our counting function as an integral over the fundamental domain \( \mathcal{F} \).

Let \( G_0 \) be a compact left \( K \)-invariant set in \( G \) that is the closure of a nonempty open set and in which every element has determinant greater than or equal to 1. We will denote the set of points \( v \in V_2 \) with \( I(v) = 0 \) by \( Y \).

Now let \( Y^\text{irr} \) denote the points of \( Y \) with no linear factor and non-zero \( J \). We use \( N(Y^\text{irr}; X) \) to denote the number of \( \text{GL}_2(\mathbb{Z}) \)-equivalence classes of binary quartic
forms in $Y$ with $|J| < X$, where points whose $G$-stabilizer lies entirely in $GL_2(\mathbb{Z})$ are counted with weight $1/2$.

We may write

$$N(Y^{irr}; X) = \frac{\int_{h \in G_0} \# \{ x \in \mathcal{F}hL \cap Y^{irr} : |J(x)| < X \} dh}{\int_{h \in G_0} dh}.$$  \hspace{1cm} (2.1)

Here $dh$ is a Haar measure on $G$. (We normalize it so that the measure of $K$ is 1.)

We write $C_{G_0}$ for $\int_{h \in G_0} dh$. Let $B(n, t, \lambda, X) = na_t \lambda G_0 L \cap \{ v : |J(v)| < X \}$. By the same process as [BhaSha] Section 2.2, we may rewrite Equation 2.1 as

$$N(Y^{irr}; X) = \frac{1}{C_{G_0}} \int_{g \in \text{NA}_\Lambda} \# \{ v \in Y^{irr} \cap B(n, t, \lambda, X) \} t^{-2} dnd^*td^*\lambda.$$  \hspace{1cm} (2.2)

We only want to count the points with no linear factors. First we show that large values of $t$ in $\mathcal{F}$ only give forms with linear factors. Let $C$ be a constant that bounds the absolute values of the coefficients for all $f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ in $G_0L$.

**Proposition 2.2.1.** If $\frac{C\lambda^4}{t^4} < 1$, then all integer forms in $Na_t\lambda G_0 L$ have linear factors.

Any point in the described region must have $a < 1$. If it is an integer point, then we must have $a = 0$, which implies that the form is divisible by $y$.

So the integrand in Equation 2.2 is 0 when $t^4 > C\lambda^4$. We also see that the integrand is 0 when $\lambda$ is greater than some constant $C'$ times $X^{\frac{1}{12}}$, since $J(f, \lambda) = \lambda^{12}J(f)$. These two facts means that in Equation 2.2 we can replace integrating over $\mathcal{F}$ with integration over the subset $\mathcal{F}'$ where $\lambda < C'X^{\frac{1}{12}}$ and $t^4 < C\lambda^4$.

Now we count the linear factors with $a \neq 0$.

**Lemma 2.2.2.** The number of integral binary quartic forms in $\mathcal{F}'G_0 L$ with $I$-invariant $\theta$, $0 < |J| < X$, $a \neq 0$ and a linear factor is $O(X^{\frac{5}{8}})$. 

11
Proof. First we count the number of such binary forms with \( e = 0 \). We see there are \( O(X^{1/3}) \) choices for \( a \), and we want to count the number of solutions to \(-3bd + c^2 = 0\). We see for every non-zero value of \( c \), of which there are \( O(X^{1/3}) \), we choose \( b \) to be some divisor of \( c^2 \), of which there are \( O(X^\varepsilon) \) and then \( d \) is uniquely determined. This gives us \( O(X^{2/3+\varepsilon}) \) binary quartic forms. If \( c = 0 \), then either \( b = 0 \) or \( d = 0 \). If \( d = 0 \), then \( b \) may take on any of \( O(X^{1/3}) \) values, giving \( O(X^{2/3}) \) such terms. If \( b = 0 \), then \( d \) may take on any of \( O(X^{1/2}) \) values, giving a total of \( O(X^{3/5}) \).

Now we count the number of such forms with \( e \neq 0 \). We have \( O(X^{3/5}) \) choices for \( ae \), so \( O(X^{3/5+\varepsilon}) \) choices for \( a \) and \( e \). Then the binary quartic form \( f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \) has a linear factor of the form \( px + qy \), and we must have \( p \mid a \) and \( q \mid e \). Since \( f(-q, p) = 0 \), we can solve for \( c \) in terms of the other 4 variables. Then \( I = 0 \) becomes \(-3bd + b^2(q/p)^2 + d^2(p^2/q^2) + n_1b + n_2d + n_3 = 0 \) for some values \( n_1, n_2, n_3 \) that depend on \( a, b, p \) and \( q \). We want to count the number of integer solutions to this equation with \( bd = O(X^{3/5}) \). We can perform a change of variables to eliminate the cross-term \( bd \), then complete the square separately in \( b \) and \( d \) to get \( Q(b, d) = k \) for some quadratic form \( Q \) and some integer \( k \). So we want to count the number of elements \( m_1 + m_2\sqrt{m} \) of fixed norm in some fixed quadratic extension \( \mathbb{Q}(\sqrt{m}) \), with \( m_1, m_2 = O(X^{2/3}) \). There are \( O(X^{\varepsilon}) \) such solutions, so there are a total of \( O(X^{2/3+2\varepsilon}) \) forms with linear factors and \( e \neq 0 \).

This fact means we may replace \( Y^{irr} \cap B(n, t, \lambda, X) \) with \( Y \cap B(n, t, \lambda, X) \) in Equation 2.2 at the cost of an error term of \( O(X^{3/5}) \). Also, we have picked our range of \( \lambda \) so that \( |J| \leq X \) for all \( \lambda \) in \( \mathcal{F}' \), so the condition \( \{ v : |J(v)| < X \} \) is now superfluous and we will write \( B(n, t, \lambda) \) for \( B(n, t\lambda, X) \).

We note here that points whose \( G \)-stabilizers lie entirely in \( \text{GL}_2(\mathbb{Z}) \) do not contribute to the main term in Theorem 1.1.4.

Lemma 2.2.3. Let \( h \in G_0 \) be any element. Then the number of integral binary quartic forms in \( \mathcal{F}'G_0L \) whose stabilizer in \( \text{GL}_2(\mathbb{Z}) \) has size 4 is \( O(X^{3/5}) \).
We will prove this lemma in Section 4.

2.3 Counting Integer Points

Now we count the points in $B(n, t, \lambda) \cap Y$. We will prove the following in Chapter 3.

**Proposition 2.3.1.** Fix $n, \lambda$ and $t$ with $t < C\lambda$ and $\eta > 0$. The number of points in $B(n, t, \lambda) \cap Y$ is

$$\sigma_\infty \sigma \lambda^{12} + O_\eta(\lambda^{8+\eta} t^{4+\eta}).$$

Here

$$\sigma_\infty = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{x \in na_t G_0 L : |I(x)| < \varepsilon\},$$

where $l$ is Lebesgue measure and

$$\sigma = \prod \sigma_p, \text{ where } \sigma_p = \lim_{n \to \infty} p^{-4n} \# \{v \in V/p^n V : I(v) \equiv 0 \pmod{p^n}\}.$$

We apply this proposition to the equation (2.2) and get

$$N(Y^{\text{irr}}, X) = \frac{\sigma}{C_{G_0}} \int_{g \in F'} \lambda^{12} \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{x \in na_t G_0 L : |I(x)| < \varepsilon\} t^{-2} d^* t d^* \lambda \, d\nu$$

$$+ \int_{g \in F'} O_\eta(\lambda^{8+\eta}) t^2 d^* t d^* \lambda \, d\nu. \quad (2.5)$$

Here we have written our Haar measure on $F'$ in terms of the Iwasawa decomposition. The measures $d^* t$ and $d^* \lambda$ are multiplicative Haar measures. We see that the second summand is $O_\eta(X^{3+\eta}).$

For the first summand, we note that

$$l\{x \in na_t G_0 L : |I(x)| < \varepsilon\} = \lambda^{-20} l\{x \in \lambda na_t G_0 L : |I(x)| < \lambda^8 \varepsilon\}. $$
Making this substitution in Equation 2.3 gives \( N(Y^\text{irr}; X) = \)

\[
\frac{\sigma}{C_{G_0}} \int_{g \in \mathcal{F}} \lambda^{-8} \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{ x \in n a t \lambda G_0 L : |I(x)| < \lambda^8 \varepsilon \} t^{-2} d^* t^* \lambda d n + O_\eta(X^{\frac{s}{8} + \eta}).
\]

(2.6)

Since we are taking a limit, the two occurrences of \( \lambda^8 \) cancel each other. We can now rewrite Expression (2.6) as an integral over \( G_0 \), as in \([\text{BhaSha}]\):

\[
\frac{\sigma}{C_{G_0}} \int_{h \in G_0} \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{ x \in \mathcal{F}'hL : |I(x)| < \varepsilon \} dh
\]

This integral does not depend on \( h \). Therefore we get

\[
N(Y^\text{irr}, X) = \sigma \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{ x \in \mathcal{F}'L : |I(x)| < \varepsilon \} + O_\eta(X^{\frac{s}{8} + \eta}).
\]

2.4 The Constants

2.4.1 The Infinite Place

We first evaluate

\[
\lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} l\{ x \in \mathcal{F}'L : |I(x)| < \varepsilon \}. 
\]

(2.7)

Expression (2.7) can be viewed as an integral of an indicator function. We wish to pull the integral back to \( \text{SL}_2(\mathbb{R}) \times I \times J \). We define the usual subgroups of \( \text{SL}_2(\mathbb{R}) \),

\[
\overline{N} = \begin{pmatrix} 1 & \mu \\ 1 & 1 \end{pmatrix}, A = \begin{pmatrix} t^{-1} \\ t \end{pmatrix}, \text{ and } N = \begin{pmatrix} 1 \\ \nu \\ 1 \end{pmatrix},
\]

(2.8)

where \( \mu, \nu \in \mathbb{R} \) and \( t \in \mathbb{R}^* \). It is well-known that the map \( \overline{N} \times A \times N \to \text{SL}_2(\mathbb{R}) \) is a bijection onto a set of full measure on \( \text{SL}_2(\mathbb{R}) \) under a Haar measure. This map defines a Haar measure \( dg \) on \( \text{SL}_2(\mathbb{R}) \), namely the measure \( dg = t^{-2} d^* td\mu d\nu \). We use the measure \( dg \) and Lebesgue measure on \( I \times J \) to give a measure on \( \text{SL}_2(\mathbb{R}) \times I \times J \).
Recall that \( L = \{ x^3y - \frac{s}{3}xy^3 + \frac{2}{27}y^4 | -1 \leq s \leq 1 \} \). An element of \( L \) has \( J \)-invariant equal to \(-2\) and \( I \)-invariant equal to \( s \). For a pair \((I_0, J_0)\), there is at most one element \( v \in L \) and one positive real number \( \lambda \) with \( I(\lambda v) = I_0 \) and \( J(\lambda) = J_0 \). For an element \( g_0 \in \text{SL}_2(\mathbb{R}) \), there is at most one element \( g\lambda \in \mathcal{F}' \), with \( g \in \text{SL}_2(\mathbb{R}) \), that is \( \text{SL}_2(\mathbb{Z}) \)-equivalent to \( g_0 \). Let \( G \) denote a fundamental domain for the left action of \( \text{SL}_2(\mathbb{Z}) \) on \( \text{SL}_2(\mathbb{R}) \), and let \( G' \) denote the subset of \( G \) that maps onto \( \mathcal{F}' \) under the correspondence describe above. In this way, we get a map from a subset of \( G' \times I \times J \) onto \( \mathcal{F}'L \), so we can pull the integral back to \( \text{SL}_2(\mathbb{R}) \times I \times J \).

The Jacobian of this map is \( \frac{2}{27} \) so that Expression (2.7) is equal to

\[
\frac{2}{27} \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_0^X \int_{-\varepsilon}^\varepsilon \int_{G'} dgdIdJ.
\]

Since

\[
\int_{G-G'} Xdg = O(X) \int_{t=X}^{\infty} \int_{t}^\infty t^{-2}Xd\pi d^*tn) = O(X^{\frac{5}{2}}), \tag{2.9}
\]

we may replace integration over \( G' \) by integration over \( G \), at the cost of an error term \( O(X^{\frac{5}{2}}) \). Making this replacement and integrating gives us

\[
N(Y_{irr};X) = \frac{2\zeta(2)s}{27}X + O(\eta(\sigma^{5/6+\eta}).
\]

2.4.2 The Finite Places, \( p \neq 2, 3 \)

By Proposition 2.3.1, we need to count the number of solutions to \( I \equiv 0 \pmod{p^k} \) in \( V_{\mathbb{Z}}/p^kV_{\mathbb{Z}} \), divide by \( p^{8k} \), and take the limit as \( k \to \infty \). Fix \( p \) a prime not equal to 2 or 3. We start by fixing some \( k \geq 3 \).

Consider the solutions of \( I = 0 \) over \( \mathbb{F}_p \). By the theory of quadratic forms over finite fields [Ger], there are \( p^4 \) solutions, one of which is \( \vec{0} \). For every other solution, one of the coefficients in non-zero. Suppose it is \( a \). Since \( p \neq 2, 3 \), \( \frac{\partial I}{\partial e} = 12a \neq 0 \pmod{p} \). Therefore, for any of the \( p^{4k-4} \) lifts of the other 4 coefficients to \( \mathbb{Z}/p^k\mathbb{Z} \),
there is a unique lift of \( e \) by Hensel’s Lemma. The same reasoning holds if any other coefficient is non-zero. This gives us \( p^{4k} - p^{4k-4} \) solutions.

Now suppose \( p \) divides all the coefficients. Write \( a = pa' \) and similarly for the other coefficients. Then we want to count solutions to \( p^2(12ae' - 3bd' + (c')^2) \equiv 0 \pmod{p^k} \), where the coefficients take values from 0 to \( p^{k-1} \). We see that in fact that only their value \( \pmod{p^{k-2}} \) matters. So the number of solutions in \( \mathbb{Z}/p^k\mathbb{Z} \) where all the coefficients are divisible by \( p \) is \( p^5 \) times the number of solutions of \( 12ae - 3bd + c^2 \equiv 0 \pmod{p^{k-2}} \), where the coefficients take values in \( \mathbb{Z}/p^{k-2}\mathbb{Z} \). So if

\[
N(p; k) := \# \{ \bar{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 : I(\bar{x}) \equiv 0 \pmod{p^k} \},
\]

then we have the recursion relation

\[
N(p; k) = p^{4k} - p^{4k-4} + p^5 N(p; k - 2)
\]

with \( N(p; 1) = p^4 \). Now assume \( k \) is odd (since we know the limit exists, we can take the limit along any subsequence). Say \( k = 2n + 1 \). Then unraveling the recursion relations gives \( N(p; k) = p^{4k} (1 + \sum_{i=1}^{n} p^{-3i} (1 - p^{-1})) \). We divide by \( p^{-4k} \) and let \( k \) go to infinity. Then summing the geometric series gives

\[
\sigma_p = \lim_{k \to \infty} p^{-4k} N(p; k) = 1 + \frac{p^{-3} - p^{-4}}{1 - p^{-3}} = 1 + \frac{1}{p^3 + p^2 + p}.
\]

**2.4.3 \( p = 2 \)**

Now we want to count the number of solutions to \( I \equiv 0 \pmod{2^k} \). This case is more involved because the coefficient of \( ae \) is 12. This means there are non-zero solutions to \( I(\bar{x}) \equiv 0 \pmod{2} \) where all the partial derivatives vanish. So first we count the solutions where \( b \) is odd. We start by fixing \( k \geq 5 \).

If \( b \) is odd, then we may choose \( a, e \) and \( c \) arbitrarily in \( \mathbb{Z}/2^k\mathbb{Z} \), and then \( d \) is
uniquely determined. This gives $2^{4k-1}$ solutions to $I \equiv 0 \pmod{2^k}$ in $(\mathbb{Z}/2^k\mathbb{Z})^5$.

So suppose $b$ is even. Then we must have $c$ is even as well. Write $b = 2b'$, $c = 2c'$, where $b'$ and $c'$ take values from $0$ to $2^{k-1}$. Now we want to count solutions to $2(6ae - 3b'd + 2(c')^2) \equiv 0 \pmod{2^k}$. This is equal to $2^3$ times the number of solutions to $(6a'e' - 3b'd' + 2(c')^2) \equiv 0 \pmod{2^{k-1}}$, where now all the coefficients are in $\mathbb{Z}/p^{k-1} \mathbb{Z}$. Again, we start by counting the solutions where $b'$ is odd. Then $a', e'$ and $c'$ are arbitrary and then $d'$ is uniquely determined. This gives $2^{4k-2}$ solutions to $I \equiv 0 \pmod{2^k}$ in $(\mathbb{Z}/2^k\mathbb{Z})^5$ where $b \equiv 2 \pmod{4}$.

Now suppose $b'$ is even and write $b' = 2b''$, where $b''$ is in the range $0$ to $2^{k-2}$. We are trying to count the number of solutions to $2(3a'e' - 3b''d' + (c')^2) \equiv 0 \pmod{2^{k-1}}$, which is $2^4$ times the number of solutions of $3ae - 3bd + c^2 \equiv 0 \pmod{2^{k-2}}$ where the coefficients now take values in $\mathbb{Z}/p^{k-2} \mathbb{Z}$. To recap, if $b \equiv 0 \pmod{4}$, then we must have $c \equiv 0 \pmod{2}$, and so the number of such solutions in $(\mathbb{Z}/2^k\mathbb{Z})^5$ to $12ae - 3bd + c^2 \equiv 0 \pmod{2^k}$ is equal to $2^7$ times the number of solutions in $(\mathbb{Z}/2^{k-2}\mathbb{Z})^5$ to $3ae - 3bd + c^2 \equiv 0 \pmod{2^{k-2}}$.

Let $I' = 3ae - 3bd + c^2$ and let $N'(2; k) = \#\{x \in (\mathbb{Z}/2^k\mathbb{Z})^5 : I'(x) \equiv 0 \pmod{2^k}\}$. Then we have just shown that $N(2; k) = 2^{4k-1} + 2^{4k-2} + 2^7N'(2; k - 2)$. So we need to investigate the number of solutions of $I' \equiv 0 \pmod{2^{k-2}}$. Now for this equation, the partial derivatives are only all zero when $a, b, d$ and $e$ are even. There are no solutions when $a, b, d, e$ are even and $c$ is odd. If $c$ is even, we can reduce the problem to counting the number of solutions in $(\mathbb{Z}/p^{k-4}\mathbb{Z})^5$ as we did in the previous section. This gives us the recursion relation

$$N'(2; k) = 2^{4k} - 2^{4k-4} + p^5N'(2; k - 2)$$
with $N'(2; 1) = 2^4$. This gives us

$$
\sigma_2 = \lim_{k \to \infty} 2^{-4k}(2^{4k-1} + 2^{4k-2} + 2^7 N'(2; k-2)) = \frac{3}{4} + 2^{-1} \lim_{k \to \infty} 2^{-4(k-2)} N'(k; 2) = \frac{9}{7}.
$$

2.4.4 $p = 3$

This case has the same difficulty as the case $p = 2$, and we will work on it the same way. Fix $k \geq 3$. In order to have $12ae - 3bd + c^2 \equiv 0 \pmod{3^k}$, we must first of all have $c \equiv 0 \pmod{3}$. Write $c = 3c'$. Then we have $I = 3(4ae - bd + 3(c')^2)$.

Suppose $a \not\equiv 0 \pmod{3}$. Then $b, c', d$ are arbitrary and $e$ is determined $\pmod{3^{k-1}}$. This gives $3^{4k} - 3^{4k-1}$ solutions in $(\mathbb{Z}/3^k \mathbb{Z})^5$ to $I \equiv 0 \pmod{3^k}$.

Now suppose $a \equiv 0 \pmod{3}$ and $b \not\equiv 0 \pmod{3}$. Write $a = 3a'$. Then $a', c'$ and $e$ can be chosen arbitrarily, and $d$ is determined $\pmod{3^{k-1}}$. This gives $3^{4k} - 3^{4k-2}$ solutions in $(\mathbb{Z}/3^k \mathbb{Z})^5$ to $I \equiv 0 \pmod{3}$ with $a \equiv 0 \pmod{3}$ and $b \not\equiv 0 \pmod{3}$.

Now suppose $b \equiv 0 \pmod{3}$ and write $b = 3b'$. Now our equation reads $9(4a'e - b'd + (c')^2) \equiv 0 \pmod{3^k}$. This is equal to $3^7$ times the number of solutions to $4ae - bd + c^2 \equiv 0 \pmod{3^{k-2}}$, where now the coefficients all take values in $\mathbb{Z}/3^{k-2} \mathbb{Z}$.

Let $I'' = 4ae - bd + c^2$ and let $N''(3; k) = \# \{x \in (\mathbb{Z}/3^k \mathbb{Z} : I''(x) \equiv 0 \pmod{3^k})\}$. Then we have just shown that $N(3; k) = 3^{4k} - 3^{4k-2} + 3^7 N''(3; k-2)$. By the same reasoning as all other primes, $N''(3; k)$ has the recursion relation $N''(3; k) = 3^{4k} - 3^{4k-4} + N''(3; k - 2)$. This gives us

$$
\sigma_3 = \lim_{k \to \infty} 3^{-4k} N(3; k) = \frac{8}{9} + 3^{-1} \lim_{k \to \infty} 3^{4(k-2)} N''(3; k-2) = \frac{16}{13}.
$$

The results of the previous 3 sections are summed up in this proposition.

**Proposition 2.4.1.**

- For $p \neq 2, 3$, we have $\sigma_p = 1 + \frac{1}{p^r + p^{r-1} + p}$.

- $\sigma_2(I) = \frac{9}{7}$. 

18
• \( \sigma_3(I) = \frac{16}{13} \).
Chapter 3

The Circle Method

In this chapter, we discuss the circle method in the form considered by Heath-Brown [HB]. We begin by stating what Heath-Brown proves and giving an outline of how his proof proceeds. We then explain what work we need to do to get the theorem in the form used in Chapter 2. This work takes up the remainder of the chapter.

We pause to fix some notation for this section. We denote vectors with arrows overhead, as in \( \vec{x} \). We use \( c_i \) to refer to the \( i \)th component of the vector \( \vec{c} \). For two vectors \( \vec{x} \) and \( \vec{y} \), we use \( \vec{x} \cdot \vec{y} \) to denote their dot product. We write \( |\vec{x}| \) for the length of a vector \( \vec{x} \). If we write a sum as being over \( \vec{x} \pmod{q} \), this means each component of \( x \) is taking values in \( \mathbb{Z}/q\mathbb{Z} \) independently. A sum over \( \vec{x} \pmod{q}^* \) means each component of \( \vec{x} \) takes values independently over the units in \( \mathbb{Z}/q\mathbb{Z} \). The function \( e_q(x) \) is defined as \( \exp\left(\frac{2\pi ix}{q}\right) \). We use the Vinogradov notation \( f \ll g \) to mean that \( f \) is less than a constant times \( g \).

3.1 The Work of Heath-Brown

Let \( \omega \) be a smooth, compactly supported function on \( \mathbb{R}^n \) and let \( F \) be a non-singular quadratic form in \( n \) variables with coefficients in \( \mathbb{Z} \). For \( P \) a real number, we wish to
analyze the sum

\[ N(F, \omega, P) = \sum_{\vec{x} \in \mathbb{Z}^n \mid F(\vec{x}) = 0} \omega(P^{-1} \vec{x}) \]

as \( P \) goes to infinity. If \( \omega \) is an approximation of a characteristic function for some bounded region \( R \), then \( N(F, \omega, P) \) is an approximation of the number of zeros of \( F \) in the region \( PR \).

The Heath-Brown refinement [HB] of the Hardy-Littlewood circle method gives us asymptotics for \( N(F, \omega, P) \) for \( n \geq 3 \). For \( n \geq 5 \), we have

\[ N(F, \omega, P) = \sigma_\infty \sigma P^{n-2} + O_{\omega, \eta}(P^{n-4+\eta}), \]

where \( \delta = 0 \) or 1, according as \( n \) is odd or even,

\[ \sigma = \prod_p \sigma_p, \quad \sigma_p = \lim_{k \to \infty} p^{-4k} \# \{ \vec{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 : F(\vec{x}) \equiv 0 \pmod{p^k} \} \]

and

\[ \sigma_\infty = \lim_{\epsilon \to 0} \frac{1}{2\epsilon} \int_{|F(\vec{x})|<\epsilon} \omega(\vec{x}) d\vec{x}. \]

The \( \omega \)-dependence in the constant is determined only by \( \max \{|x| : \omega(\vec{x}) \neq 0\} \), \( \epsilon \), and \( \left\{ \max_{\vec{x}} \left| \frac{\partial^j \omega(\vec{x})}{\partial x_1^{j_1} \cdots \partial x_n^{j_n}} \right| \right\} \), for all \( n \)-tuples of non-negative integers \( (j_1, \ldots, j_n) \) with \( j = j_1 + \cdots + j_n \).

For the remaining formulas, the definition of \( \sigma_\infty \) and \( \sigma_p \) are the same as above. For \( n = 4 \), if the determinant of \( F \) is not a square, we have

\[ N(F, \omega, P) = \sigma_\infty \sigma P^2 + O_{\omega, \eta}(P^{3/2+\eta}). \]  

We need some more notation for the remaining cases. Let \( \sigma^*(F) = \prod_p \sigma'_p \), where \( \sigma'_p = (1 - p^{-1}) \sigma_p \).
If \( n = 4 \) and the determinant is a square, we have

\[
N(F, \omega, P) = \sigma_\infty \sigma^*(F) P^2 \log P + \sigma_1(F, \omega) P^2 + O_{\omega, \eta}(P^{3/2+\eta}),
\]

for some constant \( \sigma_1(F, \omega) \).

Finally, for \( n = 3 \), we have

\[
N(F, \omega, P) = \frac{1}{2} \sigma_\infty \sigma^*(F) P \log P + \sigma_1(F, \omega) P + O_{\omega, \eta}(P^{5/6+\eta}).
\]

for some constant \( \sigma_1(F, \omega) \).

For all \( n \geq 3 \), the Heath-Brown method begins with the statement

**Theorem 3.1.1.** There is an infinitely differentiable function \( h(x, y) \) defined on the set \((0, \infty) \times \mathbb{R}\) such that for any \( Q > 1 \),

\[
N(F, \omega, P) = \left(1 + O_N(Q^{-N})\right) Q^{-2} \sum_{q=1}^{\infty} \sum_{a \mod q} \omega(P^{-1} \vec{x}) e_q(a F(\vec{x})) h \left( \frac{q}{Q}, \frac{F(\vec{x})}{Q^2} \right).
\]

Furthermore, we have

\[
N(F, \omega, P) = \left(1 + O_N(Q^{-N})\right) Q^{-2} \sum_{\vec{c} \in \mathbb{Z}^n} q^{-n} S_q(\vec{c}) H_q(\vec{c}),
\]

where

\[
S_q(\vec{c}) = \sum_{a \mod q} \sum_{\vec{b} \mod q} e_q(a F(\vec{b}) + \vec{c} \cdot \vec{b})
\]

and

\[
H_q(\vec{c}) = \int_{\mathbb{R}^n} \omega(P^{-1} \vec{x}) h \left( \frac{q}{Q}, \frac{F(\vec{x})}{Q^2} \right) e_q(-\vec{c} \cdot \vec{x}) dx.
\]

Moreover \( h(x, y) \ll x^{-1} \) for all \( y \), and \( h(x, y) \) is non-zero only for \( x \leq \max(1, 2|y|) \).

The second equation for \( N(F, \omega, P) \) follows from the first from writing \( x = \vec{b} + q\vec{y} \), applying Poisson summation, and then performing a change of variable in the integral.
3.1.1 The Singular Integral

Heath-Brown then lets $Q = P$ and considers the integral.

$$H_q(\overline{c}) = \int_{\mathbb{R}^n} \omega(P^{-1}\overline{x})h(P^{-1}q, P^{-2}F(\overline{x}))e_q(-\overline{c}.\overline{x})d\overline{x} \quad (3.6)$$

$$= P^n \int_{\mathbb{R}^n} \omega(\overline{x})h(P^{-1}q, F(\overline{x}))e_q(-P\overline{c}.\overline{x})d\overline{x} \quad (3.7)$$

He shows

**Lemma 3.1.2 ([HB, Lemma 13]).** We have $H_q(0) = P^n(\sigma_\infty + O_N((q/P)^N))$.

3.1.2 Bounds on $H_q(\overline{c})$

Heath-Brown next proves bounds on $H_q(\overline{c})$. First we have the following bound.

**Lemma 3.1.3 ([HB, Lemma 16]).** $H_q(\overline{c}) \ll P^n$. The implied constant here only depends on the maximum value of $F(\overline{x})$ on $\text{supp}(\omega)$.

Now we have bounds that depend on $\overline{c}$. He states these bounds in terms of $|\overline{c}|$. However, he proves them by reference to $\max_i\{|c_i|\}$, and for our purposes it is more useful to state them in this form. Heath-Brown proves the following lemma.

**Lemma 3.1.4 ([HB, Lemma 18]).** We have $H_q(\overline{c}) \ll_N P^{n+1}q^{-1}(\max_i\{|c_i|\})^{-N}$.

This lemma shows that the contribution from terms with $\max_i\{|c_i|\} > P^n$ contribute $O_q(1)$ to the sum $N(F, \omega, P)$.

Heath-Brown has another bound on the integral $H_q(\overline{c})$. We will use this bound when $\max_i\{|c_i|\}$ is small but non-zero.

**Lemma 3.1.5 ([HB, Lemma 22]).** We have

$$H_q(\overline{c}) \ll_{\omega, \eta} P^n \left( \frac{\max_i\{|c_i|\}}{q^2} \right)^\eta \left( \frac{P\max_i\{|c_i|\}}{q} \right)^{1-n/2}$$
3.1.3 The Singular Series

Heath-Brown then analyzes the singular series $S_q(\vec{c})$. First we have two lemmas we will use to bound error terms. We have the following general lemma.

**Lemma 3.1.6 ([HB, Lemma 25]).** We have

$$|S_q(\vec{c})| \ll q^{1+n/2}.$$  

We will use this lemma several times. We also need the following lemma.

**Lemma 3.1.7 ([HB, Lemma 28]).** Let $\max_i{|c_i|} < P$. Suppose $n$ is odd. Then for any $\varepsilon > 0$ we have

$$\sum_{q \leq R} |S_q(\vec{c})| \ll \varepsilon R^{(3+n)/2}O_{\eta}(1 + P^n)$$

Heath-Brown actually proves this lemma for some cases when $n$ is even, but we will not need those cases.

Heath-Brown actually needs a better estimate for the case where $n = 3$ and the case $n = 4$ and the determinant of $F$ is a square, but as it is involved and we have no need of it, we will not state it here.

Finally we have the following lemma about the local densities. This lemma is used to get the constants for the main term.

**Lemma 3.1.8 ([HB, Lemma 31]).** When $n \geq 5$ we have

$$\sum_{q \leq R} q^{-n}S_q(\vec{0}) = \prod_p \sigma_p + O_{\eta}(R^{(3+\delta-n)/2+\eta}).$$

When $n = 4$ and $F$ has non-square determinant, we have

$$\sum_{q \leq R} q^{-n}S_q(\vec{0}) = \sigma + O_{F,\eta}(R^{-1/2+\eta}).$$
When \( n = 4 \) and \( F \) has square determinant, or \( n = 3 \), we have

\[
\sum_{q \leq R} q^{-n} S_q(\vec{0}) = c \sigma^*(F) \log R + \sigma^* + O_{F,\eta}(X^{\alpha+\eta-n}),
\]

where if \( n = 4 \), then \( c = 1 \) and \( \alpha = 7/2 \), while if \( n = 3 \), then \( c = 1/2 \) and \( \alpha = \frac{17}{6} \).

### 3.1.4 Final Analysis

Now we show how Heath-Brown puts all these ingredients together in the situation where \( n \geq 5 \) or \( n = 4 \) and the determinant of \( F \) is not a square. The case \( n = 4 \) where the determinant of \( F \) is a square, as well as the case where \( n = 3 \), are more involved and we do not include them here. We will treat the coefficient of \( 1 + O_N(Q^{-N}) \) as 1 in this section. In this section, when we say bounded by, we mean bounded by a constant times.

Let \( T \) be \( \max(F(\vec{x})) \) on supp(\( \omega \)). Since \( h(x, y) = 0 \) for \( x > \max(1, 2|y|) \), we have \( H_q(\vec{c}) = 0 \) if \( q > 2TP \).

We use Equation (3.5) with \( Q = P \) to obtain

\[
N(F, \omega, P) = P^{-2} \sum_{q=1}^{2TP} q^{-n} S_q(\vec{0}) H_q(\vec{0})
\]

\[
+ P^{-2} \sum_{\vec{c} \in \mathbb{Z}_n^n} q^{-n} S_q(\vec{c}) H_q(\vec{c})
\]

We call Expression (3.8) the main term and Expression (3.9) the error terms. We will deal first with the error terms.

Fix \( \eta > 0 \). Let \( B_1 \) be the set of \( \vec{c} \) with \( \max_i \{|(c_i)|\} \leq P^\eta \) and at least one \( c_i \) non-zero. For \( \max_i \{|(c_i)|\} > P^\eta \), we apply Lemma 3.1.4 and Lemma 3.1.6 to get that the part of Equation (3.9) over those values is \( O_{\eta}(1) \). Then Expression (3.9) is equal
to
\[ P^{-2} \sum_{c \in B_1} \sum_{q=1}^{2TP} q^{-n} S_q(\vec{c}) H_q(\vec{c}) + O_\eta(1). \] (3.10)

By Lemma 3.1.5, \( H_q(\vec{c}) \ll_\eta P^{n/2+1+\eta} q^{n/2-1-2\eta} (\max_i \{|c_i|\})^{1-n/2+\eta} \). So Expression 3.10 is bounded by
\[ P^{n/2-1+\eta} \sum_{c \in B_1} \sum_{q=1}^{2TP} q^{-n/2-1-2\eta} |S_q(\vec{c})| (\max_i \{|c_i|\})^{1-n/2+\eta} + O_\eta(1). \] (3.11)

Let \( \delta \) equal 1 if \( n \) is even and 0 if \( n \) is odd. By Lemma 3.1.6 for even \( n \) and Lemma 3.1.7 for odd \( n \),
\[ \sum_{q=1}^{2R} q^{-1-n/2-2\eta} |S_q(\vec{c})| \ll_\eta R^{(1+\delta)/2-\eta}, \]
so Expression 3.11 is bounded by
\[ P^{n/2-1/2+\delta/2-\eta} \sum_{c \in B_1} (\max_i \{|c_i|\})^{1-n/2+\eta} + O_\eta(1). \]

The summand is less than 1, and there are \( P^{m\eta} \) terms. So Expression 3.11 is \( O_\eta(P^{n-1+\delta)/2+mn}) \).

Now we consider \( \vec{c} = \vec{0} \). For \( q > P^{1-\eta} \), by Lemma 3.1.3 and Lemma 3.1.7 we have
\[ P^{-2} \sum_{M \leq q \leq 2M} q^{-n} S_q(\vec{0}) H_q(\vec{0}) \ll_\eta P^{n-2} M^{(3+\delta-n)/2+\eta}, \]
for any \( M \), so that \( \sum_{q>P^{1-\eta}} q^{-n} S_q(\vec{0}) H_q(\vec{0}) \ll_\eta P^{(n-1+\delta)/2+\eta} \).

For \( q < P^{1-\eta} \), we use Lemma 3.1.2 and 3.1.8 to get
\[ P^{-2} \sum_{q \leq P^{1-\eta}} q^{-n} S_q(\vec{0}) H_q(\vec{0}) = P^{n-2} \sigma_\infty \sum_{q \leq P^{1-\eta}} q^{-n} S_q(\vec{0}) + O_\eta(1) \]
\[ = P^{n-2} \sigma_\infty \prod_p \sigma_p + O_\eta(P^{(n-1+\delta)/2+\eta}). \]
3.2 Necessary Modifications

Throughout Heath-Brown’s analysis, he works with a fixed $\omega$ and allows the error terms to depend on this $\omega$. In our case, we want to vary $\omega$ and track how the error terms change as a result. Instead of working with a fixed region, we work with $n a_t G_0 L$ for varying $n$ and $a_t$. We want to count the number of integral zeros of $I$ in $P n a_t G_0 L$, where $P = \lambda^4$,

$$n \in N = \left\{ \begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix}, u \in \nu(\alpha) \right\}, \quad a_t = \begin{pmatrix} t^{-1} \\ t \end{pmatrix},$$

$$\frac{\sqrt{3}}{2} < t < C \lambda,$$ and $u$ is in the union of one or two subintervals of $[-\frac{1}{2}, \frac{1}{2}]$ depending on the value of $t$. We need to be explicit about how these error terms vary with $a_t$.

Recall that $GL_2(\mathbb{R})$ acts on binary quartic forms by change of variables, that is, for $g \in G$, $(g.f)(x, y) = f((x, y)g)$. Thus if we view a binary quartic form as an element of $\mathbb{R}^5$ by the embedding $ax^4 + bx^3 y + cx^2 y^2 + dxy^3 + ey^4 \rightarrow (a, b, c, d, e)$, then $a_t$ acts on $\mathbb{R}^5$ by $a_t \vec{x} = (t^{-4} x_1, t^{-2} x_2, x_3, t^2 x_4, t^4 x_5)$.

We start by defining $\omega$ as a fixed smooth approximation to the characteristic function of $G_0 L$, define $\omega_{n,t}(\vec{x}) = \omega((na_t)^{-1} \vec{x})$, and then analyze $N(I, \omega_{n,t}, P)$. Heath-Brown is not explicit about the effect of linear transformations on the error terms. By going through Heath-Brown’s proof, we will see that the error term is $O_{\omega, \epsilon}(P^{2+\epsilon} t^{6+\epsilon})$, where the implied constant is now independent of $n$ and $a_t$.

For $t > \lambda^{\frac{2}{3}}$, the error term will be larger than the main term, so a new analysis is needed. Note that $P^{2+\epsilon} t^{6+\epsilon}$ is the correct order of magnitude for how many integer points there are in $n a_t G_0 L$ with $x_1 = x_2 = x_3 = 0$, and on these points $I(\vec{x})$ is identically zero. Since these points have a linear factor we do not want to count them. This suggests we only count points with $x_1 \neq 0$, which will require a modified approach. We will deal with this issue in Subsection 3.5.
In the rest of this chapter, dependence on $\lambda$ or $t$ is always made explicit. Since $n$ takes values in a compact set, we can (and do) ignore its effect on bounds. For $\vec{x} = (x_1, x_2, x_3, x_4, x_5)$, we let $\vec{x}' = (x_2, x_3, x_4, x_5)$ be the projection of $\vec{x}$ onto its final 4 coordinates.

### 3.3 A Modified Circle Method

We begin again with the equation

$$N(I, \omega_{n,t}, P) = (1 + O_N(Q^{-N}))Q^{-2} \sum_{\vec{c} \in \mathbb{Z}^5} \sum_{q=1}^{\infty} q^{-5} S_q(\vec{c}) H_q(\vec{c}),$$

(3.12)

where

$$S_q(\vec{c}) = \sum_{a \equiv q^*} \sum_{\vec{b} \equiv q} e_q(aI(\vec{b}) + \vec{c} \cdot \vec{b})$$

and

$$H_q(\vec{c}) = \int_{\mathbb{R}^5} \omega_{n,t}(P^{-1}\vec{x}) h \left( \frac{q}{Q} \frac{I(\vec{x})}{Q^2} \right) e_q(-\vec{c} \cdot \vec{x}) dx.$$  

Now we make a change of variables to get

$$H_q(\vec{c}) = \int_{\mathbb{R}^5} \omega(P^{-1}\vec{x}) h \left( \frac{q}{Q} \frac{I(\vec{x})}{Q^2} \right) e_q(-na_t \vec{c} \cdot \vec{x}) dx.$$  

(3.13)

Note that $I(na_t\vec{x}) = I(\vec{x})$ since $I$ is an invariant, and that $d(na_t\vec{x}) = d\vec{x}$ because $n$ and $a_t$ have determinant 1.

The difficulty now is that in Heath-Brown’s final analysis, he starts by dealing with all terms with $\max_i \{|c_i|\} > P^n$. In our case, this analysis handles the terms with $\max_i \{|(na_t c_i)|\} > P^n$. If $t^2 > P^n$, this inequality is true for all $\vec{c}$ with $c_4$ or $c_5$ non-zero, but we still have all $\vec{c}$ with $|c_1| < t^4 P^n$, $|c_2| < t^2 P^n$ and $|c_3| < P^n$. After this initial step, Heath-Brown only has $O(P^{3n})$ of the $\vec{c}$ left, but we still have $O(t^6 P^{3n})$ of them. This problem means we need a new approach for $t^2 > P^n$. Note that the
calculations for $\vec{c} = \vec{0}$ are unchanged by the presence of $a_t$, so the main term is always the same.

### 3.4 The Error Terms for $t^2 < P^\eta$

We can go through Heath-Brown’s analysis again with the substitution noted above, and we get that

**Proposition 3.4.1.** $N(I, \omega_{n,t}, P) = \sigma_\infty \sigma P^3 + O_\eta(P^{2+\eta}t^{m\eta}),$

for some fixed integer $m$.

We are only interested in binary quartic forms without linear factors, so we need to confirm that the number of these forms with linear factors is small. By Lemma 2.2.2, there are $O(P^{5/2+\eta})$ integral forms in our region with linear factors and $x_1 \neq 0$, so we only need to count the forms with linear factors and $x_1 = 0$. If $x_1 = 0$ then $x_5$ is arbitrary, so the number of quintuples is $t^4P$ times the number of triplets $(x_2, x_3, x_4)$ with $-3x_2x_4 + x_3^2 = 0$, where $|x_2| < t^{-2}P$, $|x_3| < P$, and $|x_4| < t^2P$. The number of such triplets is less than or equal to the number of solutions with all 3 coordinates bounded by $t^2P$, which by Equation (3.3) is $O(t^2P \log(t^2P))$. We thus have a total of $O(t^6P^2 \log(t^2P))$ solutions with $x_1 = 0$, which is $O(P^{2+4\eta})$.

### 3.5 The Error Terms for $t^2 > P^\eta$

Now suppose $t^2 > P^\eta$.

For this case, we start with Equation (3.4).

$$N(I, \omega_{n,t}, P) = P^{-2} \sum_{q=1}^{2TP} \sum_{a \mod q} \sum_{\vec{x} \in \mathbb{Z}^5} \omega_{n,t}(P^{-1}\vec{x})e_q(aI(\vec{x}))h\left(\frac{q}{P}, \frac{I(\vec{x})}{P^2}\right)$$

Let $x = \vec{b} + q\vec{y}$, and we write
\[ N(I, \omega_{n,t}, P) = P^{-2} \sum_{q=1}^{2TP} \sum_{a \mod q} \sum_{\bar{b} \mod q} e_q(aI(\bar{b})) \sum_{y \in \mathbb{Z}^5} \omega_{n,t}(P^{-1}(\bar{b} + qy)) h \left( \frac{q}{P}, \frac{I(\bar{b} + qy)}{P^2} \right) \]

Now, we only want to count solutions with \( x_1 \neq 0 \). This means either that \( b_1 \neq 0 \) (mod \( q \)), or that \( b_1 = 0 \) and \( y_1 \neq 0 \). So we have

\[ \sum_{\tilde{x} \in \mathbb{Z}^5 \atop x_1 \neq 0 \atop I(\tilde{x}) = 0} \omega_{n,t}(P^{-1}\tilde{x}) = \]

\[ P^{-2} \sum_{q=1}^{2TP} \sum_{a \mod q} \sum_{\bar{b} \mod q \atop b_1 \neq 0} e_q(aI(\bar{b})) \sum_{y \in \mathbb{Z}^5} \omega_{n,t}(P^{-1}(\bar{b} + qy)) h \left( \frac{q}{P}, \frac{I(\bar{b} + qy)}{P^2} \right) \]  

(3.14)

\[ + P^{-2} \sum_{q=1}^{2TP} \sum_{a \mod q} \sum_{\bar{b} \mod q \atop b_1 = 0 \atop y_1 \neq 0} e_q(aI(\bar{b})) \sum_{y \in \mathbb{Z}^5} \omega_{n,t}(P^{-1}(\bar{b} + qy)) h \left( \frac{q}{P}, \frac{I(\bar{b} + qy)}{P^2} \right) \]  

(3.15)

### 3.5.1 The Expression 3.14

We apply Poisson summation to Expression (3.14) and get

\[ P^{-2} \sum_{q=1}^{2TP} \sum_{a \mod q} \sum_{\bar{b} \mod q \atop b_1 \neq 0 \mod q} e_q(aI(\bar{b})) \sum_{\tilde{c} \in \mathbb{Z}^5} \int_{\mathbb{R}^5} \omega_{n,t}(P^{-1}(\tilde{b} + q\tilde{y})) h \left( \frac{q}{P}, \frac{I(\tilde{b} + q\tilde{y})}{P^2} \right) e(-\tilde{c} \cdot \tilde{y}) d\tilde{y}. \]

We perform the change of variable \( \tilde{y} = (\tilde{x} - \tilde{b})/q \), and our expression turns into

\[ P^{-2} \sum_{q=1}^{2TP} \sum_{\tilde{c} \in \mathbb{Z}^5} q^{-5} H_q(\tilde{c}na_t) S'_q(\tilde{c}), \]

where \( H_q(\tilde{c}) \) is defined as in Theorem 3.1.1 and
\[ S'_q(\tilde{c}) = \sum_{a \mod q^*} \sum_{b \mod q \atop b_1 \neq 0 \mod q} e_q(aI(\tilde{b}) + \tilde{c} \cdot \tilde{b}). \]

If \( \max_i \{|(na_t\tilde{c})_i|\} > P^n \), we use Lemma 3.1.4 and Lemma 3.1.6. These lemmas gives us an error term of \( O_\eta(1) \), as in the case \( t^2 < P^n \).

Otherwise, we have \( c_4 = c_5 = 0 \). In Section 3.5.3, we will prove the following lemma

**Lemma 3.5.1.** Let \( B_2 \) be the set of \( \tilde{c} \in \mathbb{Z}^5 \) with \( c_4 = c_5 = 0 \), \( 0 < |c_1| \leq t^4 P^n \), \( |c_2| \leq t^2 P^n \), and \( |c_3| \leq P^n \). Then

\[
P^{-2} \sum_{\tilde{c} \in B_2} \sum_{q = t^{-4} P}^{2tP} q^{-5} S'_q(\tilde{c}) H_q(cna_t) = O_\eta(P^{2+\eta t^4+\eta}).
\]

The terms with \( c_1 = c_4 = c_5 = 0 \) can be handled the same as in the Heath-Brown case, as there are only \( t^2 P^{2\eta} \) of them. So Expression (3.14) is

\[
P^{-2} \sum_{q = 1}^{t^{-4} P} \sum_{\tilde{c} \in B_2} q^{-5} H_q(cna_t) S'_q(\tilde{c}) + P^{-2} \sum_{q = 1}^{t^{-4} P} q^{-5} H_q(\tilde{0}) S'_q(\tilde{0}) + O(P^{5/2+\eta t^2+\eta}). \tag{3.16}
\]

### 3.5.2 The Expression 3.15

For Expression (3.15), the first coordinate of \( b + qy \) is at least \( q \). If \( q \gg t^{-4} P \), then \( P^{-1}(b + qy) \) is not in \( \text{supp}(\omega_{n,t}) \), so the contribution from these terms is 0.

Therefore we may assume \( q \leq Ct^{-4} P \) for some constant \( C \) that only depends on \( G_0L \). So Expression (3.15) is

\[
P^{-2} \sum_{q = 1}^{Ct^{-4} P} \sum_{a \mod q^*} \sum_{\tilde{b} \mod q \atop b_1 \equiv 0 \mod q} e_q(aI(\tilde{b})) \sum_{\substack{\tilde{y} \\ y_1 \neq 0}} \omega_{n,t} (P^{-1}(b + q\tilde{y})) h \left( \frac{q}{P}, \frac{I(\tilde{b} + q\tilde{y})}{P^2} \right). \]

Now we would like to add the terms with \( y_1 = 0 \) back in. We show that adding
these terms do not change the sum much. The terms with $y_1 = 0$ are

$$P^{-2} \sum_{q=1}^{Ct^{-4}P} \sum_{a \mod q} \sum_{\tilde{b} \in [0,q-1]^5_{b_1=0}} e_q(aI(\tilde{b})) \sum_{\tilde{y}_{y_1=0}} \omega_{n,t}(P^{-1}(\tilde{b} + q\tilde{y})) h \left( \frac{q}{P}, \frac{I(\tilde{b} + q\tilde{y})}{P^2} \right). \quad (3.17)$$

We treat the innermost sum like a function of 4 variables and perform Poisson summation. This gives us

$$\sum_{\tilde{c} \in \mathbb{Z}^4} \int_{\mathbb{R}^4} \omega_{n,t}(0, P^{-1}(\tilde{b} + q\tilde{y}')) h \left( \frac{q}{P}, \frac{I(0, \tilde{b} + q\tilde{y}'')}{P^2} \right) e\left(-P\tilde{c}.\tilde{y}'\right) d\tilde{y}'. \quad (3.18)$$

Here the first argument of $\omega$ and $I$ are fixed as 0, and the remaining 4 arguments come from the vector $\tilde{b} + q\tilde{y}$ projected onto its final 4 coordinates. For $x = (x_1, x_2, x_3, x_4, x_5)$, we use the notation $\tilde{x}' = (x_2, x_3, x_4, x_5)$. We make a change of variables to get that Expression (3.17) equals

$$P^{-2} \sum_{q=1}^{Ct^{-4}P} \sum_{\tilde{c} \in \mathbb{Z}^5_{c_1=0}} q^{-1} \tilde{S}_q(\tilde{c}) t^4 P^4 \int_{\mathbb{R}^4} \omega(0, \tilde{x}') h \left( \frac{q}{P}, -3x_2x_4 + x_3^2 \right) e_q((P\tilde{c}'(nax)^')d\tilde{x}', \quad (3.19)$$

where $\tilde{S}_q(\tilde{c}) = \sum_{a \mod q} \sum_{\tilde{b} \mod q} e_q(aI(\tilde{b}) + \tilde{b}.\tilde{c})$. Note that the change of variables gives us a factor of $t^4$ because that is the determinant of $a_t$ acting on the final four coordinates of $\mathbb{R}^5$.

We now consider the integral in Expression (3.19) as we have considered previous integrals. We note as usual the vectors $\tilde{c}$ with $\max_i \{(nax)_{c_i}\} > P^\eta$ contribute $O_\eta(1)$ by Lemma 3.1.4.

We fix $x_5$ and consider the integral as a function of 3 variables and apply the 3 variable case of Lemma 3.1.5. Since $x_5$ takes values in a compact set, we may make our bounds uniform over all possible values of $x_5$. This lemma allows us to say
Expression (3.19) is bounded by a constant times

\[ P^{3/2+\eta t^4} \sum_{q=1}^{Ct^{-4}P} \sum_{|c_2|<t^2 P^\eta} \sum_{|c_3|<P^\eta} q^{-7/2-2\eta} \tilde{S}_q(0, c_2, c_3, 0, 0)(\max\{t^{-2}|c_2|, |c_3|\})^{-1/2+\eta}. \]

Now we consider \( \tilde{S}_q(0, c_2, c_3, 0, 0) \). Since the summand fixes \( b_1 \) as 0, and \( c_5 \) is zero, \( \tilde{S}_q \) can be viewed as \( q \) times a singular series in 3 variables. We apply Lemma 3.1.7 to conclude that Expression 3.19 is \( O(\eta(P^{2+\eta t^4+\eta})) \).

So Expression (3.15) is

\[ P^{-2} \sum_{q=1}^{Ct^{-4}P} \sum_{a \mod q} \sum_{\vec{b} \mod q} e_q(aI(\vec{b})) \sum_{\vec{y} \in \mathbb{Z}^5} \omega_{n,t}(P^{-1}(\vec{b}+q\vec{y}))h\left(\frac{q}{P^2}, \frac{I(\vec{b}+q\vec{y})}{P^2}\right) + O(\eta(P^{2+\eta t^4+\eta})) \]

(3.20)

We apply Poisson summation to the main term above and get

\[ P^{-2} \sum_{q=1}^{Ct^{-4}P} \sum_{a \mod q} \sum_{\vec{b} \mod q} e_q(aI(\vec{b})) \sum_{\vec{c}} \int \omega_{n,t}(P^{-1}(\vec{b}+q\vec{y}))h\left(\frac{q}{P^2}, \frac{I(\vec{b}+q\vec{y})}{P^2}\right) e(\vec{c} \cdot \vec{y}) d\vec{y}. \]

Once again, for \( \vec{c} \) with \( \max_i\{|(na_t c)_i|\} > P^\eta \), we use Lemma 3.1.4 and 3.1.6. Recall that \( B_2 \) is the set of \( \vec{c} \) not satisfying this inequality and not equal to \( \vec{0} \). We now add the derived expressions for Expressions (3.14) and (3.15) to get that

\[ \sum_{\vec{x} \in \mathbb{Z}^5} \omega_{n,t}(x) = \sigma_\infty P^3 + P^{-2} \sum_{q=1}^{Ct^{-4}P} \sum_{\vec{c} \in B_2} q^{-5} S_q(\vec{c}) H_q(\vec{c}) + O(\eta(P^{2+\eta t^4+\eta})). \]

(3.21)

We can analyze the second term above by the same process as in Section 3.1.4 and derive that it is \( O(\eta(P^{2+\eta t^4+\eta})) \).
3.5.3 Proof of Lemma 3.5.1

Proof. We start by rearranging the terms of the singular series to take advantage of the fact that \( c_5 = 0 \). We have

\[
S'_q(\vec{c}) = \sum_{a \mod q^*} \sum_{b \mod q \atop b_1 \neq 0 \mod q} e_q(a(b_3^2 - 3b_2b_4) + c_1b_1 + c_2b_2 + c_3b_3) \sum_{b_5 \mod q} e_q(12ab_1b_5).
\]

The sum over \( b_5 \) is 0 unless \( 12ab_1 \equiv 0 \pmod{q} \). Since \( a \) is a unit \((\mod q)\), \( 12ab_1 \equiv 0 \pmod{q} \) only if \( 12b_1 \equiv 0 \pmod{q} \). Since \( b_1 \neq 0 \pmod{q} \), this can not happen if \( q \) is coprime to 12. So if \((q,12) = 1\), \( S'_q(\vec{c}) = 0 \).

Otherwise, let \( d = \gcd(12,q) > 1 \). The the values of \( b_1 \) where the innermost sum is non-zero are those with \( b_1/q = m/d \) for some \( m \) with \( 1 \leq m < d \), with \( m \) and \( d \) coprime.

In this case, \( e_q(b_1) \) is a \( d \)th root of unity. It is not 1 because \( b_1 \neq 0 \pmod{q} \). The variable \( b_1 \) takes on all \( d \) values between 1 and \( d - 1 \) inclusive. The innermost sum is equal to \( q \). We write

\[
S'_q(\vec{c}) = q \sum_{a \mod q^*} \sum_{b_2,b_3,b_4 \mod q} e_q(a(b_3^2 - 3b_2b_4) + c_2b_2 + c_3b_3) \sum_{m=1}^{d-1} e_d(mc_1)
\]

Now if we could simply sum \( S'_q(\vec{c}) \) over a range of \( d \) consecutive values of \( c_1 \), we would get zero. However the summand we consider in the lemma is \( H_q(\vec{c})S'_q(\vec{c}) \), so we must also account for the change of value of \( H_q(\vec{c}) \). Although there is a lot of notation in the proof of this lemma, the idea is simple. If we have 2 large numbers \( M_1 \) and \( M_2 \) which are approximately equal, then \( M_1 - M_2 \) is small. Similarly, if \( M_1 \) through \( M_{12} \) are 12 large numbers that are approximately equal, then \( \sum_{i=1}^{12} e_{12}(i)M_i \) is small. Let \( M_1 \) be the integral \( H_q((k+1,c_2,c_3,0,0)) \) for some \( k \), and \( M_i = H_q((k+i,c_2,c_3,0,0)) \). The \( M_i \) are approximately equal because the difference is that \( M_1 \) involves the integrand \( e_q(P(k+1)t^{-4}x) \) and \( M_i \) involves the integrand \( e_q(P(k+i)t^{-4}x) \),
and we have that $P/t^4q < 1$. The rest of this section makes this idea precise.

Let

$$S_q''(c_2, c_3) = \sum_{b_2, b_3, b_4 \mod q} e_q(a(b_3^2 - 3b_4b_2) + c_2b_2 + c_3b_3). \quad (3.22)$$

Fix some integer $k$, a multiple of $d$. Now

$$\sum_{c_1 = k}^{k+d-1} S_q'(\vec{c})H_q(\vec{c}na_t) = P^5qS_q''(c_2, c_3)\sum_{m=1}^{d-1} \sum_{c_1 = k}^{d-1} f_1(m, c_1, c_2, c_3), \quad (3.23)$$

where $f_1(m, c_1, c_2, c_3) =$

$$\int_{\mathbb{R}^5} \omega(\vec{x})h\left(\frac{q}{P}, I(\vec{x})\right)e_q(P((c_2, c_3) \cdot ((na_t\vec{x})_2, (na_t\vec{x})_3)))e_d(mc_1)e_q(P(c_1)(na_t\vec{x})_1)d\vec{x}. \quad (3.24)$$

Note that we have factored out the $c_1$ term from $e_q(Pc_1\vec{x})$.

Now we move the sum over $c_1$ inside the integral and consider

$$\sum_{c_1 = k}^{k+d-1} e_d(mc_1)e_q(P(c_1)(na_t\vec{x})_1). \quad (3.25)$$

First we note that $(na_t\vec{x})_1$ is $t^{-4}x_1$. Let $z = \frac{2\pi P x_1}{Pq}$. Since $P/(t^4q) < 1$ and the value of $|x_1|$ is bounded on supp$(\omega)$, $z \ll 1$ on supp$(\omega)$ Therefore we can define constants $s_N$ such that if $M = s_N \log P$, $\frac{e^m}{m!} = O_N(P^{-N})$ for $m > M$.

Now we use the Taylor series expansion of the exponential to write $e_q(Pc_1t^{-4}x_1) =

$$e_q(Pkt^{-4}x_1)e_q(P(c_1 - k)t^{-4}x_1) = e_q(Pkt^{-4}x_1)(1 + \sum_{l=1}^{M} \frac{z(c_1 - k)^l}{l!}) + O_N(P^{-N}). \quad (3.26)$$

So Expression (3.25) is equal to

$$e_q(Pkt^{-4}x_1)(\sum_{j=0}^{d-1} e_d(jm) + \sum_{j=0}^{d-1} e_d(jm) \sum_{l=1}^{M} \frac{(zj)^l}{l!}) + O_N(P^{-N}).$$
We have shown that Expression (3.23) is equal to

\[
P^5 q S''_q(c_2, c_3) \sum_{m=1}^{d-1} \sum_{j=0}^{d-1} c_d(m_j) f_2(j, k, c_2, c_3) + O_q(1),
\]

where \( f_2(j, k, c_2, c_3) = \)

\[
\sum_{l=1}^{M} \int_{\mathbb{R}^5} \omega(\vec{x}) h \left( \frac{q}{P}, I(\vec{x}) \right) e_q(P((k, \vec{c}').(na_t \vec{x}))(2\pi i P x_1 j / t^4 q)^l) / l! d\vec{x}.
\]

We will find it useful to to factor out a \( P/t^4 q \). Now we consider the weight \( \sum_{l=1}^{M} \omega(\vec{x})(2\pi i P x_1 j / t^4 q)^l) / l! \). Recall that \( (P/qt^4) < 1 \). Since \( |x_1| \) is bounded on \( \text{supp}(\omega) \), there is a maximum value to \( x_1^{l}/l! \), and so we can bound this weight by a constant times \( \omega(\vec{x}) \). The partial derivatives of \( \omega(\vec{x})(2\pi i P x_1 j / t^4 q)^l) / l! \) are also bounded by a constant times the partial derivatives of \( \omega \). We can therefore apply Lemma 3.1.5 to \( f_2(j, k, c_2, c_3) \). That bound gives us \( \sum c_1=k S''_q(\vec{c}) H_q(\vec{c}) \)

\[
\ll_{\eta} \frac{P}{t^4 q} S''_q(c_2, c_3) P^{7/2+\eta} q^{5/2-2\eta}(\max \{ |t^{-4} c_1|, |t^{-2} c_2|, |c_3| \} )^{-3/2+\eta}
\]

Since \( t^{-4} P/q < 1 \) and \( 0 < m < 12 \), \( \sum_{l=1}^{M} (t^{-4} P m/q)^l / l! \ll t^{-4} P/q \). Now we analyze

\[
P^{-2} \sum_{c \in B_2} \sum_{q=t^{-4} P}^{2TP} S'_q(\vec{c}) H_q(\vec{c}) q^{-5}
\]

\[
= P^{-2} \sum_{c_2, c_3 \in B_2} \sum_{l \in \mathbb{Z}}^{2TP} \sum_{q=t^{-4} P}^{ld+d-1} \sum_{c_1=l d} S'_q(c_1, c_2, c_3) H_q(\vec{c}) q^{-5}
\]

\[
\ll P^{5/2+\eta} t^{-4} \sum_{c_2, c_3 \in B_2} \sum_{l \in \mathbb{Z}}^{2TP} \sum_{q=t^{-4} P}^{\max \{ |t^{-4} dl|, |t^{-2} c_2|, |c_3| \} } S''_q(c_2, c_3) q^{-7/2-2\eta}(\max \{ |t^{-4} dl|, |t^{-2} c_2|, |c_3| \} )^{-3/2+\eta}
\]

(3.31)
We use Lemma 3.1.7 to conclude this expression is

\[
\ll P^{2} t^{-2} \sum_{c_2, c_3 \in B_2} \sum_{l \in \mathbb{Z}} (\max \{|t^{-4}ld|, |t^{-2}c_2|, |c_3|\})^{-3/2+\eta} \quad (3.32)
\]

\[
\ll P^{2+3\eta/2} t^{4+\eta}.
\]

\[\square\]
Chapter 4

The Mean Number of 2-Torsion Elements in the Class Groups of Pure Monogenic Cubic Fields

A pure cubic field over \( \mathbb{Q} \) is a field \( K \) which can be written as \( \mathbb{Q}(\sqrt[3]{d}) \) for some integer \( d \). A field \( K \) is called monogenic over \( \mathbb{Q} \) if its ring of integers \( \mathcal{O}_K \) can be written in the form \( \mathbb{Z}[\alpha] \) for some \( \alpha \in K \). We say a pure cubic field \( K \) is purely monogenic if its ring of integers is \( \mathbb{Z}[\sqrt[3]{d}] \) for some integer \( d \). In this chapter, we compute a bound on the average size of 2-torsion in purely monogenic cubic fields. We use the following theorem.

**Theorem 4.0.2** ([Woo, Bha3]). Suppose \( \mathbb{Z}[\sqrt[3]{d}] \) is the ring of integers of \( \mathbb{Q}(\sqrt[3]{d}) \). Then there is a canonical bijection between \( \text{GL}_2(\mathbb{Z}) \)-equivalence classes of integral binary quartic forms with \( I \)-invariant 0 and \( J \)-invariant \( 27d \) and elements of the 2-torsion subgroup of the class group of \( \mathbb{Q}(\sqrt[3]{d}) \). For a fixed \( J \), the reducible binary quartic forms form a single orbit, and under this bijection, this orbit corresponds to the identity element of the class group.
4.1 Computation of $p$-adic Densities for Purely Monogenic Cubic Fields

We recall the following theorem of Dedekind [Ded]

**Theorem 4.1.1.** Let $d = ab^2$, where $a$ and $b$ are coprime and square-free. Let $\alpha = \sqrt[3]{ab^2}$ and $\beta = \sqrt[3]{a^2b}$. Let $K = \mathbb{Q}(\sqrt[3]{d})$. Let $\mathcal{O}_K$ be the ring of integers in $K$ and let $D_K$ be the discriminant of $K$.

1. Suppose that $a^2 \not\equiv b^2 \pmod{9}$. Then $\mathcal{O}_K = \mathbb{Z}(1, \alpha, \beta)$ and $D_K = -27a^2b^2$.

2. Suppose $a^2 \equiv b^2 \pmod{9}$. Let $\gamma := 1 + a\alpha + b\beta$.

Then $\mathcal{O}_K = \mathbb{Z}(\alpha, \beta, \gamma)$ and $D_K = -3a^2b^2$.

We see therefore that $\mathbb{Z}[\sqrt[3]{d}]$ is the ring of integers in $\mathbb{Q}(\sqrt[3]{d})$ if and only if $d$ is square-free and $d \not\equiv 1, 8 \pmod{9}$. Since $J = 27d$, we have

**Lemma 4.1.2.** The binary quartic forms that correspond to maximal pure cubic rings are exactly those forms $f$ with $I(f) = 0$, $J(f)/27$ square-free, and $J(f)/27 \not\equiv 1, 8 \pmod{9}$.

Being square-free is a local condition, so for each prime $p$, we wish to restrict our count of the solutions to $I = 0$ to solutions with $J \not\equiv 0 \pmod{p^2}$. At $p = 3$ we have additional conditions. Recall that computations with the circle method involved computing the local densities $\sigma_p = \lim_{k \to \infty} p^{-4k} \#\{\bar{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 : I(\bar{x}) \equiv 0 \pmod{p^k}\}$. It follows easily from Heath-Brown’s proof that if we want to count $\bar{x}$ with $I(\bar{x}) = 0$ and $\bar{x} = \bar{a} \pmod{p^l}$, we replace $\sigma_p$ with $\sigma_p(\bar{a}) = \lim_{k \to \infty} p^{-4k} \#\{\bar{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 : I(\bar{x}) \equiv 0 \pmod{p^k}, \bar{x} \equiv \bar{a} \pmod{p^l}\}$. It is also the case that if we wish
to impose conditions on $\vec{x}$ at finitely many primes, we may consider each prime separately. The rest of the section consists of computing

$$\sum_{\vec{a} \pmod{p^2}} \sigma_p(a), \quad (4.1)$$

for each prime $p$.

### 4.1.1 Binary Quartic Forms with $p^2 \mid J$, $p \neq 2, 3$

We count here the number of solutions in $(\mathbb{Z}/p^2\mathbb{Z})^5$ to $I \equiv 0$, $J \not\equiv 0 \pmod{p^2}$. We deduce from Section 2.4.2 that the total number of solutions to $I \equiv 0 \pmod{p^2}$ in $(\mathbb{Z}/p^2\mathbb{Z})^5$ is $p^8 + p^5 - p^4$. We will count here the number of solutions to $I \equiv J \equiv 0 \pmod{p^2}$.

First we count the solutions with $a \not\equiv 0 \pmod{p}$. In this case, $I \equiv 0$ implies $e \equiv \frac{3bd-c^2}{12a}$. We substitute this expression for $e$ into $J$ and get $J \equiv 27cbd - 8c^3 - 27ad^2 - \frac{27b^3d}{4a} + \frac{9b^2c^2}{4a}$. We are going to complete the square for $d$. We divide by $-27a$ and now we have

$$(-27a)^{-1}J \equiv (d + \frac{b^3}{8a^2} - \frac{bc}{2a})^2 - \frac{b^6}{64a^4} + \frac{b^4c}{8a^3} - \frac{b^2c^2}{3a^2} + \frac{8c^3}{27a}.$$  

We make the change of variables $d \to d - \frac{b^3}{8a^2} + \frac{bc}{2a}$ and get

$$(-27a)^{-1}J \equiv d^2 - \frac{1}{64 \cdot 27 \cdot a^4} (3b^2 - 8ac)^3.$$  

For $a \not\equiv 0$, $3b^2 - 8ac$ represents every non-zero element $\pmod{p}$ $p^2 - p$ times. The expression $\frac{(3b^2 - 8ac)^3}{64 \cdot 27 \cdot a^4}$ will be a square the same number of times that $3b^2 - 8ac$ is, so there are $(p^2 - p) \cdot (p - 1)/2$ choices of $a, b, c$ that make $\frac{1}{64 \cdot 27 \cdot a^4} (3b^2 - 8ac)^3$ a square $\pmod{p}$. Then there are 2 choices for $d$, and $e$ is uniquely determined. So we have
a total of $p(p-1)^2$ solutions $\pmod{p}$ with $a \not\equiv 0$, $3b^2 - 8ac \not\equiv 0 \pmod{p}$. For each of these choices, $d$ is non-zero, so for any lift of $a, b$ and $c \pmod{p^2}$, there are two choices of $d$ and $e$ is uniquely determined by Hensel’s Lemma. Therefore there are $p^4(p-1)^2$ solutions to $I \equiv J \equiv 0 \pmod{p^2}$ with $a \not\equiv 0$ and $3b^2 - 8ac \not\equiv 0 \pmod{p}$.

Now suppose $a \not\equiv 0 \pmod{p}$ and $3b^2 - 8ac \equiv 0 \pmod{p}$. There are $p^2 - p$ choices for $a, b, c \pmod{p}$ that fit these criteria. Any lift of these $\pmod{p^2}$ will result in $(3b^2 - 8ac)^3$ being $0 \pmod{p^2}$, for a total of $p^5 - p^4$ choices of $a, b$ and $c \pmod{p^2}$. Then $J \equiv 0$ requires that $d \equiv 0 \pmod{p}$, so there are $p$ choices for $d$. Then $e$ is uniquely determined, for a total of $p^6 - p^5$ solutions to $I \equiv J \equiv 0 \pmod{p^2}$ with $a \not\equiv 0 \pmod{p}$ and $3b^2 - 8ac \equiv 0 \pmod{p}$.

There remain the solutions with $a \equiv 0 \pmod{p}$. We start by assuming $b \not\equiv 0 \pmod{p}$. We have $I \equiv 3bd - c^2 \pmod{p}$, so $d \equiv \frac{c^2}{3b}$, and $J \equiv c^3 - 27eb^2$. If $p \equiv 2 \pmod{3}$, then cubing is a bijection $\pmod{p}$, so any choice of $e$ and $b$ gives a unique choice of $c$. If $p \equiv 1 \pmod{3}$, then we need $e$ and $b$ to be in the same cubic residue class for $J \equiv 0 \pmod{p}$ to be solvable, and each such pair $e, b$ gives 3 values for $c$. In either case, there are $p^2 - p$ values of $b, c$ and $e \pmod{p}$ with $b \not\equiv 0 \pmod{p}$. The partial derivative of $J$ with respect to $e$ is non-zero in this case, so for any lift of $a, b$ and $c$, we have $d$ and $e$ are uniquely determined. This gives us $p^5 - p^4$ solutions to $I \equiv J \equiv 0 \pmod{p^2}$ with $a \equiv 0 \pmod{p}, b \not\equiv 0 \pmod{p}$.

So assume $a \equiv b \equiv 0 \pmod{p}$. Then for $I \equiv 0 \pmod{p}$, we must have $c \equiv 0 \pmod{p}$ as well. So we have $I \equiv 12ae - 3bd \pmod{p^2}$ and $J \equiv 27ad^2 \pmod{p^2}$. Suppose $a \not\equiv 0 \pmod{p^2}$. Then for $J \equiv 0 \pmod{p^2}$ we must have $d \equiv 0 \pmod{p}$, and then for $I \equiv 0 \pmod{p^2}$ we must have $e \equiv 0 \pmod{p}$. This gives $p^5 - p^4$ solutions $\pmod{p^2}$ with $a \equiv 0 \pmod{p}$ and $a \not\equiv 0 \pmod{p^2}$. Finally, suppose $a \equiv 0 \pmod{p^2}$ and $b \equiv 0 \pmod{p}$. Then $I \equiv -3bd \pmod{p^2}$ and $J$ is identically $0$. So either $b \equiv 0 \pmod{p^2}$ and $d$ is arbitrary, or $b \not\equiv 0 \pmod{p^2}$ and $d \equiv 0 \pmod{p}$. This gives $2p^5 - p^4$ solutions to $I \equiv J \equiv 0 \pmod{p^2}$ with $a \equiv 0 \pmod{p^2}$ and $b \equiv 0 \pmod{p}$. 41
In total we have \(2p^6 + p^5 - 2p^4\) solutions to \(I \equiv J \equiv 0 \pmod{p^2}\). The number of solutions of \(I \equiv 0 \pmod{p^2}\) is \(p^8 + p^5 - p^4\). The solutions with \(J \equiv 0\) include all the solutions where all 5 coefficients are 0 (mod \(p\)). This means that all solutions with \(I \equiv 0 \pmod{p^2}\) and \(J \not\equiv 0 \pmod{p^2}\) are non-singular, so we can easily compute 

\[
\sigma_p(J \not\equiv 0 \pmod{p^2}) = \left(1 - \frac{1}{p^2}\right)^2.
\]

### 4.1.2 Binary Quartic Forms with \(4 \nmid J\)

We can count by computer all 144 solutions to \(I \equiv 0 \pmod{4}\), \(J \not\equiv 0 \pmod{4}\). For all of these solutions, at least one of the partial derivatives is odd, so they are all non-singular. Therefore 

\[
\sigma_2(J \not\equiv 0 \pmod{4}) = \frac{144}{2^8} = \frac{9}{16}.
\]

### 4.1.3 Binary Quartic Forms with \(J/27 \not\equiv 0, 1, 8 \pmod{9}\)

Since \(I \equiv c^2 \pmod{3}\), any solutions to \(I = 0 \pmod{3^k}\) must have \(c \equiv 0 \pmod{3}\). Write \(c = 3c'\). Then \(J/27 = 8ac'e + bc'd - ad^2 - eb^2 - 2(c')^3\), and since we only need to know \(J/27 \pmod{9}\), it suffices to count solutions to \(I \equiv 0 \pmod{27}\), \(J \not\equiv 0 \pmod{9}\) with the coefficients in \(\mathbb{Z}/27\mathbb{Z}\). We count by computer that there are 3\(^{12} - 3^{11} - 3^{10} + 3^9\) such quintuplets. The computer list also shows that for all these solutions, at least one coefficient is \(\not\equiv 0 \pmod{3}\), so every solution is non-singular. Therefore 

\[
\sigma_3(J/27 \not\equiv 0, 1, 8 \pmod{9}) = \frac{16}{27}.
\]

### 4.2 The Bound on The Average Size of 2-Torsion In Pure Monogenic Cubic Fields

Let \(U\) denote the set of cubic rings of the form \(\mathbb{Z}[\sqrt[3]{d}]\) with \(d\) cube-free and let \(U(U)\) denote the elements of \(U\) which are the ring of integers inside their field of fractions. By Dedekind’s Theorem [Ded], we see that the discriminant of an element \(\mathbb{Z}[\sqrt[3]{d}]\) of
\( \mathcal{U}(U) \) is \(-27d^2\). Let \( N(\mathcal{U}(U); X) \) be the number of elements of \( \mathcal{U}(U) \) with absolute discriminant less than \( X \).

To begin with, we need

**Lemma 4.2.1.** The number of pure monogenic cubic rings \( \mathbb{Z}[\sqrt[3]{d}] \) that are non-maximal at \( p \) with \(|-27d^2| < X \) is \( O(X^{1/2}/p^2) \), where the implied constant is independent of \( p \).

This lemma follows easily from Dedekind’s theorem. Now we have the following count.

**Proposition 4.2.2.** We have

\[
\lim_{X \to \infty} \frac{N(\mathcal{U}(U); X)}{X^{1/2}} = \frac{1}{36\zeta(2)}.
\]

**Proof.** Let \( \mathcal{U}_p(U) \) be the subset of elements of \( U_{\mathbb{Z},1} \) that are maximal at \( p \). Because a pure cubic ring \( \mathbb{Z}[\sqrt[3]{d}] \) is maximal if and only if \( d \) is square-free, and \( d \not\equiv 1, 8 \mod 9 \), we have, for \( M \) with \( M > 3 \),

\[
\lim_{X \to \infty} \frac{N(\cap_{p<M} \mathcal{U}_p(U); X)}{X^{1/2}} = \frac{1}{27} \prod_{p<M} \left( 1 - \frac{1}{p^2} \right) \left( \frac{9}{8} \right) \left( \frac{2}{3} \right).
\]

Letting \( M \to \infty \), we have

\[
\lim \sup_{X \to \infty} \frac{N(\mathcal{U}(U); X)}{X^{1/2}} = \frac{1}{36\zeta(2)}.
\]

By the uniformity estimate of Lemma 4.2.1, we have, for any fixed \( M > 3 \),

\[
\lim_{X \to \infty} \frac{N(\mathcal{U}(U); X)}{X^{1/2}} \geq \frac{1}{36} \prod_{p<M} \left( 1 - \frac{1}{p^2} \right) + O(\sum_{p>M} p^{-2}).
\]

Letting \( M \) tend to infinity completes the proof. \( \square \)
If we had a uniformity estimate for binary quartic forms, we could use the count of Section 4.1 to similarly count the number of irreducible binary quartic forms that correspond to maximal cubic rings. Without the uniformity estimate, we can still get an upper bound.

Recall that $Y$ is the set of integral binary quartic forms with $I = 0$ and $0 < |J| < X$. Let $\mathcal{V}(Y)$ be the subset of elements of $Y$ that correspond to maximal cubic rings, and $N(\mathcal{V}(Y); X)$ the number of $\text{GL}_2(\mathbb{Z})$-equivalence classes of elements of $\mathcal{V}(Y)$ with $0 < J < X$. Note that since $\mathbb{Z}[\sqrt[3]{d}] = \mathbb{Z}[\sqrt[3]{-d}]$, we count only the $\text{GL}_2(\mathbb{Z})$-equivalence classes of elements of $\mathcal{V}(Y)$ with $J > 0$.

**Proposition 4.2.3.** We have

$$\lim_{X \to \infty} \frac{N(\mathcal{V}(Y); X)}{X} \leq \frac{1}{36\zeta(2)}.$$  

**Proof.** Let $\mathcal{V}_p(Y)$ be the subset of elements of $Y$ that correspond to maximal cubic rings at $p$. Because an element of $V$ corresponds to a maximal cubic ring if and only if $J/27$ is square-free at all $p$ and $J/27 \not\equiv 0, 1, 8 \pmod{9}$, we have for all $M > 3$

$$\lim_{X \to \infty} \frac{N(\cap_{p < M} \mathcal{V}_p(Y); X)}{X^{1/2}} = \frac{\zeta(2)}{27} \prod_{p < M} \left(1 - \frac{1}{p^2}\right)^2 \left(\frac{9}{8}\right)^2 \left(\frac{16}{27}\right).$$

Letting $M \to \infty$, we have

$$\limsup_{X \to \infty} \frac{N(\mathcal{V}(V); X)}{X^2} = \frac{1}{36\zeta(2)}.$$

Combining these two results, we prove Theorem 1.1.5.
Proof. We have
\[
\lim_{x \to \infty} \frac{\sum_{d < x} \text{Cl}_2(K)}{\sum_{\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]} 1} \leq 1 + \lim_{x \to \infty} \frac{N(\mathcal{V}(Y); X)}{N(U(U); X^2)} = 2
\]

\[\square\]

4.3 Proof of Lemma 2.2.3

We need the following theorem.

Theorem 4.3.1 ([Woo]). There is a canonical bijection between \(\text{GL}_2(\mathbb{Z})\)-equivalence classes of integral binary quartic forms and isomorphism classes of pairs \((Q, C)\), where \(Q\) is a quartic ring over \(\mathbb{Z}\) and \(C\) is a monogenized cubic resolvent ring of \(Q\).

For more details see [Woo] and [Bha3].

Now we may prove the lemma.

Proof. Suppose an integral binary quartic form \(f\) has a stabilizer of size 2 in \(\text{PGL}_2(\mathbb{Z})\), and let \((Q, C)\) be the corresponding pair of rings. Then \(Q\) has a non-trivial automorphism over \(\mathbb{Z}\) and therefore can not be an order in an \(A_4\) or \(S_4\) field. If \(Q\) is an order in a \(D_4\), \(C_4\), or \(V_4\) quartic field, or is a quartic ring lying in a direct sum of two quadratic \(\mathbb{Q}\)-algebras, then the cubic resolvent ring \(C\) of \(Q\) cannot be an integral domain. If \(\mathbb{Z}[\sqrt[3]{d}]\) is not an integral domain, then \(d\) must be a cube. From [BhaSha, Lemma 3.21], we know that the number of quartic rings having resolvent \(\mathbb{Z}[\sqrt[3]{d}]\) is \(O(d^{\frac{3}{2}})\). Therefore the number of quartic rings with cubic resolvents that are pure and reducible is \(O(\sum_{d = n^3} d^{\frac{1}{2}}) = O(X^{\frac{5}{6}})\).

Now, by the proof of Lemma 2.4 in [BhaSha], the only remaining possibility for \(Q\) is that it is a quartic ring in an etale quartic \(\mathbb{Q}\)-algebra of the form \(F = \mathbb{Q} \oplus K\), where
$K$ is a cubic field. Furthermore, the cubic resolvent of $\mathbb{Q} \oplus K$ is $K$, and $K$ must be an $A_3$ extension. Since all pure cubic fields are $S_3$ extensions, there are no such $Q$ with pure monogenic cubic resolvents.
Chapter 5

The Selmer Group

5.1 Connection with Binary Quartic Forms

Theorem 5.1.1. Let \( E \) be a fixed elliptic curve over \( \mathbb{Q} \) written in the form \( y^2 = x^3 + Ax + B \), where \( p^6 \nmid B \) if \( p^4 \mid A \). We define \( I(E) = -3A \) and \( J(E) = -27B \). Then elements of the 2-Selmer group of \( E \) are in one-to-one correspondence with \( \text{PGL}_2(\mathbb{Q}) \)-equivalence classes of locally soluble integral binary quartic forms having invariants equal to \( 2^4 I \) and \( 2^6 J \).

In this chapter we wish to count each \( \text{PGL}_2(\mathbb{Z}) \)-orbit of binary quartic forms with \( I = 0 \) and fixed non-zero \( J \)-invariant, weighed by \( \frac{1}{m(f)} \), where \( n(f) \) is the number of \( \text{PGL}_2(\mathbb{Z}) \)-equivalence classes inside the \( \text{PGL}_2(\mathbb{Q}) \)-equivalence class of \( f \). We instead weigh the orbits by \( \frac{1}{m(f)} \), where \( m(f) = n(f) \frac{\#\text{Aut}_Q(f)}{\#\text{Aut}_Z(f)} \). \( \text{Aut}_Q(f) \) is the stabilizer subgroup of \( f \) inside \( \text{PGL}_2(\mathbb{Q}) \), and \( \text{Aut}_Z(f) \) is the stabilizer subgroup of \( f \) inside \( \text{PGL}_2(\mathbb{Z}) \). We can use \( m(f) \) because, by the proof of Lemma 2.2.3, the number of forms where \( n_f \neq m_f \) is small relative to the total number of forms.

For a prime \( p \), define \( n_p \) and \( m_p \) as above, with \( \mathbb{Q} \) replaced by \( \mathbb{Q}_p \) and \( \mathbb{Z} \) replaced by \( \mathbb{Z}_p \). Proposition 5.12 in Bhargava-Shankar states
Proposition 5.1.2. Suppose \( f \) has non-zero discriminant. Then \( m(f) = \prod_{p \text{ prime}} m_p(f) \).

Let \( Y_{\mathbb{Z}_p} \) be the set of binary quartic forms over \( \mathbb{Z}_p \) that lie on the quadric \( I = 0 \).

To compute the average value of \( m_p(f) \) over all \( \text{PGL}_2(\mathbb{Z}) \)-equivalence classes with \( I \)-invariant 0 and \( 0 < |J| < X \), we view \( Y_{\mathbb{Z}_p} \) as a homogenous space and view the average as an integral over the acting group. We now develop this idea.

5.2 The Counting Measure

Fix a prime \( p \) and a positive integer \( d \). Let \( A_{p,d} = \{ x \in Y_{\mathbb{Z}_p} | m_p(x) = d \} \). We wish to compute

\[
\sum_{d=1}^{\infty} \left( \text{proportion of } Y_{\mathbb{Z}_p} \text{ in } A_{p,d} \right) \frac{1}{d}.
\] (5.1)

We introduce a measure to do this. For a set \( A \subset Y_{\mathbb{Z}_p} \), let \( A' \) be its pullback to \( Y \) under the inclusion map \( \mathbb{Z} \to \mathbb{Z}_p \). Then we have a measure \( \mu_p \) on \( Y_{\mathbb{Z}_p} \) defined by

\[
\mu_p(A) = \lim_{X \to \infty} \frac{\# \{ x \in A' \cap \mathcal{F}G_0L : 0 < |J(x)| < X \}}{\# \{ x \in Y \cap \mathcal{F}G_0L : 0 < |J(x)| < X \}},
\]

whenever this limit exists. This limit is defined for any \( A \) defined by congruence conditions. We see then that Expression (5.1) is equal to \( \sum_{d=1}^{\infty} \mu_p(A_{p,d}) \frac{1}{d} \).

5.3 \( Y \) as a Homogenous Space for the Orthogonal Group

For this section, let \( H = \text{SO}(I) \). Then \( H \) acts on the variety \( S \) defined by \( I = 0 \), so if we fix a point \( v \in S \), we get a map \( H \to S \). Furthermore, \( H \) acts transitively, so if \( P \) is the stabilizer of \( v \), we have \( H/P = S \). This isomorphism gives a Haar measure on \( S \), which we describe now.
For the sake of concreteness, let \( v = (0, 1, 0, 0, 1)^T \). This point corresponds to the quartic form \( x^3 y + y^4 \), which has \( I \)-invariant equal to 0 and \( J \)-invariant equal to \(-27\).

The Lie algebra \( \mathfrak{h} \) of \( H \) is a linear subspace of \( \mathfrak{gl}_n \). With \( \mathfrak{a}' \) equal to diagonal matrices and the standard ordering of the roots of \( \mathfrak{gl}_n \), let \( \mathfrak{n}' \) and \( \mathfrak{n} \) be the subspaces of \( \mathfrak{gl}_n \) corresponding to the positive roots and negative roots respectively. Then let \( \mathfrak{n} = \mathfrak{n}' \cap \mathfrak{h} \), \( \mathfrak{a} = \mathfrak{a}' \cap \mathfrak{h} \), and \( \mathfrak{n} = \mathfrak{n}' \cap \mathfrak{h} \). By decomposing the Lie algebra \( \mathfrak{h} \) of \( H \) as \( \mathfrak{n} \oplus \mathfrak{a} \oplus \mathfrak{n} \) we get a \( \overline{\mathfrak{n}} \mathfrak{A} \mathfrak{n} \) decomposition of \( H \), which parametrizes a full measure set of \( H^0 \), the connected component of the identity of \( H \).

We have

\[
\overline{N} = \begin{pmatrix}
1 & y_4 & y_3 & y_2 & 4y_2y_4 - 3y_3^2 \\
0 & 1 & 2y_6 & 3y_6^2 & 4y_2 - 12y_6y_3 + 12y_4y_6^2 \\
0 & 0 & 1 & 3y_6 & -6y_3 + 12y_4y_6 \\
0 & 0 & 0 & 1 & 4y_4 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix},
\]
\[
A = \begin{pmatrix}
s^{-1} & 0 & 0 & 0 & 0 \\
0 & t^{-1} & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & t & 0 \\
0 & 0 & 0 & 0 & s
\end{pmatrix}, \text{ and}
\]
\[
N = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
4b_1 & 1 & 0 & 0 & 0 \\
-6b_3 + 12b_1b_2 & 3b_2 & 1 & 0 & 0 \\
4b_4 - 12b_2b_3 + 12b_1b_2^2 & 3b_2^2 & 2b_2 & 1 & 0 \\
4b_4b_1 - 3b_3^2 & b_4 & b_3 & b_1 & 1
\end{pmatrix},
\]

for a set of 10 parameters \( y_i, b_i, s \) and \( t \).

Now we want a set of coset representatives of \( H/P \). First we will describe \( P \). For
the vector \( v_0 = y^4 \), the stabilizer \( P_0 \) of \( v_0 \) in the above coordinates is \( y_2 = y_3 = y_4 = 0 \) and \( s = 1 \). Therefore, letting \( y_2, y_3, y_4 \) and \( s \) vary, with \( s \neq 0 \), while the other 6 parameters are fixed gives us a complete set of coset representatives for \( H/P_0 \). Now if we take a \( g \in H \) with \( gv_0 = v \), then \( P = gP_0g^{-1} \). By doing this computation, we find the above parameterization is still a complete set of representatives. We perform a change of variables and get the parametrization

\[
H/P = \begin{cases}
\begin{pmatrix}
s^{-1} & y_4 & -y_3 & y_2 & \frac{3y_2y_4 - y_3^2}{12s} \\
0 & 1 & 0 & 0 & y_2 \\
0 & 0 & 1 & 0 & y_3 \\
0 & 0 & 0 & 1 & y_4 \\
0 & 0 & 0 & 0 & s
\end{pmatrix}, \ s \neq 0
\end{cases}
\]

We see that a Haar measure on the space is given by \( dy_2dy_3dy_4ds \). Call this measure \( \nu_p \).

We define the integer points \( (H/P)(\mathbb{Z}_p) \) to be the elements \( h \in H/P \) such that \( hv \) is a \( \mathbb{Z}_p \)-binary quartic form. Write \( hv = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \). In this notation, \( b, c, d \) and \( e \) are elements of \( \mathbb{Z}_p \) if and only if \( s, y_4, y_3 \) and \( y_2 \) are elements of \( \mathbb{Z}_p \). The remaining coefficient \( a \) is equal to \( \frac{3y_4 + 3y_2y_4 - y_3^2}{12s} \). Since \( H \) acts transitively on \( Y_{\mathbb{Z}_p} \), we see that \( Y_{\mathbb{Z}_p} \) is in one-to-one correspondence with the set of \( s, y_2, y_3, y_4 \) which are all in \( \mathbb{Z}_p \) and such that \( 12s \) divides \( 3y_4 + 3y_2y_4 - y_3^2 \) in \( \mathbb{Z}_p \).

We can use this parametrization to count the proportion of \( v \in \mathbb{Z}_p \) in \( A_{p,d} \) for a positive integer \( d \) if we find the constant \( c_p \) such that \( c_p\nu_p(H/P(\mathbb{Z}_p)) = 1 \). We perform the change of variable \( y_2 \to y_2 - 1 \). Now we wish to compute the \( \nu_p \)-measure of points where \( 3y_2y_4 - y_3^2 \) is divisible by \( 12s \) in \( \mathbb{Z}_p \).
5.3.1 \( p \neq 2, 3 \)

Since \( p \neq 3 \), we may replace \( y_4 \) by \( y_4 / 3 \). Suppose \( |s|_p = p^i \). Then the condition \( 12s \) divides \( y_2 y_4 - y_3^2 \) is a restriction on the values of \( y_2, y_3 \) and \( y_4 \pmod{p^i} \). The \( \nu \)-volume then of such points with \( |s|_p = p^i \) is \( \left( 1 - \frac{1}{p} \right) \left( p^{-3i} \# \{ y_2, y_3, y_4 \pmod{p^i} \} \mid y_2 y_4 - y_3^2 \equiv 0 \pmod{p^i} \} \). Note that the volume of \( p^i \mathbb{Z}_p \) is \( (1 - 1/p) \) with respect to the multiplicative Haar measure.

The \( \nu \)-volume of \( H/P(\mathbb{Z}_p) \) is thus

\[
\left( 1 - \frac{1}{p} \right) \left( 1 + \sum_{i=1}^{\infty} p^{-3i} \# \{ y_2, y_3, y_4 \pmod{p^i} \} \mid y_2 y_4 - y_3^2 \equiv 0 \pmod{p^i} \} \right). \tag{5.2}
\]

We denote by \( Q(y_2, y_3, y_4) \) the quadratic form \( y_2 y_4 - y_3^2 \). We see that \( Q \) has \( p^2 \) solutions \( \pmod{p} \) and \( p^4 - p^2 + p^3 \) solutions \( \pmod{p^2} \). If we denote by \( N(p; k) \) the number of zeros of \( Q \pmod{p^k} \), then by a similar process to Section 2.4.2, we get the recurrence relation \( N(p; k) = p^{2k} - p^{2k-1} + p^3 N(p; k-2) \). This relation allows us to compute that Expression (5.2) is \( \sigma_p(I) \), where \( \sigma_p \) is as in Proposition 2.3.1.

5.3.2 \( p = 2 \) or \( p = 3 \)

We are trying to compute normalization constants, that is, constants \( c_p \), such that for any \( n \) and any set \( A \) specified by congruence conditions \( \pmod{p^n} \), we have

\[
\lim_{k \to \infty} \frac{\# \{ \overline{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 \mid I(\overline{x}) \equiv 0 \pmod{p^k}, \overline{x} \in A \}}{\# \{ \overline{x} \in (\mathbb{Z}/p^k\mathbb{Z})^5 \mid I(\overline{x}) \equiv 0 \pmod{p^k} \}} = c_p \nu(g \in H/P(\mathbb{Z}_p) \mid g.\overline{v} \in A). \tag{5.3}
\]

where \( \nu \) is Haar measure. We can therefore choose an \( A \) where the cardinalities and the Haar measure are easy to compute. Note that for all other primes, we were letting \( A \) equal \( Y_{\mathbb{Z}_p} \).

For \( p = 2 \) we let \( A \) equal elements of \( \mathbb{Z}_2^5 \) where every coordinate is odd. Then
from Section 2.4.2 we see that $2^{-4k} \# \{ \vec{x} \in (\mathbb{Z}/2^k \mathbb{Z})^5 | I(\vec{x}) \equiv 0 \pmod{2^k}, \vec{x} \in A \} = \frac{1}{16}$, while the limit of $2^{-4k}$ times the denominator of the left side of Expression (5.3) is $\sigma_2$. The Haar measure on the right side of Equation (5.3) is equal to the volume in $\mathbb{Z}_2^3$ of odd $y_2, y_3, y_4$ with $3y_2y_4 - y^3$ divisible by 4 times the volume of odd $s$. Since the $y_i$ are all odd, we have $y_1 = y_2^2/3y_4$ (mod 4), which has a density of $\frac{1}{16}$. Odd $s$ have density $\frac{1}{2}$, so the Haar measure of our set is $\frac{1}{32}$. Therefore $c_2 = \frac{2}{\sigma_2}$.

For $p = 3$, let $A$ be the subset of elements of $\mathbb{Z}_3^5$ where the 5th coordinate is not divisible by 3. The limit of $3^{-4k}$ times the denominator of Expression (5.3) is equal to $\sigma_3$, while $3^{-4k}$ times the numerator is equal to $\frac{2}{3}$, again by Section 2.4.2. (Note that in Section 2.4.2 we counted the density of solutions where the first coordinate was not divisible by 3, but the first and fifth coordinate are symmetric in the quadratic form $I$). The Haar measure on the right side is equal to $1 - \frac{1}{3}$ times the density of $y_2, y_3, y_4$ such that $3y_2y_4 - y_3^2 \equiv 0 \pmod{3}$. We see that $y_3 \equiv 0 \pmod{3}$ while the other two variables are arbitrary, so the Haar measure of this set is $\frac{2}{9}$. Therefore $c_3 = \frac{3}{\sigma_3}$.

5.4 Comparing Measures

We have a Haar measure for $\text{SL}_2(\mathbb{C})$ by taking the $NAN$ decomposition of this group. That is, for $g$ in a set of full measure in $\text{SL}_2(\mathbb{C})$, we write

$$g = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}.$$ 

A Haar measure is then given by $t^{-2} d^* t d u d v$. We let these matrices act on the right on a vector in $\mathbb{C}^2$ and therefore on the left on the space of binary quartic forms. We take the action of this product of matrices on the binary quartic form $x^3 y - \frac{J}{27} y^4$.

This action gives us some binary quartic form. We then find the corresponding element of $H/P$. In this way, we get a map $\phi$ from $(u, t, v, J)$-coordinates to
Taking the Jacobian of this map allows us to compare integration over the two spaces, and we find, for a compactly supported continuous function \( f \),

\[
\int_{\mathbb{C}^3} \int_{\mathbb{C}^*} f(y_2, y_3, y_4, s) d^* s dy_2 dy_3 dy_4 = 12 \int_{\mathbb{C}^3} \int_{\mathbb{C}^*} f(\phi(u, t, v, J)) t^{-2} d^* t du dv dJ.
\]

### 5.5 Local Densities

Recall that we let \( Y \) denote the set of integral binary quartic forms with \( I \)-invariant 0. Let \( Y^{\text{inv}} = \{ J(E) | E \in Y \} \). Let the \( p \)-adic closure of \( Y^{\text{inv}} \) in \( \mathbb{Z}_p \) be denoted \( Y^{\text{inv}}_p \). Let \( T(Y^{\text{inv}}) \) denote the set of all locally soluble integral binary quartic forms having invariants \( I = 0 \) and \( 2^6 J \) with \( J \in F^{\text{inv}} \), and let \( T_p(Y^{\text{inv}}) \) denote the \( p \)-adic closure of \( T(Y^{\text{inv}}) \) in \( \mathbb{Z}_p \). For \( J \neq 0 \), let \( E_J \) be the elliptic curve \( y^2 = x^3 - J/27 \).

**Theorem 5.5.1.** Let \( A_p(k) = \{ f \in T_p(F^{\text{inv}}) | m_p(f) = k \} \). We have

\[
\sum_{k=1}^{\infty} \frac{\mu_p(A_p(k))}{k} = \frac{[2^6]_p}{\sigma_p} M_p(Y)
\]

where

\[
M_p(Y) = \left( 1 - \frac{1}{p^2} \right) \int_{J \in Y^{\text{inv}}_p} \sum_{\sigma \in E_J(Q_p) / 2E_J(Q_p)} \frac{1}{\#E_J[2](Q_p)} dJ.
\]

**Proof.** Let \( S_p(J) \subset Y_{\mathbb{Z}_p} \) be a set consisting of one element in each soluble \( \text{PGL}_2(\mathbb{Z}_p) \)-orbit on the elements in \( Y_{\mathbb{Z}_p} \) having invariant equal to \( 2^6 J \). Define the multiset \( \tilde{S}_p(F^{\text{inv}}) \) by

\[
\tilde{S}_p(F^{\text{inv}}) := \bigcup_{J \in Y^{\text{inv}}_p} \text{PGL}_2(\mathbb{Z}_p) \cdot f.
\]
Now we have
\[
\sum_{k=1}^{\infty} \mu_p(\{f \in T_p(Y^{inv}) | m_p(f) = k\}) \cdot \frac{1}{k}
= \sum_{k=1}^{\infty} \mu_p(\{f \in S_p(Y^{inv}) | m_p(f) \# \text{Aut}_{\mathbb{Z}_p}(f) = k\}) \cdot \frac{1}{k}
= \sum_{k=1}^{\infty} \mu_p(\{f \in S_p(Y^{inv}) | n_p(f) \# \text{Aut}_{\mathbb{Q}_p}(f) = k\}) \cdot \frac{1}{k}.
\]

Now, by the change of variables discussed in Subsections 5.2 and 5.4, we have
\[
\sum_{k=1}^{\infty} \mu_p(\{f \in S_p(Y^{inv}) | n_p(f) \# \text{Aut}_{\mathbb{Q}_p}(f) = k\}) \cdot \frac{1}{k} = \left|\frac{2^7}{\sigma_p}\right| \cdot \text{Vol}(\text{PGL}_2(\mathbb{Z}_p)) \cdot \int_{J \in F^{inv}_p} \sum_{f \in B_p(J)} \frac{1}{n_p(f) \# \text{Aut}_{\mathbb{Q}_p}(f)}.
\]

Note that we have the factor \(2^7 \cdot \sigma_p\) instead of \(2\sigma_p\) because \(f \in B_p(J)\) has invariant \(2^6(J)\) as opposed to \(J\). Lemmas 5.3, 5.4, and 5.5 of [BhaSha] imply that if \(f\) is a locally soluble element of \(Y_{\mathbb{Q}_p}\) with \(J\)-invariant \(2^6J\), then there exists \(g \in Y_{\mathbb{Z}_p}\) with \(J\)-invariant \(2^6J\) that is \(\text{PGL}_2(\mathbb{Q}_p)\)-equivalent to \(f\). By Lemmas 5.10 and 5.11 of [BhaSha], we know that \(\sum_{f \in B_p(J)} \frac{1}{n_p(f)}\) is equal to the cardinality of \(E_J(\mathbb{Q}_p)/2E_J(\mathbb{Q}_p)\), and the cardinality of \(\text{Aut}_{\mathbb{Q}_p}(f)\) is equal to the cardinality of \(E_J(\mathbb{Q}_p)[2]\). The theorem is now proved because the volume of \(\text{PGL}_2(\mathbb{Z}_p)\) with respect to the Haar measure obtained from the \(\overline{NAN}\) decomposition is \((1 - 1/p^2)\) for \(p \geq 3\) and \(2(1 - 1/2^2)\) for \(p = 2\).

In an analogous manner, if we denote by \(U_1\) the space of monic integral cubic polynomials, then we define \(M_p(U_1)\) to be the measure of \(F^{inv}_p\) with respect to the measure \(dJ\) on \(\mathbb{Z}_p\), where the measure is normalized so that \(\mathbb{Z}_p\) has measure 1. That is, we have
\[
M_p(U_1) = \int_{J \in F^{inv}_p} dJ.
\]
5.6 Proof of Theorem 1.1.2

We only want to count the locally soluble binary quartic forms. Bhargava and Shankar call certain forms strongly maximal. For binary quartic forms with $I = 0$, strongly maximal is equivalent to $J/27$ being square free and $\not\equiv 1, 8 \pmod{9}$.

**Proposition 5.6.1.** [BhaSha, Prop. 5.14] If $f \in V_Z$ is not $\mathbb{Q}_p$-soluble or if there exists an element $f' \in V_Z$ that is $\mathbb{Q}_p$-equivalent but not $\mathbb{Z}_p$-equivalent to $f$, then $f$ is not strongly maximal.

If we had a uniformity estimate, we could use it to sieve and count the number of strongly maximal forms. This problem remains an area of ongoing research.

The following count follows easily from the use of a uniformity estimate, as in Lemma 5.16 of [BhaSha].

**Lemma 5.6.2.** The number of elliptic curves with $I = 0$ and $|J| < X$ is $\frac{2}{27}X \prod_p M_p(U_1) + O(1)$.

Now we can compute the bound on the average size of the Selmer 2-group for elliptic curves with $I = 0$.

**Theorem 5.6.3.** We have

$$\lim_{X \to \infty} \frac{\sum_{|J| < X} \# S_2(E_J)}{\sum_{E_J \in F, |J| < X} 1} \leq 3.$$ 

**Proof.** The numerator, by Theorem 1.1.4 and Lemma 5.5.1 is bounded above by

$$\frac{2^7\sigma(2)X}{27} \prod_{p \text{ prime}} \frac{1}{\sigma_p} \left(1 - \frac{1}{p^2}\right) \int_{J \in E_J^{\text{inv}}} \sum_{E_J(\mathbb{Q}_p)/2E_J(\mathbb{Q}_p)} \frac{1}{\# E_J[2](\mathbb{Q}_p)} dJ + O_\delta(X^{5/6+\delta}).$$

This bound follows from the same means as Proposition 4.2.2. The sum is 1 at all primes except $p = 2$, where it is 2. Thus the numerator is $\frac{4X}{27}$. The denominator is given by Lemma 5.6.2. Finally we add 1 for the trivial element to get 3. □
Bibliography


[BhaSha] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves


[Ger] Larry Gerstein Basic Quadratic Forms American Mathematical Society, 2008


[Kan] D. Kane, On the ranks of 2-Selmer groups of Twists of a given elliptic curve Submitted

[Kla] Z. Klagsbrun, On the distribution of 2-Selmer ranks within quadratic twist families of elliptic curves with partial rational two-torsion Submitted

[KMR] Z. Klagsbrun, B. Mazur, and K. Rubin, Selmer ranks of quadratic twists of elliptic curves Submitted


