The average rank of elliptic curves over number fields

Arul Shankar

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
Advisor: Manjul Bhargava

January 2013

UMI Number: 3553228

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI 3553228

Published by ProQuest LLC (2013). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.
All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

© Copyright by Arul Shankar, 2012.

All Rights Reserved

Abstract

In joint work with Manjul Bhargava (see [7]), we proved that the average rank of rational elliptic curves, when ordered by their heights, is bounded above by 1.5. This result was accomplished by using Bhargava's geometry-of-numbers methods (developed in [1] and [2]) to obtain asymptotics for the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary quartic forms having bounded invariants.

This thesis extends the methods of [7] and generalizes the counting results to the space of binary quartic forms over the ring of integers of any number field. As a consequence, we prove that the average rank of elliptic curves over any number field is at most 1.5.

Acknowledgements

This thesis would not have been possible without the help, support, and guidance of many people. First and foremost, I would like to thank my advisor Manjul Bhargava. Manjul was immeasurably generous with his time and ideas. From him, I learned most of the mathematics I know, and also how to think about mathematics. Manjul and his work have been a constant inspiration to me right through graduate school. I have been shaped, both as a mathematician and a person, by his ideas and sense of aesthetics, and his patience and generosity.

I have benifited greatly from talking to many mathematicians. I would particularly like to thank Professors Alireza Salehi Golsefidy, Jonathan Hanke, Peter Sarnak, Takashi Taniguchi, Frank Thorne, and Shou-Wu Zhang for sharing their knowledge and insights with me.

In graduate school, I have had the great fortune to work with and talk to many amazing students. I would like to thank my fellow graduate students Ali Altug, Sam Ruth, Jacob Tsimerman, Ila Varma, and Kevin Wilson with whom I have had the oppurtunity to work with and from whom I have learnt so very much. In addition, I have benefited from innumerable conversations with Boris Alexeev, Owen Biesel, Will Cavendish, Alex Conway, Tushar Das, Wei Ho, Bob Hough, Kevin Hughes, Junehyuk Jung, Stefan Patrikis, Aaron Pollack, Ashwath Rabindranath, Rodolfo Rios-Zertuche, Hatice Sahinoglu, Sucharit Sarkar, Shrenik Shah, Vivek Shende, Jack Thorne, Ilya Vinogradov, Jerry Wang, Percy Wong, and Melanie Wood. The help I have recieved from them is invaluable and I owe them my deepest gratitute.

It's my pleasure to thank Jill LeClair, the graduate student administrator, who has been a great friend to me and to all the math grad students at Princeton. Many of us would have fallen into disarray without her help.

It would have been impossible to handle graduate school without support from my wonderful friends. I will forever be grateful to all of you. I would particularly like

to thank Bhamini, Kishori, and Terence for their infinite hospitality and wonderful company on dozens of trips to New York. I would like to give special thanks to my girlfriend Ashley whose love, support, and encouragement have lit up my life.

Finally, it's my greatest pleasure to thank my parents Usha and Shiva, and my brother Ananth for everything. More than anything else, they have shaped me into who I am. This thesis would never have been possible without them. They have always been there for me in every way, and they have my eternal love and gratitude.

Contents

Chapter 1

Introduction

Let F be a number field, i.e., a finite extension of $\mathbb{Q}$. Any elliptic curve E/F may be expressed as

$$E = E_{A,B} : y^2 = x^3 + Ax + B,$$

where $A, B \in F$. We may further assume that A and B are contained in $\mathcal{O}$, the ring of integers of F. We may further assume that if $\alpha^4 \mid A$ and $\alpha^6 \mid B$ for $\alpha \in \mathcal{O}$, then α is a unit (i.e., $\alpha \in \mathcal{O}^\times$). If these two conditions are satisfied, we say that $E_{A,B}$ is in *reduced short Weierstrass form*. We then define the *height* of $E_{A,B}$ to be

$$H(E_{A,B}) = \max\{4H(A)^3, 27H(B)^2\}, \tag{1.1}$$

where the height $H(\alpha)$ of an element $\alpha \in \mathcal{O}$ is defined to be the maximum of its Archimedean valuations (see (2.1)).

Our goal in this thesis is to prove the following theorem.

Theorem 1.0.1. *When elliptic curves $E_{A,B}/F$ in reduced short Weierstrass form are ordered by height, the limsup of their average rank is finite and bounded by* 1.5.

We prove Theorem 1.0.1 by obtaining an upper bound for the average size of the 2-Selmer group of these elliptic curves. Recall that $S_2(E)$, the 2-Selmer group of E,

is a finite abelian 2-group and fits into the exact sequence

$$0 \to E(F)/2E(F) \to S_2(E) \to Ш_E[2] \to 0, \tag{1.2}$$

where $Ш_E[2]$ denotes the 2-torsion subgroup of the Shafarevich-Tate group $Ш_E$ of E. The 2-Selmer group has order 2^s for some integer $s \geq 0$, and s is called the 2-*Selmer rank of* E. Thus the 2-Selmer rank of E gives an upper bound for the rank of E. Our main theorem on the 2-Selmer group is as follows:

Theorem 1.0.2. *When elliptic curves $E_{A,B}/F$ in reduced short Weierstrass forms are ordered by height, the limsup of the average size of their 2-Selmer group is at most 3.*

Since $2s \leq 2^s$, the above theorem proves that the average rank of the 2-Selmer group is bounded by 1.5. Thus, Theorem 1.0.2 implies Theorem 1.0.1.

In joint work with Manjul Bhargava, we proved Theorem 1.0.1 for $F = \mathbb{Q}$. In fact, we proved something stronger:

Theorem 1.0.3 ([7])**.** *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer group $S_2(E)$ is 3.*

We proved the above theorem by counting integer orbits, having bounded invariants, for the action of $\mathrm{GL}_2(\mathbb{Z})$ on the space on integral binary quartic forms. The group $\mathrm{GL}_2(\mathbb{Z})$ acts on the space of integral binary quartic forms $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ (with $a,\ b,\ c,\ d,\ e \in \mathbb{Z}$) by linear change of variable. The ring of invariants for this action is generated (at least over $\mathbb{C}$) by two independent invariants denoted I and J. For $f(x, y)$ as above, these invariants are given by:

$$\begin{aligned} I(f) &= 12ae - 3bd + c^2, \\ J(f) &= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3. \end{aligned} \tag{1.3}$$

We define the *height* of $f(x,y)$ by $H(f) := \max\{|I|^3, J^2/4\}$ and ask the question: what is the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integer binary quartic forms having height bounded by X? Using techniques developed by Bhargava in [1] and [2], we determine asymptotics for this number.

To apply the result involving binary quartic forms to determining the average size of the 2-Selmer group of rational elliptic curves, we proceed as follows: an element in the 2-Selmer group of an elliptic curve E over $\mathbb{Q}$ (or indeed, over any number field) may be thought of as a locally soluble 2-covering of E. A result of Birch and Swinnerton-Dyer (see [10, Lemma 2]) asserts that a locally soluble 2-covering possesses a canonically associated degree 2 divisor defined over $\mathbb{Q}$, thus yielding a double cover $C \to \mathbb{P}^1$ ramified at 4 points. This produces a locally soluble binary quartic form. We use this connection and the counting result on binary quartic forms to prove Theorem 1.0.3.

This thesis closely follows the proof of Theorem 1.0.3. In Chapter 2, we first recall some basic notions about number fields. Then, for a number field F, we precisely state the connection between the 2-Selmer group of an elliptic curve E/F and $\mathrm{PGL}_2(F)$-orbits on binary quartic forms over F. In Chapter 3, we then prove our main counting result by determining asymptotics for the number of $\mathrm{PGL}_2(\mathcal{O})$-orbits on binary quartic forms over $\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of our number field F. In fact, we prove a more general result that allows us to replace $\mathrm{PGL}_2(\mathcal{O})$ with a subgroup Γ that is commensurable with it, and replace the set of binary quartic forms over $\mathcal{O}$ with certain weighted sets $\mathcal{L}$ of binary quartic forms that are Γ-invariant, so long as these weights are defined by congruence conditions. If they are defined by finitely many congruence conditions, then we obtain exact asymptotics for our count. However, for our applications we require weights that are defined by infinitely many congruence conditions. In this case, we only obtain upper bounds for the number of weighted orbits having bounded height. We hope to carry out the sieve required for

lower bounds (which is one of the more technical parts of [7]) in future work.

In Chapter 4, we first express the number of locally soluble $\mathrm{PGL}_2(F)$-orbits on binary quartic forms over F having bounded height as a sum of the number of weighted Γ-orbits on $\mathcal{L}$ (Γ and $\mathcal{L}$ as above). We then prove that the weights on $\mathcal{L}$ are indeed defined by congruence conditions by expressing them as products of local weights. Finally, in Chapter 5, we tie together the results from previous chapters to prove our main theorems.

The proofs of the results in Chapter 4 can be both clarified and greatly simplified by following the approach of Poonen [20]. The idea is to embed the space of binary quartic forms over F into a discrete lattice in the space of binary quartic forms over the adeles $\mathbb{A}_F$. Since it is rational orbits (as opposed to integral orbits) that we are interested in understanding for our purpose here, this approach would be significantly faster and cleaner.

Finally, we note that the results of this thesis are special cases of forthcoming joint work with Manjul Bhargava [8] in which we list a set of general assumptions on (G, V) that are used to obtain asymptotics for the number of "irreducible" $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$. These assumptions have already been shown to hold for many such representations (see [1], [2], [4], [9], [5], [6]). We then show in [8] that these *same* assumptions in fact imply that the analogous results hold when $\mathbb{Q}$ is replaced with any global field.

Chapter 2

Preliminaries

2.1 Basic notions for number fields

Throughout this thesis, we shall work over a number field F that is a degree n extension of $\mathbb{Q}$. We shall assume that F has r real embeddings and s pairs of complex embeddings. Thus we have $r + 2s = n$. Let $\mathrm{Arch}(F)$ denote the set of Archimedean embeddings of F. We define F_∞ by

$$F_\infty := \prod_{\nu \in \mathrm{Arch}(F)} F_\nu,$$

which is a product of r copies of $\mathbb{R}$ and s copies of $\mathbb{C}$ and has real dimension equal to n. We denote the diagonal embedding of F into F_∞ by ι, and throughout this thesis we identify F with its image $\iota(F) \subset F_\infty$. Let $\mathcal{O}$ denote the ring of integers of F. Then ι maps $\mathcal{O}$ into a lattice in F_∞ having finite covolume equal to $\sqrt{|\mathrm{Disc}(F)|}$, where $\mathrm{Disc}(F)$ is the discriminant of F.

Recall that the *norm map* $\mathbf{N} : F \to \mathbb{R}$ is defined to be

$$\mathbf{N}(\alpha) := \prod_{\nu \in \mathrm{Arch}(F)} |\alpha|_\nu,$$

for $\alpha \in F$. We naturally extend $\mathbf{N}$ to all of F_∞ by defining the norm of $(\alpha_\nu)_{\nu \in \mathrm{Arch}(F)}$ to be $\prod_{\nu \in \mathrm{Arch}(F)} |\alpha_\nu|_\nu$. Note that the image of the restriction of $\mathbf{N}$ to $\mathcal{O}$ is contained in $\mathbb{Z}$. Furthermore, if $\mathcal{L} \subset F_\infty$ is any lattice commensurable with $\mathcal{O}$, then the image of $\mathbf{N}$ restricted to $\mathcal{L}$ is discrete in $\mathbb{R}$.

The norm provides an unsuitable partial ordering on $\mathcal{O}$ because the number of elements in $\mathcal{O}$ having bounded norm is usually not finite. In fact, unless $F = \mathbb{Q}$ or a quadratic imaginary field, the group of units in $\mathcal{O}$, which all have norm ± 1 is not finite. Therefore, we define the following height function on F_∞:

$$H((\alpha_\nu)_\nu) := \max\{|\alpha_\nu|_\nu\}, \tag{2.1}$$

where $|\alpha|$ is the absolute value of α if $\alpha \in \mathbb{R}$, and $|\alpha| = a^2 + b^2$ if $\alpha = a + ib \in \mathbb{C}$. The function H also provides height functions on $F \subset F_\infty$ and $\mathcal{O} \subset F_\infty$ via their embedding ι into F_∞.

The set $F_\infty(X)$ consisting of elements in F_∞ having height bounded by X is compact. To estimate the number of elements in $\mathcal{O}$ having height bounded by X, we have the following theorem proved by Davenport [15].

Theorem 2.1.1. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and that is defined by at most k polynomial inequalities each having degree at most ℓ. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\bar{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implied constant in the second summand depends only on n, m, k, and ℓ.

The following result, which is the simplest case of the type of results we prove in this thesis, is a corollary of Theorem 2.1.1. Let $\tau = (\tau_\nu)_\nu$ be a Tamagawa measure on the ring of adeles $\mathbb{A}$ of F. Let $d\alpha = \prod_{\mathrm{Arch}(F)} \tau_\nu$ be the corresponding Haar measure on F_∞. Finally, let $N(\mathcal{O}; X)$ denote the number of elements in $\mathcal{O}$ having height bounded by X.

Corollary 2.1.2. *With notation as above, we have*

$$N(\mathcal{O}; X) = \mathrm{Vol}(F_\infty(X)) \prod_{\mathfrak{P}} \int_{\mathcal{O}_\mathfrak{P}} \tau_\mathfrak{P} + O(X^{n-1}),$$

where the volume of sets in F_∞ is taken with respect to $d\alpha$, and $\mathfrak{P}$ runs over all finite places of F.

Proof. By the definitions of $N(\mathcal{O}; X)$ and ι, we have

$$N(\mathcal{O}; X) = \#\{F_\infty(X) \cap \iota(\mathcal{O})\}.$$

Since $F_\infty(X)$ is a compact subset of $F_\infty \cong \mathbb{R}^r \oplus \mathbb{C}^s \cong \mathbb{R}^n$, Theorem 2.1.1 implies that

$$N(\mathcal{O}; X) = \mathrm{Vol}_\mathcal{O}(F_\infty(X)) + O(X^{n-1}),$$

where the volume $\mathrm{Vol}_\mathcal{O}(F_\infty(X))$ is taken with respect to Haar measure on F_∞ normalized such that $\mathcal{O} \subset F_\infty$ has covolume 1. Classical results state that $\mathcal{O}$ has covolume $\sqrt{\mathrm{Disc}(F)}$ in F_∞ under the measure $d\alpha$. From the well-known equality $\int_{F\backslash\mathbb{A}} \tau = 1$, we deduce that

$$\prod_{\mathfrak{P}} \int_{\mathcal{O}_\mathfrak{P}} \tau_\mathfrak{P} = \frac{1}{\sqrt{\mathrm{Disc}(F)}}.$$

Therefore, the corollary follows. □

2.2 Binary quartic forms and the 2-Selmer groups of elliptic curves

Throughout this thesis, we work with the algebraic group $G := \mathrm{PGL}_2$ and its representation on $V = \mathrm{Sym}^4(2)$, the space of binary quartic forms. For any ring R, we let G_R and V_R denote the R-points of G and V, respectively. The action of G_R on V_R is as follows: if $\gamma \in G_R$ and $f(x, y) \in V_R$, then we have

$$\gamma \cdot f(x, y) := \frac{1}{(\det \gamma)^2} f((x, y) \cdot \gamma).$$

This representation (G, V) is coregular [3]. This means that the ring of invariants for the action of $G_{\mathbb{C}}$ on $V_{\mathbb{C}}$ is free. In fact, it is freely generated by two elements. These invariants are traditionally denoted I and J, and are given by

$$\begin{aligned} I(f) &= 12ae - 3bd + c^2, \\ J(f) &= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3, \end{aligned} \tag{2.2}$$

where $f = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ is an element of $V_{\mathbb{C}}$. Every polynomial invariant for the action of $G_{\mathbb{C}}$ on $V_{\mathbb{C}}$ is a polynomial in I and J. For example, the discriminant $\Delta(f)$ of f can be expressed as

$$\Delta(f) := \Delta(I(f), J(f)) := (4I(f)^3 - J(f)^2)/27.$$

For any ring R, we let Inv_R denote the space $R \times R$ and think of an element $\mathbb{I} = (I, J) \in \mathrm{Inv}_R$ as a possible pair of invariants of an element $f \in V_R$.

We now detail the connection between binary quartic forms and the 2-Selmer group of elliptic curves. We say that a binary quartic form f over a field K is *K-soluble* if the equation $z^2 = f(x, y)$ has solutions with $x, y, z \in K$ and $(x, y) \neq (0, 0)$. Then we have the following theorem which is a consequence of [14, Proposition 2.2]

and [13, §3-5 and Remark 1]. For more details, see [3].

Theorem 2.2.1. *Let K be a field having characteristic not 2 or 3. Let $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ be an elliptic curve over K. Then there exists a bijection between elements in $E(K)/2E(K)$ and $\mathrm{PGL}_2(K)$-orbits of K-soluble binary quartic forms having invariants equal to I and J, given by*

$$(\xi, \eta) + 2E(K) \mapsto \mathrm{PGL}_2(K) \cdot \left(\frac{1}{4}x^4 - \frac{3}{2}\xi x^2 y^2 + 2\eta x y^3 + \left(\frac{I}{3} - \frac{3}{4}\xi^2 \right) y^4 \right).$$

Under this bijection, the identity element in $E(K)/2E(K)$ corresponds to the $\mathrm{PGL}_2(K)$-orbit of binary quartic forms that have a linear factor over K.

Furthermore, the stabilizer in $\mathrm{PGL}_2(K)$ of any (not necessarily K-soluble) binary quartic form f in V_K, having nonzero discriminant and invariants I and J, is isomorphic to $E(K)[2]$, where E is the elliptic curve defined by $y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$.

Now, let F be a number field. For an elliptic curve $E_{A,B}/F$ in reduced short Weierstrass form, we define the invariants

$$\begin{aligned} I(E_{A,B}) &= -3 \cdot 2^4 \cdot A, \\ J(E_{A,B}) &= -3 \cdot 2^6 \cdot B. \end{aligned} \tag{2.3}$$

Denote the elliptic curve having invariants I and J by $E^{I,J}$. We say that a binary quartic form f over a number field F is *locally soluble* if f is F_ν soluble for each completion F_ν of F. We then have the following theorem relating the 2-Selmer group of $E^{I,J}$ to binary quartic forms having invariants I and J:

Theorem 2.2.2. *Let $E = E^{I,J}$ be an elliptic curve over F. Then the elements of the 2-Selmer group of E are in one-to-one correspondence with $\mathrm{PGL}_2(F)$-equivalence classes of locally soluble integral binary quartic forms having invariants equal to I and J.*

Furthermore, the set of integral binary quartic forms that have a rational linear factor and invariants equal to I and J lie in one $\mathrm{PGL}_2(F)$-equivalence class, and this class corresponds to the identity element in the 2-Selmer group of E.

Chapter 3

Counting $G_{\mathcal{O}}$-orbits on integral binary quartic forms of bounded height

As before, we work over a number field F which we identify with its image under the embedding $\iota : F \to F_\infty$. Let V_{F_∞} and G_{F_∞} denote, respectively, the products

$$\begin{aligned} V_{F_\infty} &:= \prod_{\nu \in \mathrm{Arch}(F)} V_{F_\nu}, \\ G_{F_\infty} &:= \prod_{\nu \in \mathrm{Arch}(F)} G_{F_\nu}. \end{aligned}$$

The space V_F embeds in V_{F_∞} and under this embedding, $V_{\mathcal{O}}$ maps into a lattice having finite covolume. We have a natural action of G_{F_∞} on V_{F_∞} where elements in G_{F_∞} act component-by-component on V_{F_∞}. It is important to note that under this action, $G_{\mathbb{Q}} \subset G_{F_\infty}$ (resp. $G_{\mathcal{O}} \subset G_{F_\infty}$) preserves $V_{\mathbb{Q}} \subset V_{F_\infty}$ (resp. $V_{\mathcal{O}} \subset V_{F_\infty}$).

We now define a height function on V_{F_∞}. Since V_F and $V_{\mathcal{O}}$ embed into V_{F_∞}, this

will also give height functions on them. The space $\mathrm{Inv}_{\mathbb{F}_\infty}$ is given by

$$\mathrm{Inv}_{F_\infty} = \prod_{\nu \in \mathrm{Arch}(F)} \mathrm{Inv}_{F_\nu}$$

and is a product of r copies of $\mathrm{Inv}_{\mathbb{R}} = \mathbb{R}^2$ and s copies of $\mathrm{Inv}_{\mathbb{C}} = \mathbb{C}^2$. We have a natural G_{F_∞}-invariant map

$$\begin{array}{rcl} \mathrm{inv} : V_{F_\infty} & \to & \mathrm{Inv}_{F_\infty} \\ (f_1, \ldots, f_{r+s}) & \mapsto & ((I(f_1), J(f_1)), \ldots, (I(f_{r+s}), J(f_{r+s}))) \end{array} \tag{3.1}$$

which we use to define a height function on V_{F_∞}. Let $H : \mathrm{Inv}_{F_\infty} \to \mathbb{R}$ be the height function defined by

$$H((I_1, J_1), \ldots, (I_{r+s}, J_{r+s})) := \max_{i \in \{1,\ldots,r+s\}} \max(|I_i|^3, |J_i|^2/4). \tag{3.2}$$

We define $H : V_{F_\infty} \to \mathbb{R}$ to be be $H(\mathrm{inv}(v))$.

In this chapter, our aim is to determine asymptotics for the number of $G_{\mathcal{O}}$-orbits on $V_{\mathcal{O}}$ having bounded height.

3.1 The case $F = \mathbb{Q}$

We start with the case $F = \mathbb{Q}$. For any $G_{\mathbb{Z}}$-invariant set $S \subset V_{\mathbb{Z}}$, let $N(S; X)$ denote the number of irreducible $G_{\mathbb{Z}}$-orbits $G_{\mathbb{Z}} \cdot f$ on S with $0 < H(f) \leq X$, where the orbit of $f \in S$ is counted with weight $1/\#\mathrm{Aut}_{G_{\mathbb{Z}}}(f)$.

In joint work with Manjul Bhargava, we proved the following theorem:

Theorem 3.1.1 ([7])**.** *We have*

$$N(V_{\mathbb{Z}}; X) = \frac{44}{5} X^{5/6} + o(X^{5/6}).$$

In what follows, we briefly sketch a proof of the above theorem. The proof in the case of a general number field F will closely follow these ideas and methods.

Step 1: Reduction theory

For $i \in \{0,1,2\}$, let $V_{\mathbb{R}}^{(i)}$ denote the set of binary quartic forms in $V_{\mathbb{R}}$ that have nonzero discriminant and i pairs of complex conjugate roots in $\mathbb{P}^1_{\mathbb{C}}$ (and $4-2i$ real roots in $\mathbb{P}^1_{\mathbb{R}}$). Elements in $V_{\mathbb{R}}^{(2)}$ are definite forms. We denote the set of positive definite forms in $V_{\mathbb{R}}^{(2)}$ by $V_{\mathbb{R}}^{(2+)}$ and the set of negative definite forms by $V_{\mathbb{R}}^{(2-)}$. In this step, we construct a finite cover of a fundamental domain for the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$ for $i \in \{0,1,2+,2-\}$.

First, we construct fundamental sets $R^{(i)}$ for the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}^{(i)}$. To do this, we need the following facts (see [12, Remark 2]).

1 Let (I,J) in $\mathbb{R}\times\mathbb{R}$ with $\Delta(I,J)>0$ be fixed. Then the set of binary quartic forms in $V_{\mathbb{R}}$ having invariants I and J consists of three $G_{\mathbb{R}}$-orbits. There is one such orbit in $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(2+)}$, and $V_{\mathbb{R}}^{(2-)}$. Furthermore, the stabilizer in $G_{\mathbb{R}}$ of an element in any of these orbits is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

2 Let (I,J) in $\mathbb{R}\times\mathbb{R}$ with $\Delta(I,J)<0$ be fixed. Then the set of binary quartic forms in $V_{\mathbb{R}}$ having invariants I and J consists of one $G_{\mathbb{R}}$-orbit that lies in $V_{\mathbb{R}}^{(1)}$. Furthermore, the stabilizer in $G_{\mathbb{R}}$ of any element in this orbit is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Using these facts, we follow [7, Table 1] and construct fundamental sets for the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}^{(i)}$. In [7, Table 1], we had listed fundamental sets $L^{(i)}$ for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$; to then construct a fundamental set for the action of $\mathrm{PGL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$, we merely multiply $L^{(i)}$ with $\mathbb{R}_{>0}$.

We list two important properties of these sets that will be crucial in what follows. The first is straightforward. The second follows because the set of all the coefficients

$$
\begin{aligned}
R_V^{(0)} &= \left\{\lambda\Big(x^3y - \frac{1}{3}xy^3 - \frac{J}{27}y^4\Big) : -2 < J < 2,\ \lambda \in \mathbb{R}_{>0}\right\} \\
R_V^{(1)} &= \left\{\lambda\Big(x^3y - \frac{I}{3}xy^3 + \frac{\pm 2}{27}y^4\Big) : -1 \le I < 1,\ \lambda \in \mathbb{R}_{>0}\right\} \\
&\cup \left\{\lambda\Big(x^3y + \frac{1}{3}xy^3 - \frac{J}{27}y^4\Big) : -2 < J < 2,\ \lambda \in \mathbb{R}_{>0}\right\} \\
R_V^{(2+)} &= \left\{\lambda\Big(\frac{1}{16}x^4 - \frac{\sqrt{2-J}}{3\sqrt{3}}x^3y + \frac{1}{2}x^2y^2 + y^4\Big) : -2 < J < 2,\ \lambda \in \mathbb{R}_{>0}\right\} \\
R_V^{(2-)} &= \left\{f : -f \in R_V^{2+}\right\}
\end{aligned}
$$

Table 3.1: Explicit constructions of fundamental sets $R_V^{(i)}$ for $\mathrm{PGL}_2(\mathbb{R})\backslash V_{\mathbb{R}}^{(i)}$

of all the elements $f \in L^{(i)}$ is absolutely bounded.

1. For any $g \in G_{\mathbb{R}}$ and $i \in \{0, 1, 2+, 2-\}$, the set $g \cdot R^{(i)}$ is a fundamental set for the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}^{(i)}$.

2. The size of each coefficient of $f \in R^{(i)}$ having height X is bounded by $O(X^{1/6})$. (The exponent $1/6$ arises since the height is a $G_{\mathbb{R}}$-invariant degree 6 function on $V_{\mathbb{R}}$.)

Next, we choose a Siegel domain $\mathfrak{S} \subset G_{\mathbb{R}}$ that contains a fundamental domain $\mathcal{F}$ for the action of $G_{\mathbb{Z}}$ on $G_{\mathbb{R}}$. Let $G_{\mathbb{R}} = NTK$ be the Iwasawa decomposition of $G_{\mathbb{R}}$, where N is the set of lower triangular matrices with 1's on the diagonal, T is the split torus in $G_{\mathbb{R}}$, and $K = \mathrm{SO}_2(\mathbb{R})$ is the maximal compact subgroup of $G_{\mathbb{R}}$. Then we choose $\mathfrak{S}$ to be $\mathfrak{S} = N'T'K$, where

$$
N'(t) = \left\{ \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} : u \in \left[-\frac{1}{2}, \frac{1}{2}\right] \right\},\ T' = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \ge \sqrt[4]{3}/\sqrt{2} \right\},\ K = \mathrm{SO}_2(\mathbb{R}). \tag{3.3}
$$

Is it well known that $\mathfrak{S}$ contains a fundamental domain for the action of $G_{\mathbb{Z}}$ on $G_{\mathbb{R}}$. Let $\mathcal{F}$ be any such domain and consider the multiset $\mathcal{F} \cdot R^{(i)}$, where the multiplicity

of $x \in V_{\mathbb{R}}$ in $\mathcal{F} \cdot R^{(i)}$ is defined to be the number of pairs $(g, f) \in \mathcal{F} \times \mathbb{R}^{(i)}$ with $g \cdot f = x$. In the discussion surrounding [7, Equation (8)], we show that that the $G_{\mathbb{Z}}$-orbit of $x \in V_{\mathbb{R}}$ is represented $\#\mathrm{Aut}_{G_{\mathbb{R}}}(x)/\#\mathrm{Aut}_{G_{\mathbb{Z}}}(x)$ times in this multiset. Hence, we obtain the following proposition:

Proposition 3.1.2. *Let g be any element in $G_{\mathbb{R}}$. We have*

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \#\{\mathcal{F} \cdot R^{(i)}(X) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\},$$

where $R^{(i)}(X)$ denotes the set of elements in $R^{(i)}$ having height bounded by X, the set $V_{\mathbb{Z}}^{\mathrm{irr}}$ denotes irreducible elements in $V_{\mathbb{Z}}$, and n_i is given by $n_0 = n_{2+} = n_{2-} = 4$, $n_1 = 2$.

Step 2: Averaging and cutting off the cusp

The main difficulty in estimating the number of integral points in $\mathcal{F} \cdot R^{(i)}(X)$ is that the region is not bounded since $\mathcal{F}$ is noncompact. In this key step, we use the averaging technique of Bhargava, developed in [1] and [2], that allows us to estimate $N(V_{\mathbb{Z}}^{(i)}; X)$ by counting integral points in bounded domains. To this end, let G_0 be a fixed K-invariant compact set in $G_{\mathbb{R}}$ such that G_0 is the closure of some nonempty set. Proposition 3.1.2 implies that we may write

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\int_{h \in G_0} \#\{x \in \mathcal{F}h \cdot R^{(i)}(X) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\}\, dh}{n_i \int_{h \in G_0} dh}, \tag{3.4}$$

where dh is any Haar measure on $G_{\mathbb{R}} = \mathrm{PGL}_2(\mathbb{R})$. The denominator of the right hand side in (3.4) is a constant depending only on G_0 and i. We denote it by $C_{G_0}^{(i)}$. For now, we choose dh to be the Haar measure $t^{-2} dn d^{\times} t dk$ on $G_{\mathbb{R}} = NTK$. Following [7,

(11)–(16)], we obtain

$$\begin{aligned} C_{G_0}^{(i)} N(V_{\mathbb{Z}}^{(i)}; X) &= \int_{h \in G_0} \#\{x \in \mathcal{F}h \cdot R^{(i)}(X) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\}\, dh \\ &= \int_{g \in \mathcal{F} \subset N'(t)T'K} \#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap gG_0 \cdot R^{(i)}(X)\} t^{-2} dn\, d^{\times}t\, dk \qquad (3.5) \\ &= \int_{g = N'(t)T' \subset \mathcal{F}} \#\{x \in V_{\mathbb{Z}}^{\mathrm{irr}} \cap gG_0 \cdot R^{(i)}(X)\} t^{-2} dn\, d^{\times}t, \end{aligned}$$

where the final equality follows from the fact that G_0 is K-invariant and dk is normalized to have measure 1.

We write $B(n,t;X) = \left(\begin{smallmatrix} 1 & \\ n & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} t^{-1} & \\ & t \end{smallmatrix}\right) G_0 \cdot R^{(i)}(X)$ and estimate the number of integral points in it using Theorem 2.1.1. This yields good estimates when t is "small" compared to X. Let C be a constant such that $CX^{1/6}$ is an upper bound on the coefficients of the elements in $R^{(i)}(X)$. If $t^4 > CX^{1/6}$, then the x^4-coefficient of any element in $B(n,t;X)$ has absolute value less than 1. Then any integral binary quartic form in $B(n,t;X)$ must have x^4-coefficient equal to 0 and so is reducible. In other words, we have the following proposition.

Proposition 3.1.3. *The number of integral binary quartic forms* $(ax^4+bx^3y+cx^2y^2+dxy^3+ey^4) \in B(n,t,X)$ *with* $a \neq 0$ *is given by*

$$\begin{cases} 0 & \text{if } t > C^{1/4}X^{1/24}; \\ \mathrm{Vol}(B(n,t,X)) + O(t^4X^{4/6}) & \text{otherwise.} \end{cases}$$

The proof follows that of [7, Proposition 2.7].

Denoting the set $\{ntk \in \mathcal{F} : t \leq C^{1/4}X^{1/24}\}$ by $\mathcal{F}'$, we have

$$\begin{aligned} N(V_{\mathbb{Z}}^{(i)}; X) &= \frac{1}{C_{G_0}^{(i)}} \iint\limits_{nt \in \mathcal{F}'} \mathrm{Vol}(B(n,t,X)) t^{-2} dn\, d^{\times}t + O(E_1) + O(E_2) \\ &= \frac{1}{C_{G_0}^{(i)}} \iint\limits_{nt \in \mathcal{F}} \mathrm{Vol}(B(n,t,X)) t^{-2} dn\, d^{\times}t + O(E_1) + O(E_2) + O(E_3) \\ &= \frac{1}{n_i} \mathrm{Vol}(\mathcal{F} \cdot R^{(i)}(X)) + O(E_1) + O(E_2) + O(E_3), \end{aligned} \tag{3.6}$$

where E_1, E_2, and E_3 are given by

$$\begin{aligned} E_1 &:= O\Big(\iint\limits_{nt \in \mathcal{F}'} \#\{B(n,t,X) \cap V_{\mathbb{Z}}^{\mathrm{red}}\} t^{-2} dn d^{\times}t \Big), \\ E_2 &:= O\Big(\iint\limits_{nt \in \mathcal{F}'} t^4 X^{4/6} t^{-2} dn d^{\times}t \Big), \\ E_3 &:= O\Big(\iint\limits_{nt \in \mathcal{F} \setminus \mathcal{F}'} \mathrm{Vol}(B(n,t,X)) t^{-2} dn d^{\times}t \Big). \end{aligned} \tag{3.7}$$

In the above definition of E_1, the set $V_{\mathbb{Z}}^{\mathrm{red}}$ denotes the set of $f \in V_{\mathbb{Z}}$ that are reducible over $\mathbb{Q}$.

Since $\mathrm{Vol}(B(n,t,X))$ is seen to be $O(X^{5/6})$, the terms E_2 and E_3 are easily computed to be $O(X^{3/4})$. We bound E_1 by $o(X^{5/6})$ in the next step.

Step 3: Bounds on the number of reducible orbits

In this step, we show that

$$\int_{N'(t)} \int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{C^{1/4}X^{1/24}} \#\{B(n,t,X) \cap V_{\mathbb{Z}}^{\mathrm{red}}\}) t^{-2} dn d^{\times}t = o(X^{5/6}).$$

If f is an element of $V_{\mathbb{Z}}^{\mathrm{red}}$, then the reduction of f modulo p is reducible over $\mathbb{F}_p$ for every prime p. Denote the set of irreducible binary quartic forms in $V_{\mathbb{F}_p}$ by $V_{\mathbb{F}_p}^{\mathrm{irr}}$. Since the number of $\mathbb{F}_p$-conjugate quadruples of distinct points in $\mathbb{F}_{p^4}$ is $(p^4 - p^3 - p^2 + p)/4$,

it follows that that $\#V_{\mathbb{F}_p}^{\mathrm{irr}} \geq (1/4 - o(1))\#V_{\mathbb{F}_p}$. Therefore, for every positive number Y, there exists a large enough number X such that when $t \ll X^{1/24}$, we have

$$\#\{B(n,t,X) \cap V_{\mathbb{Z}}^{\mathrm{red}}\} = O\left(\mathrm{Vol}(B(n,t,X)) \prod_{p \leq Y} \left(1 - \frac{1}{4} + o(1)\right)\right).$$

Since $\prod_{p \leq Y}\left(1 - \frac{1}{4} + o(1)\right) \to 0$ as $Y \to \infty$, we are done.

Remark: It would in fact be sufficient to have the weaker estimate $\#V_{\mathbb{F}_p}^{\mathrm{irr}} \gg \frac{1}{p}\#V_{\mathbb{F}_p}$ since $\prod_{p \leq Y}(1 - 1/p) \to 0$ as $Y \to \infty$. This observation will be useful for spaces that are more complicated than the space of binary quartic forms.

Step 4: Computing the volume

The results of the previous step combined with (3.6) imply that to complete the proof of Theorem 3.1.1, we only have to compute the volume of $\mathcal{F} \cdot R^{(i)}(X)$.

The sets $R^{(i)}$ are in canonical one-to-one correspondence with the set $\{(I,J) \in \mathbb{R} \times \mathbb{R} : \Delta(I,J) > 0\}$ for $i \in \{0, 2+, 2-\}$, and with $\{(I,J) \in \mathbb{R} \times \mathbb{R} : \Delta(I,J) < 0\}$ for $i = 1$. We impose the measure $dIdJ$ on these sets $R^{(i)}$. Let ω be a differential which generates the rank 1 module of top-degree differentials of G over $\mathbb{Z}$. (ω is well-defined up to sign.) Consider the natural map $\psi : G_{\mathbb{R}} \times R^{(i)} \to G_{\mathbb{R}} \cdot R^{(i)}$. It is shown in [7, Proposition 2.8] that the Jacobian change of variables of ψ is a rational constant $\mathcal{J} = 1/27$. Therefore, we have

$$\int_{\mathcal{F} \cdot R^{(i)}(X)} dv = \frac{1}{27} \int_{R^{(i)}(X)} \int_{\mathcal{F}} dg\, dI\, dJ = \frac{2}{27} \cdot \zeta(2) \int_{R_V^{(i)}(X)} dI\, dJ,$$

where the final equality follows from the fact that $\mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}_2}) = 2\zeta(2)$ (see [18]). When $i = 0$ or 2, we compute $\int_{R^{(i)}(X)} dI\, dJ$ to be

$$\int_{I=0}^{X^{1/3}} \int_{J=-2I^{3/2}}^{2I^{3/2}} dIdJ = \frac{8}{5} X^{5/6}. \tag{3.8}$$

Meanwhile, $\int_{R_V^{(1)}(X)} dI\,dJ$ is equal to

$$\int_{I=-X^{1/3}}^{X^{1/3}} \int_{j=-2X^{1/2}}^{2X^{1/2}} dIdJ - \mathrm{Vol}(R_V^{(0)}(X)) = 8X^{5/6} - \frac{8}{5}X^{5/6} = \frac{32}{5}X^{5/6}. \tag{3.9}$$

This completes the proof of Theorem 3.1.1.

3.2 Preliminaries for the general case

We now consider the case when F is a number field of degree n. With notation as in the beginning of this chapter, let $\Gamma \subset G_F$ be a subgroup commensurable with $G_{\mathcal{O}}$ and let $\mathcal{L} \subset V_F$ be a Γ-invariant lattice commensurable with $V_{\mathcal{O}}$. For any Γ-invariant subset $S \subset \mathcal{L}$, let $N(S, \Gamma; X)$ denote the number of Γ-orbits on S having bounded height, where each orbit $\Gamma \cdot v$ is counted with weight $1/\#\mathrm{Stab}_\Gamma(v)$. Our aim in the rest of this chapter is to determine asymptotics for $N(\mathcal{L}^{\mathrm{irr}}, \Gamma; X)$, where $\mathcal{L}^{\mathrm{irr}} \subset \mathcal{L}$ denotes the set of binary quartic forms in $\mathcal{L}$ that have no linear factor over F.

3.3 Reduction theory

In the next four sections, $\mathcal{L}$, V_{F_∞}, Γ, and G_{F_∞} will respectively play the roles that $V_{\mathbb{Z}}$, $V_{\mathbb{R}}$, $G_{\mathbb{Z}}$, and $G_{\mathbb{R}}$, played in the case of $F = \mathbb{Q}$. We now describe what the analogues of the sets $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(1)}$, and $V_{\mathbb{R}}^{(2\pm)}$ are. Let $\Sigma_{V,\infty}$, the set of splitting types of V at infinity, be $\{0, 1, 2+, 2-\}^r$. For $\sigma \in \Sigma_{V,\infty}$ with $\sigma = (\sigma_1, \ldots, \sigma_r)$, we define $V_{F_\infty}^{(\sigma)}$ to be the set of all $(f_1, \ldots, f_{r+s}) \in V_{F_\infty}$ such that $f_i \in V_{\mathbb{R}}^{(\sigma_i)}$ for $i \in \{1, \ldots, r\}$ and $f_i \in V_{\mathbb{C}}^{(\Delta \neq 0)}$ for $i \in \{r+1, \ldots, r+s\}$. If $r = 0$, then $\Sigma_{V,\infty}$ consists of just one point σ, and $V_{F_\infty}^{(\sigma)}$ is the set of points in V_{F_∞} such that each component has nonzero discriminant. In this section we describe the reduction theory for the action of Γ on $V_{F_\infty}^{(\sigma)}$ for $\sigma \in \Sigma_{V,\infty}$. We start with the following lemma:

Lemma 3.3.1. *For fixed $\sigma = (\sigma_i) \in \Sigma_{V,\infty}$, the size of the stabilizer in G_{F_∞} of $v \in V_{F_\infty}^{(\sigma)}$ is independent of v. We denote this size by $\#\mathrm{Aut}(\sigma)$ which is given by*

$$\#\mathrm{Aut}(\sigma) = 4^s \prod_{i=1}^{r} n_{\sigma_i},$$

where $n_0 = n_{2\pm} = 4$ and $n_1 = 2$.

Proof. We had already stated that the size of the stabilizer in $G_{\mathbb{R}}$ of $v \in V_{\mathbb{R}}^{(i)}$ is equal to 4 when $i = 0$, $2+$, or $2-$, and equal to 2 when $i = 1$. Furthermore, it follows from Theorem 2.2.1 that the size of the stabilizer in $G_{\mathbb{C}}$ of $v \in V_{\mathbb{C}}^{(\Delta \neq 0)}$ is equal to 4. The lemma follows immediately from these facts. □

Analogously to the case $F = \mathbb{Q}$, we construct fundamental sets for the action of G_{F_∞} on $V_{F_\infty}^{(\sigma)}$. To this end, we first study the image of inv when restricted to $V_{F_\infty}^{(\sigma)}$. Let $\Sigma_{\mathrm{Inv},\infty}$ denote the set $\{-1, 1\}^r$. Consider the map

$$\begin{array}{rcl} \mathrm{inv} : \Sigma_{V,\infty} & \to & \Sigma_{\mathrm{Inv},\infty} \\ (\sigma_i) & \mapsto & (\mathrm{inv}(\sigma_i)), \end{array} \tag{3.10}$$

where $\mathrm{inv}(1) = -1$ and $\mathrm{inv}(0) = \mathrm{inv}(2\pm) = 1$. For $\alpha = (\alpha_i) \in \Sigma_{\mathrm{Inv},\infty}$, let $\mathrm{Inv}_{F_\infty}^{(\alpha)}$ denote the set of $((I_1, J_1), \ldots, (I_{r+s}, J_{r+s})) \in \mathrm{Inv}_{F_\infty}$ such that $\Delta(I_i, J_i) \in \alpha_i \mathbb{R}_{>0}$ for $i \in \{1, \ldots, r\}$. If $f \in V_{\mathbb{R}}^{(i)}$, then $\Delta(f) = \Delta(I(f), J(f))$ is positive if $i = 0$ or $2\pm$ and negative if $i = 1$. Thus the image under inv of $V_{F_\infty}^{(\sigma)}$ is $\mathrm{Inv}_{F_\infty}^{(\mathrm{inv}(\sigma))}$.

The fact that (G, V) is coregular implies that if $\mathbb{I} \in \mathrm{Inv}_{\mathbb{C}}$ has nonzero discriminant, then the set of elements in $V_{\mathbb{C}}$ having invariant $\mathbb{I}$ consists of one $G_{\mathbb{C}}$-orbit. In conjunction with the first fact stated in Step 1 of Section 3.1, we infer that for a fixed $\sigma \in \Sigma_{V,\infty}$ and an element $\mathbb{I} \in \mathrm{Inv}_{F_\infty}^{(\mathrm{inv}(\sigma))}$, the set of elements in $V_{F_\infty}^{(\sigma)}$ having invariants $\mathbb{I}$ consists of one G_{F_∞}-orbit. Therefore, to construct a fundamental domain for the action of G_{F_∞} on $V_{F_\infty}^{(\sigma)}$, it suffices to pick one element in $V_{F_\infty}^{(\sigma)}$ having invariants $\mathbb{I}$ for each $\mathbb{I} \in \mathrm{Inv}_{F_\infty}^{(\mathrm{inv}(\sigma))}$. We have already constructed fundamental sets for the action of

$G_{\mathbb{R}}$ on $V_{\mathbb{R}}^{(i)}$ for $i \in \{0, 1, 2+, 2-\}$. The following is a fundamental set for the action of $G_{\mathbb{C}}$ on $V_{\mathbb{C}}^{(\Delta \neq 0)}$:

$$R_V := \left\{ \lambda\Big(x^3y - \frac{I}{3}xy^3 - \frac{J}{27}y^4\Big) : (I, J) \in \mathbb{C} \times \mathbb{C},\ H(I, J) = 1,\ \lambda \in \mathbb{C}^\times \right\}.$$

Then $R^{(\sigma)} := \prod_i R^{(\sigma_i)}$ is a fundamental set for the action of G_{F_∞} on $V_{F_\infty}^{(\sigma)}$ that satisfies the following two properties:

1. If $v \in R^\sigma$ has height X, then the coefficients of v are bounded by $O(X^{1/6})$ independent of v.

2. $\gamma \cdot R^\sigma$ is also a fundamental set for the action of G_{F_∞} on V_{F_∞} for $\gamma \in G_{F_\infty}$.

We now construct a Siegel set $\mathfrak{S}$ in G_{F_∞} such that a fundamental domain for the action of Γ on G_{F_∞} is contained in a finite union of G_F-translates of $\mathfrak{S}$. Let $G_{F_\infty} = NTK$ be the Iwasawa decomposition of G_{F_∞}, where $N \subset G_{F_\infty}$ is the subgroup of unipotent lower triangular matrices, $T \subset G_{F_\infty}$ is the maximal split torus consisting of diagonal matrices, and $K \subset G_{F_\infty}$ is a maximal compact subgroup. Let $N' \subset N$ be a fundamental domain for the action of $N \cap G_{\mathcal{O}}$ on N. Since there exists a bounded fundamental set for the action of $\mathcal{O}$ on F_∞, we may assume that N' is bounded. Let $T'_{c,C} \subset T$ be the following set:

$$T'_{c,C} = \left\{ \left(\begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix}, \ldots, \begin{pmatrix} t_{r+s} & \\ & t_{r+s}^{-1} \end{pmatrix} \right) : \mathbf{N}(t_1) > c, \frac{\mathbf{N}(t_1)}{C} \leq \mathbf{N}(t_i) \leq C\mathbf{N}(t_1) \forall i \right\}.$$

We define the Siegel domain $\mathfrak{S}_{c,C}$ to be $N'T'_{c,C}K$. Theorem 11 in [17] asserts that $G_{F_\infty} = \cup_i G_{\mathcal{O}} g_i \mathfrak{S}_{c,C}$ for suitable c, C if and only if $G_F = \cup_i G_{\mathcal{O}} g_i N_F T_F$. By considering the action of $G_F/N_F T_F$ on $\mathbb{P}^1(F)$, it is seen that we may find finitely many g_i such that $G_F = \cup_i G_{\mathcal{O}} g_i N_F T_F$. Since Γ is commensurable with $G_{\mathcal{O}_F}$, it follows that there exist nonzero positive real numbers c and C along with a finite set of elements $\{g_i : 1 \leq i \leq k\} \subset G_F$ such that $\cup_i g_i \mathfrak{S}_{c,C}$ contains a fundamental domain for the action

of Γ on G_{F_∞}. We fix $\mathcal{F}_\Gamma$ to be one such fundamental domain.

Consider the multiset $\mathcal{F}_\Gamma \cdot R^{(\sigma)}$, where the multiplicity of $v \in V_{F_\infty}$ in $\mathcal{F}_\Gamma \cdot R^{(\sigma)}$ is $\#\{(\gamma, v') : \gamma \in \mathcal{F}_\Gamma,\ v' \in R^{(\sigma)},\ \gamma \cdot v' = v\}$. We shall need the following proposition whose proof exactly follows the discussion surrounding [7, (8)].

Proposition 3.3.2. *The Γ-orbit of $v \in V_{F_\infty}^{(\sigma)}$ is represented $\#\mathrm{Aut}(\sigma)/\#\mathrm{Stab}_\Gamma(v)$ times in the multiset $\mathcal{F}_\Gamma \cdot R^{(\sigma)}$.*

Proof. Given $v \in V_{F_\infty}^{(\sigma)}$, there exists a unique $v_R \in R^{(\sigma)}$ such that v_R is $G_{\mathbb{R}}$-equivalent to v. Suppose $g \cdot v_R = v$, for $g \in G_{\mathbb{R}}$. Then $g' \cdot v_R$ is in the Γ-orbit of v if and only if g and g' map to the same element in the double coset space

$$\Gamma \backslash G_{F_\infty} / \mathrm{Aut}_{G_{F_\infty}}(v).$$

The number of such double cosets in the right single coset $\Gamma \cdot g$ is $\#\mathrm{Aut}_{G_{F_\infty}}(v)/\#\mathrm{Aut}_\Gamma(v)$. Therefore, the number of times that the Γ-orbit of v is represented in the multiset $\mathcal{F}_\Gamma \cdot R^{(\sigma)}$ is $\#\mathrm{Aut}_{G_{F_\infty}}(v)/\#\mathrm{Aut}_\Gamma(v)$ which is equal to $\#\mathrm{Aut}(\sigma)/\#\mathrm{Stab}_\Gamma(v)$ from Lemma 3.3.1. □

Since $g \cdot R^{(\sigma)}$ is also a fundamental set for the action of G_{F_∞} on $V_{F_\infty}^{(\sigma)}$, for any $g \in G_{F_\infty}$, we obtain the following theorem which follows from Proposition 3.3.2.

Theorem 3.3.3. *Let $\Gamma \subset G_{F_\infty}$ be a subgroup commensurable with $G_{\mathcal{O}}$ and let $\mathcal{L} \subset V_{F_\infty}^{(\sigma)}$ be a Γ-invariant set. Then for any $g \in G_{F_\infty}$, we have*

$$N(\mathcal{L}, \Gamma; X) = \frac{1}{\#\mathrm{Aut}(\sigma)} \#\{\mathcal{F}_\Gamma g \cdot R^{(\sigma)}(X) \cap \mathcal{L}\}.$$

3.4 Averaging and cutting off the cusp

Let G_0 be a nonempty open bounded left K-invariant set in G_{F_∞}. Using Theorem 3.3.3, we may write

$$N(\mathcal{L},\Gamma;X)=\frac{\int_{h\in G_0}\#\{x\in\mathcal{F}_\Gamma h\cdot R^{(\sigma)}(X)\cap\mathcal{L}\}dh}{\#\mathrm{Aut}(\sigma)\int_{h\in G_0}dh}, \tag{3.11}$$

where dh is any Haar-measure on G_{F_∞}. The denominator of the right hand side of the above equation is a positive constant which we denote by $C_{G_0}^{(\sigma)}$. We now estimate the numerator in the right hand side of (3.11) following [7, (11)–(16)]. Given $x\in V_{F_\infty}^{(\sigma)}$, let x_R denote the (unique) point in $R^{(\sigma)}$ that is G_{F_∞}-equivalent to x. We have

$$N(\mathcal{L},\Gamma;X)=\frac{1}{C_{G_0}^{(\sigma)}}\sum_{\substack{x\in\mathcal{L}\\ H(x)\le X}}\int_{h\in G_0}\#\{g\in\mathcal{F}_\Gamma : x=gh\cdot x_R\}dh. \tag{3.12}$$

There exist $\#\mathrm{Aut}(\sigma)$ elements $g_i\in G_{F_\infty}$ satisfying $g_i\cdot x_R=x$. We then have

$$\int_{h\in G_0}\#\{g\in\mathcal{F}_\Gamma : x=gh\cdot x_R\}dh=\sum_i\int_{h\in G_0}\#\{g\in\mathcal{F}_\Gamma : gh=g_i\}dh=\sum_j\int_{h\in G_0\cap\mathcal{F}_\Gamma^{-1}g_i}dh.$$

Since dh is G_{F_∞}-invariant, we have

$$\begin{aligned}\sum_i\int_{h\in G_0\cap\mathcal{F}_\Gamma^{-1}g_i}dh &= \sum_i\int_{h\in G_0g_i^{-1}\cap\mathcal{F}_\Gamma^{-1}}dh=\sum_i\int_{h\in\mathcal{F}_\Gamma}\#\{g\in G_0 : hg=g_i\}dh\\ &= \int_{h\in\mathcal{F}_\Gamma}\#\{g\in G_0 : x=hg\cdot x_R\}dh.\end{aligned}$$

It thus follows that

$$\begin{aligned}N(\mathcal{L},\Gamma;X) &= \frac{1}{C_{G_0}^{(\sigma)}}\sum_{\substack{x\in\mathcal{L}\\ H(x)\le X}}\int_{h\in\mathcal{F}_\Gamma}\#\{g\in G_0 : x=hg\cdot x_R\}dh\\ &= \frac{1}{C_{G_0}^{(\sigma)}}\int_{h\in\mathcal{F}_\Gamma}\#\{x\in\mathcal{L}\cap hG_0\cdot R^{(\sigma)}(X)\}\,dh.\end{aligned}$$

Let us write $B(h, X) = hG_0 \cdot R(X)$ so that we have

$$N(\mathcal{L}, \Gamma; X) = \frac{1}{C^{\sigma}_{G_0}} \int_{h \in \mathcal{F}_\Gamma} \#\{x \in \mathcal{L} \cap B(h; X)\} dh. \tag{3.13}$$

Let $h = nak \in G_{F_\infty}$, where n, a, and k are the factors of g with respect to the Iwasawa decomposition. If a is given by

$$a = \left(\begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix}, \dots, \begin{pmatrix} t_{r+s} & \\ & t_{r+s}^{-1} \end{pmatrix} \right),$$

we define $t(h)$ to be $|t_1|_{\nu_1}$. The purpose of $t(h)$ is to quantify where $h \in \mathfrak{S}$ is located in the cusp. The larger $t(h)$ is, the higher h is in the cusp. Note that it does not make much difference to choose $t(h) = |t_i(h)|_{\nu_i}$ for some other $i \in \{1, \dots, r+s\}$; they are all within a constant multiple of each other by construction of $\mathfrak{S}$. Our next aim is to show that if $t(h)$ is large enough for $h \in \mathfrak{S}_{C,c}$, then any element in $g_i^{-1}\mathcal{L} \cap B(h; X)$ for $i \in \{1, \dots, k\}$ is reducible because its x^4-coefficient is 0.

Proposition 3.4.1. *There exists an absolute constant $c_0 > 0$ such that if $t(h) > c_0 X^{1/24}$ then $g_i^{-1}\mathcal{L}^{\mathrm{irr}} \cap B(h; X)$ is empty for $h \in \mathfrak{S}_{C,c}$ and $g_i \in \{g_1, \dots, g_k\}$. Equivalently, if $t(h) > c_0 X^{1/24}$ for $h \in g_i \mathfrak{S}_{C,c}$, then $\mathcal{L} \cap B(h; X)$ is empty.*

Proof. Let $v = (v_1, \dots, v_{r+s}) \in V_{F_\infty}$ where $v_i = a_i x^4 + b_i x^3 y + c_i x^2 y^2 + d_i x y^3 + e_i y^4$ is a binary quartic form with either real or complex coefficients depending on whether $i \leq r$ or not, respectively. Denote the $(r+s)$-tuple $(a_1, \dots, a_{r+s})$ by $a(v)$ and $\prod_{i=1}^{r+s} |a_i|_{\nu_i}$ by $\mathbf{N}(a(v))$. Since $g_i^{-1}\mathcal{L}$ is commensurable with $V_{\mathcal{O}}$, the possible nonzero values of $\mathbf{N}(a(v))$ is bounded from below by an absolute nonzero constant κ independent of g_i. It is clear from the description of $\mathfrak{S}_{C,c}$ that if $\mathbf{N}(t(h)) \gg X^{1/24}$ for $h \in \mathfrak{S}_{C,c}$, then $\mathbf{N}(a(h \cdot v))) \ll X^{-n/6}\mathbf{N}(a(v))$. Since $\mathbf{N}(a(v)) = O(X^{n/6})$ for $v \in R^{(\sigma)}(X)$, there exists an absolute constant c_0 such that if $t(h) > c_0 X^{1/24}$ for $h \in \mathfrak{S}_{C,c}$, then $\mathbf{N}(a(h \cdot v))) < \kappa$ for any $v \in R^{(\sigma)}(X/2, X)$. Then any point $v \in g_i^{-1}\mathcal{L} \cap B(h, X)$ will

satisfy $N(a(v)) = 0$ implying that it is reducible (since its x^4-coefficient is 0). $\square$

Therefore, we have

$$N(\mathcal{L}^{\text{irr}}, \Gamma; X) = \frac{1}{C_{G_0}^{(\sigma)}} \int_{\substack{h \in \mathcal{F}_\Gamma \\ t(h) < c_0 X^{1/24}}} \#\{\mathcal{L}^{\text{irr}} \cap B(h; X)\} dh.$$

Let $\mathcal{L}^{\text{red}}$ denote the set of reducible points in $\mathcal{L}$. In the next section, we show that the right hand side of the above equation with $\mathcal{L}^{\text{irr}}$ replaced by $\mathcal{L}^{\text{red}}$ is bounded by $o(X^{5n/6})$. Therefore, we may use Theorem 2.1.1 to obtain the following:

$$\begin{aligned} N(\mathcal{L}^{\text{irr}}, \Gamma; X) &= \frac{1}{C_{G_0}^{(\sigma)}} \int_{\substack{h \in \mathcal{F}_\Gamma \\ t(h) < c_0 X^{1/24}}} \#\{\mathcal{L} \cap B(h; X)\} dh + o(X^{5n/6}) \\ = \quad & \frac{1}{C_{G_0}^{(\sigma)}} \int_{\substack{h \in \mathcal{F}_\Gamma \\ t(h) < c_0 X^{1/24}}} \big(\text{Vol}_{\mathcal{L}}(B(h; X)) + O(\text{MP}(B(h; X))\big) dh + o(X^{5n/6}), \end{aligned}$$

where the volume $\text{Vol}_{\mathcal{L}}$ is taken with respect with Euclidean measure on V_{F_∞} normalized so that the lattice $\mathcal{L}$ has covolume 1 and $\text{MP}(B(h; X))$ denotes the greatest volume of the projection of $B(h; X)$ onto a smaller dimensional coordinate subspace. We will show that the main term grows like $X^{5n/6}$. Thus, the error term of $o(X^{5n/6})$ is indeed smaller than the main term.

Analogously to Proposition 3.1.3, $\text{MP}(B(h; X))$ is bounded by $O(t(h)^4 X^{(5n-1)/6})$. Its integral in the above equation is then seen to be bounded by $O(X^{\frac{5n}{6} - \frac{1}{12}})$. The integral of $\text{Vol}_{\mathcal{L}}(B(h; X))$ over the region $\{h \in \cup_{i=0}^{k} g_i^{-1} \mathcal{F}_\Gamma \cup \mathfrak{S}_{C,c} : t(h) \geq c_0 X^{1/24}\}$ is also easily computed to be $O(X^{\frac{5n}{6} - \frac{1}{12}})$. Therefore, since the volume $B(h; X)$ is independent of $h \in G_{F_\infty}$, we may write

$$\begin{aligned} N(\mathcal{L}^{\text{irr}}, \Gamma; X) &= \frac{1}{\#\text{Aut}(\sigma) \int_{G_0} dh} \int_{\mathcal{F}_\Gamma} \text{Vol}(B(h; X)) dh \\ &= \frac{\text{Vol}(\mathcal{F}_\Gamma) \text{Vol}_{\mathcal{L}}(G_0 \cdot R^{(\sigma)}(X))}{\#\text{Aut}(\sigma) \text{Vol}(G_0)}, \end{aligned} \tag{3.14}$$

where the volumes of sets in G_{F_∞} are taken with respect to any Haar measure on G_{F_∞}.

3.5 Bounds on the number of reducible orbits

Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ having sufficiently large norm to ensure that $\mathcal{L} \subset V_{\mathcal{O}_\mathfrak{P}}$ (i.e., the coefficients of elements in $\mathcal{L}$ are integral in $\mathcal{O}_\mathfrak{P}$) and that the reduction $\mathcal{L}$ modulo $\mathfrak{P}$ is all of $V_{\mathbb{F}_q}$, where $\mathbb{F}_q = \mathcal{O}/\mathfrak{P}$. For any $S \subset V_{\mathbb{F}_q}$, let $\mathcal{L}_S$ denote the set of elements in $\mathcal{L}$ whose reduction modulo $\mathfrak{P}$ lies in S. Then our methods of the previous section imply that

$$N(\mathcal{L}_S, \Gamma, X) \ll \frac{\#S}{\#V_{\mathbb{F}_q}} X^{5n/6}.$$

For any prime power q, let $V_{\mathbb{F}_q}^{\mathrm{irr}}$ denote the set of binary quartic forms in $V_{\mathbb{F}_q}$ that are irreducible over $\mathbb{F}_q$. Identically as when $F = \mathbb{Q}$, we have:

$$N(\mathcal{L}^{\mathrm{red}}, \Gamma, X) \ll \prod_{\mathrm{norm}(\mathfrak{P})<Y} \left(1 - \frac{\#V_{\mathbb{F}_q}^{\mathrm{irr}}}{\#V_{\mathbb{F}_q}}\right) X^{5n/6}$$

for fixed $Y > 0$. As before, this follows because the reduction modulo $\mathfrak{P}$ of a binary quartic form that is reducible over $\mathcal{O}$ is reducible over $\mathcal{O}/\mathfrak{P}$. As in Step 3 of Section 3.1, we deduce $\#V_{\mathbb{F}_q}^{\mathrm{irr}}/\#V_{\mathbb{F}_q} \gg 1/4$. We thus obtain

$$N(\mathcal{L}^{\mathrm{red}}, \Gamma, X) = o(X^{5n/6})$$

as necessary.

3.6 Computing the volume

In this section, we compute the value of

$$\frac{\mathrm{Vol}(\mathcal{F}_\Gamma)\mathrm{Vol}_\mathcal{L}(G_0 \cdot R^{(\sigma)}(X))}{\mathrm{Vol}(G_0)}.$$

The methods of Sections 3.3 and 3.4 imply that this quantity is independent of the Haar measure we choose for G_{F_∞}. Let ω be a differential which generates the rank 1 module of top-degree differentials of PGL_2 over $\mathbb{Z}$. Let dv be the usual Euclidean measure on V normalized such that $V_\mathbb{Z}$ has covolume 1 in $V_\mathbb{R}$ under this measure. Finally, we impose the measure $dr = dIdJ$ on Inv. With these measure normalizations, we have the following theorem that is proven in [7, Section 3.3].

Theorem 3.6.1. *Let K be $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ for any prime p. Let R be an open subset of $\mathrm{Inv}_K = K \times K$ and let $s : R \to V_K$ be a differentiable function such that the invariants of $s_{I,J} := s(I, J)$ are I and J. Then for any measurable function ϕ on V_K, we have*

$$\frac{1}{27}\int_R \int_{\mathrm{PGL}_2(K)} \phi(g \cdot s_{I,J})\,\omega(g)\,dIdJ = \int_{v \in \mathrm{PGL}_2(K)\cdot s(R)} \phi(v)dv,$$

where we regard $\mathrm{PGL}_2(K) \cdot s(R)$ as a multiset.

By construction of the sets $R^{(\sigma)}$, we obtain a section $\kappa : \mathrm{Inv}_{F_\infty}^{(\alpha)} \to R^{(\sigma)}$ (with $\alpha = \mathrm{inv}(\sigma)$) by sending the element $(I, J) \in \mathrm{Inv}_{F_\infty}^{(\alpha)}$ to the unique element in $R^{(\sigma)}$ having invariants I and J. Let $\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)$ denote the set of elements in $\mathrm{Inv}_{F_\infty}^{(\alpha)}$ having height bounded by X. Using Theorem 3.6.1, we may write

$$\frac{\mathrm{Vol}(\mathcal{F}_\Gamma)\mathrm{Vol}_\mathcal{L}(G_0 \cdot R^{(\sigma)}(X))}{\mathrm{Vol}(G_0)} = \frac{\prod_{\nu \in \mathrm{Arch}(F)} \left|\frac{1}{27}\right|_\nu \mathrm{Vol}(\mathcal{F}_\Gamma)\mathrm{Vol}(G_0)\mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X))}{\mathrm{Vol}(G_0)\mathrm{covol}(\mathcal{L})},$$

where the volumes are taken with respect to the measure normalizations of Theorem 3.6.1, and $\mathrm{covol}(\mathcal{L})$ denotes the covolume of $\mathcal{L}$. Since $\mathcal{L}$ is a lattice commensurable with $\mathcal{O}$, we have

$$\frac{1}{\mathrm{covol}(\mathcal{L})} = \prod_\mathfrak{P} \int_{\mathcal{L}_\mathfrak{P}} dv,$$

where $\mathcal{L}_\mathfrak{P}$ denotes the completion of $\mathcal{L}$ in $V_{F_\mathfrak{P}}$. Therefore, we have proven the following theorem:

Theorem 3.6.2. *Let $\mathcal{L} \subset V_{F_\infty}$ be a Γ-invariant lattice and let $\mathcal{L}^{(\sigma)}$ denote $\mathcal{L} \cap V_{F_\infty}^{(\sigma)}$. Then we have*

$$N(\mathcal{L}, \Gamma; X) = \frac{1}{27^n \# \mathrm{Aut}(\sigma)} \mathrm{Vol}(\mathcal{F}_\Gamma) \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \mathrm{Vol}(\mathcal{L}_{\mathfrak{P}}) + o(X^{5n/6}),$$

where $\alpha = \mathrm{inv}(\sigma)$.

3.7 Counting weighted orbits

For our applications, we need a more general version of Theorem 3.6.2, namely one which allows us to count weighted Γ-orbits on $\mathcal{L}$ (where the weights are defined via congruence conditions).

More precisely we say that a Γ-invariant function $\phi : \mathcal{L} \to [0, 1] \subset \mathbb{R}$ is *defined by congruence conditions* if, for all primes $\mathfrak{P}$, there exists functions $\phi_{\mathfrak{P}} : \mathcal{L}_{\mathfrak{P}} \to [0, 1]$, satisfying the following conditions:

1. For each $v \in \mathcal{L}$, we have $\phi_{\mathfrak{P}}(v) = 1$ for all but finitely many primes $\mathfrak{P}$.
2. For all $v \in \mathcal{L}$, we have $\phi(v) = \prod_{\mathfrak{P}} \phi_{\mathfrak{P}}(v)$.
3. For each prime $\mathfrak{P}$, the function $\phi_{\mathfrak{P}}$ is locally constant outside some set having measure 0 in $\mathcal{L}_{\mathfrak{P}}$.

Then we have the following generalization of Theorem 3.6.2.

Theorem 3.7.1. *Let $\phi : \mathcal{L} \to [0, 1]$ be a Γ-invariant function defined by congruence conditions via the functions $\phi_{\mathfrak{P}} : \mathcal{L}_{\mathfrak{P}} \to [0, 1]$. Let $N_\phi(\mathcal{L}^{\mathrm{irr}}, \Gamma; X)$ denote the number of Γ-orbits on $\mathcal{L}^{\mathrm{irr}}$ having height bounded by X, where each orbit $\Gamma \cdot v$ is counted with weight $\frac{\phi(v)}{\# \mathrm{Stab}_\Gamma(v)}$. Then we have*

$$N_\phi(\mathcal{L}, \Gamma; X) \leq \frac{1}{27^n \# \mathrm{Aut}(\sigma)} \mathrm{Vol}(\mathcal{F}_\Gamma) \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{v \in \mathcal{L}_{\mathfrak{P}}} \phi_{\mathfrak{P}}(v) dv + o(X^{5n/6}).$$

Proof. For each prime $\mathfrak{P}$, there exist a decreasing sequence of functions $1 = \psi_{\mathfrak{P},0} \geq \psi_{\mathfrak{P},1} \geq \dots$ that converge pointwise to $\phi_{\mathfrak{P}}$. We further assume that $\psi_{\mathfrak{P},n}$ is defined on $\mathcal{L}_{\mathfrak{P}}$ via congruence conditions modulo $\mathfrak{P}^n$. This means that the value of $\psi_{\mathfrak{P},n}(v)$ only depends on the residue of v modulo $\mathfrak{P}^n$. For a fixed integer Y, we define the partial weight $\phi^{(Y)} : \mathcal{L} \to [0,1]$ as follows:

$$\phi^{(Y)}(v) := \prod_{\mathfrak{P}} \psi_{\mathfrak{P},n(Y,\mathfrak{P})}(v),$$

where $n(Y,\mathfrak{P})$ is uniquely determined by $\mathrm{N}(\mathfrak{P})^n \leq Y < \mathrm{N}(\mathfrak{P})^{n+1}$. Note $n(Y,\mathfrak{P}) = 0$ when $\mathrm{N}(\mathfrak{P}) > Y$. Therefore, $\psi_{\mathfrak{P},n(Y,\mathfrak{P})} = \psi_{\mathfrak{P},0} = 1$ for all but finitely many primes $\mathfrak{P}$. This means that $\phi^{(Y)}$ is defined via congruence conditions modulo finitely many primes. Theorem 3.6.2 then implies that

$$N_{\phi^{(Y)}}(\mathcal{L}^{\mathrm{irr}}, \Gamma; X) = \frac{1}{27^n \#\mathrm{Aut}(\sigma)} \mathrm{Vol}(\mathcal{F}_\Gamma) \mathrm{Vol}(\mathrm{Inv}^{(\alpha)}_{F_\infty}(X)) \prod_{\mathfrak{P}} \int_{v \in \mathcal{L}_{\mathfrak{P}}} \phi_{\mathfrak{P},n(Y,\mathfrak{P})}(v) dv + o(X^{5n/6}).$$

Since $\phi \leq \phi^{(Y)}$ by construction, we have $N_\phi(\mathcal{L}^{\mathrm{irr}}, \Gamma; X) \leq N_{\phi^{(Y)}}(\mathcal{L}^{\mathrm{irr}}, \Gamma; X)$. Letting Y tend to infinity, we then obtain

$$N_\phi(\mathcal{L}^{\mathrm{irr}}, \Gamma; X) \leq \frac{1}{27^n \#\mathrm{Aut}(\sigma)} \mathrm{Vol}(\mathcal{F}_\Gamma) \mathrm{Vol}(\mathrm{Inv}^{(\alpha)}_{F_\infty}(X)) \prod_{\mathfrak{P}} \int_{v \in \mathcal{L}_{\mathfrak{P}}} \phi_{\mathfrak{P}}(v) dv + o(X^{5n/6})$$

because $\lim_{Y \to \infty} \int \phi_{\mathfrak{P},n(Y,\mathfrak{P})}(v) dv = \int \phi_{\mathfrak{P}}(v) dv$ by the bounded convergence theorem. This concludes the proof of Theorem 3.7.1. □

Chapter 4

Counting rational orbits using a mass formula

Let $\mathcal{A} \subset \mathrm{Inv}_{\mathcal{O}} = \mathcal{O}^2$ be a subset that is defined by congruence conditions. This means that

$$\mathcal{A} = \cap_{\mathfrak{P}} \mathcal{A}_{\mathfrak{P}},$$

where $\mathcal{A}_{\mathfrak{P}}$ is the closure of $\mathcal{A}$ in $\mathrm{Inv}_{\mathcal{O}_{\mathfrak{P}}} = \mathcal{O}_{\mathfrak{P}}^2$. We say that such a family $\mathcal{A}$ is *nice* if, for primes $\mathfrak{P}$ having sufficiently large norm, the set $\mathcal{A}_{\mathfrak{P}}$ contains at least those elements $(I, J) \in \mathcal{O}_{\mathfrak{P}}^2$ such that $\mathfrak{P} \nmid I$ or $\mathfrak{P} \nmid J$. If $\mathfrak{P} \mid (2)$, then we further assume that $\mathcal{A}_{\mathfrak{P}} \subset 2^4\mathcal{O}_{\mathfrak{P}} \times 2^6\mathcal{O}_{\mathfrak{P}}$. Let $\mathcal{A}(X)$ denote the set of elements in $\mathcal{A}$ having height bounded by X. Our aim in this chapter is to obtain upper bounds for the number of G_F-orbits on locally soluble elements in V_F having invariants in $\mathcal{A}(X)$.

This chapter, which is the analogue over number fields of [7, §3.2], is organized in the following way. In Section 4.1, we describe finitely many lattices $\mathcal{L}_i \subset V_F$ that are commensurable with $V_{\mathcal{O}}$ such that every locally soluble G_F-orbit on V_F having integral invariants is contained in at least one of these lattices. In the next section, we find groups $\Gamma_i \subset G_F$ commensurable with $G_{\mathcal{O}}$ such that Γ_i acts on $\mathcal{L}_i$. We then define a "global mass" $m : V_F \to \mathbb{R}$ having the following property: the number of locally

soluble G_F-orbits on V_F having invariants in $\mathcal{A}(X)$ is equal to the number of Γ_i-orbits on $\mathcal{L}_i$ (summed over all lattices $\mathcal{L}_i$) such that each orbit $\Gamma_i \cdot v$ is counted with weight $m(v)$. We then define "local masses" $m_{\mathfrak{P}} : V_{F_{\mathfrak{P}}} \to \mathbb{R}$ such that $m(v) = \prod_{\mathfrak{P}} m_{\mathfrak{P}}(v)$ for $v \in V_F$. Finally, in Section 4.4, we evaluate the "local mass integral" $\int_{V_{\mathcal{O}_{\mathfrak{P}}}} m_{\mathfrak{P}}(v)dv$.

4.1 Finding integral elements in a rational orbit

Recall that a binary quartic form $f \in V_F$ is said to be *locally soluble* if the equation $z^2 = f(x, y)$ has nontrivial solutions over F_ν for every completion ν of F. Our first aim is to find appropriate lattices $\mathcal{L} \subset V_F$ commensurable with $V_{\mathcal{O}}$ such that every locally soluble G_F-orbit on V_F having invariants in $\mathcal{A}$ contains some element of $\mathcal{L}$. The following important result of Cremona, Fisher, and Stoll allows us to do this.

Theorem 4.1.1 ([16])**.** *Let $F_{\mathfrak{P}}$ be a nonarchimedean local field and let $f \in V_{F_{\mathfrak{P}}}$ be a $F_{\mathfrak{P}}$-soluble element having integral invariants $(I, J) \in \mathcal{O}^2$. If $\mathfrak{P} \mid (2)$, then we further assume that $2^4 \mid I$ and $2^6 \mid J$. Then there exists $\gamma \in G_{F_{\mathfrak{P}}}$ such that $\gamma \cdot f \in V_{\mathcal{O}_{\mathfrak{P}}}$.*

Therefore, if a locally soluble element $v \in V_F$ has invariants in $\mathcal{A}$, then for every prime $\mathfrak{P}$, there exists $\gamma_{\mathfrak{P}}(v) \in G_{F_{\mathfrak{P}}}$ with $\gamma_{\mathfrak{P}}(v) \cdot v \in V_{\mathcal{O}_{\mathfrak{P}}}$. In the case when G_F has class number 1, it follows that there exists $\gamma(v) \in G_F$ such that $\gamma(v) \cdot v \in V_{\mathcal{O}_{\mathfrak{P}}}$ for all primes $\mathfrak{P}$. This implies that $\gamma(v) \cdot v \in V_{\mathcal{O}}$. Our results from the previous chapter may then be used to count G_F-orbits on locally soluble elements in V_F having invariants in $\mathcal{A}$. To handle the case when G_F has class number greater than 1, we proceed as follows.

Let $\mathbb{A}$ denote the ring of adeles of F and let $\mathbb{A}_f$ denote the ring of finite adeles. The strong approximation theorem for G_F implies that $G_{\mathbb{A}_f}$ is a finite union of $(\prod G_{\mathcal{O}_{\mathfrak{P}}}, G_F)$ double cosets. We may thus write

$$G_{\mathbb{A}_f} = \coprod_{i=1}^{\mathrm{cl}} (\prod_{\mathfrak{P}} G_{\mathcal{O}_{\mathfrak{P}}}) \beta_i G_F, \tag{4.1}$$

where cl is the class number of G_F and $\beta_i \in G_{\mathbb{A}_f}$ (see [19, Theorem 5.1]). For convenience, we shall denote the set $\{\beta_i : 1 \leq i \leq \text{cl}\}$ by Cl.

Now, given any $v \in V_F$ having invariants in $\mathcal{A}$, the element $(\gamma_{\mathfrak{P}}(v))_{\mathfrak{P}} \in G_{\mathbb{A}_f}$ may be expressed as

$$(\gamma_{\mathfrak{P}}(v))_{\mathfrak{P}} = (\delta_{\mathfrak{P}})_{\mathfrak{P}} \cdot \beta \cdot \gamma(v),$$

where $\beta \in \text{Cl}$, $\delta_{\mathfrak{P}} \in G_{\mathcal{O}_{\mathfrak{P}}}$, and $\gamma(v) \in G_F$. let $\beta_{\mathfrak{P}}$ denote the $\mathfrak{P}$-component of β. Then since $\gamma_{\mathfrak{P}}(v) \cdot v \in V_{\mathcal{O}_{\mathfrak{P}}}$ for all $\mathfrak{P}$ and $\delta_{\mathfrak{P}} \in V_{\mathcal{O}_{\mathfrak{P}}}$, we have

$$\beta_{\mathfrak{P}}\gamma(v) \cdot v \in V_{\mathcal{O}_{\mathfrak{P}}} \tag{4.2}$$

for all $\mathfrak{P}$.

For $\beta \in \text{Cl}$, we define $\mathcal{L}_\beta$ to be the set of all elements $v \in V_F$ such that $v \in \beta_{\mathfrak{P}}^{-1} V_{\mathcal{O}_{\mathfrak{P}}}$ for all $\mathfrak{P}$. The following theorem is a consequence of (4.2).

Theorem 4.1.2. *Let notation be as above. If $v \in V_F$ is any element having invariants in $\mathcal{A}$, then there exists $\beta \in \text{Cl}$ such that v is G_F-equivalent to an element in $\mathcal{L}_\beta$.*

4.2 Attaching a global mass to $v \in V_F$

Since $\beta_{\mathfrak{P}} \in G_{\mathcal{O}_{\mathfrak{P}}}$ for all but finitely many primes $\mathfrak{P}$, it follows that $\mathcal{L}_\beta$ is a lattice in V_F commensurable with $V_{\mathcal{O}}$. Let Γ_β be the group of all $g \in G_F$ such that $g \in \beta_{\mathfrak{P}}^{-1} G_{\mathcal{O}_{\mathfrak{P}}} \beta_{\mathfrak{P}}$ for all primes $\mathfrak{P}$. Then Γ_β is a subgroup of G_F commensurable with $G_{\mathcal{O}}$ that preserves $\mathcal{L}_\beta$.

Denote the set of locally soluble elements in V_F by V_F^{ls}. Let $N(V_F, G_F; \mathcal{A}(X))$ denote the number of G_F-orbits on V_F^{ls} having invariants in $\mathcal{A}(X)$, where each orbit $G_F \cdot v$ is counted with weight $1/\#\text{Aut}_{G_F}(v)$. Let $v \in V_F$ be an element such that $\text{inv}(v) \in \mathcal{A}$. For each $\beta \in \text{Cl}(G_F)$, let $v_{\beta,1}, \ldots, v_{\beta,k_v(\beta)}$ be a set of representatives for

the action of Γ_β on $\mathcal{L}_\beta \cap G_F \cdot v$. We define the "mass function" $m : V_F \to \mathbb{R}$ to be

$$m(v) := \begin{cases} \dfrac{1}{\#\mathrm{Aut}_{G_F}(v)} \left(\displaystyle\sum_{\beta} \sum_{i=1}^{k_v(\beta)} \frac{1}{\#\mathrm{Aut}_{\Gamma_\beta}(v_{\beta,i})} \right)^{-1} & \text{if } \mathrm{inv}(v) \in \mathcal{A} \text{ and } v \in V_F^{\mathrm{ls}}; \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

Note that $m(v)$ is well-defined by Theorem 4.1.2.

Let $N_m(\mathcal{L}_\beta, \Gamma_\beta; X)$ denote the number of Γ_β-orbits on $\mathcal{L}_\beta$ having height bounded by X, such that each orbit $\Gamma_\beta \cdot v$ is counted with weight $\frac{m(v)}{\#\mathrm{Aut}_{\Gamma_\beta}(v)}$. The significance of the mass function m is seen in the following proposition.

Proposition 4.2.1. *We have*

$$N(G_F, V_F; \mathcal{A}(X)) = \sum_{\beta} N_m(\mathcal{L}_\beta, \Gamma_\beta; X). \tag{4.4}$$

Proof. Every locally soluble G_F-orbit $G_F \cdot v$ having invariants in $\mathcal{A}$ is counted with weight $1/\#\mathrm{Aut}_{G_F}(v)$ in the left hand side of (4.4). In the right hand side the orbit $G_F \cdot v$ is counted with weight

$$\sum_{\beta} \sum_{i=1}^{k_v(\beta)} \frac{m(v)}{\#\mathrm{Aut}_{\Gamma_\beta}(v_{\beta,i})} = \frac{1}{\#\mathrm{Aut}_{G_F}(v)} \left(\sum_{\beta} \sum_{i=1}^{k_v(\beta)} \frac{1}{\#\mathrm{Aut}_{\Gamma_\beta}(v_{\beta,i})} \right)^{-1} \left(\sum_{\beta} \sum_{i=1}^{k_v(\beta)} \frac{1}{\#\mathrm{Aut}_{\Gamma_\beta}(v_{\beta,i})} \right),$$

where the equality follows from the definition of $m(v)$ in (4.3). This concludes the proof of the proposition. □

In the rest of this section, we express $m(v)$ in a more convenient form. Let $G_F(\mathcal{L}_\beta, v)$ denote the set

$$G_F(\mathcal{L}_\beta, v) := \{\gamma \in G_F : \gamma \cdot v \in \mathcal{L}_\beta\}.$$

It is clear that Γ_β acts on $G_F(\mathcal{L}_\beta, v)$ from the left and $\mathrm{Aut}_{G_F}(v)$ acts on it on the

right. We have a map from $\Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v)$ to the set of Γ_β-orbits on $\mathcal{L}_\beta \cap G_F \cdot v$ given by $\Gamma_\beta g \mapsto \Gamma_\beta g \cdot v$. This is clearly a surjective map between finite sets. Two elements $\Gamma_\beta g_1$ and $\Gamma_\beta g_2$ map to the same orbit under this map if and only if g_1 and g_2 map to the same element in the double coset space

$$\Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v) / \mathrm{Aut}_{G_F}(v).$$

Therefore, the number of elements in $\Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v)$ that map to the same orbit $\Gamma_\beta \cdot v'$ is equal to $\#\mathrm{Aut}_{G_F}(v)/\#\mathrm{Aut}_{\Gamma_\beta}(v')$. This yields the following important result:

Theorem 4.2.2. *Let $v \in V_F$ be a locally soluble binary quartic form having invariants in $\mathcal{A}$. Then*

$$\frac{1}{m(v)} = \#\mathrm{Aut}_{G_F}(v) \left(\sum_\beta \sum_{i=1}^{k_v(\beta)} \frac{1}{\#\mathrm{Aut}_{\Gamma_\beta}(v_{\beta,i})} \right) = \sum_\beta \#(\Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v)). \tag{4.5}$$

4.3 Attaching a local mass to $v \in V_{F_\mathfrak{P}}$

In order to evaluate $N_m(\mathcal{L}_\beta, \Gamma_\beta; X)$, we shall need to write m as a product of "local mass functions". Let $\mathfrak{P} \subset \mathcal{O}$ be a prime ideal and let $V_{F_\mathfrak{P}}^{\mathrm{sol}} \subset V_{F_\mathfrak{P}}$ be the set of $F_\mathfrak{P}$-soluble binary quartic forms. We now define a local mass function $m_\mathfrak{P} : V_{F_\mathfrak{P}} \to \mathbb{R}$ that depends on $\mathcal{A}_\mathfrak{P}$. Analogously to the previous section, we consider the $G_{F_\mathfrak{P}}$-equivalence class of v in $V_{\mathcal{O}_\mathfrak{P}}$ and let $v_1, \ldots, v_{k_v}$ be representatives for the action of $G_{\mathcal{O}_\mathfrak{P}}$ on this set. For $v \in V_{F_\mathfrak{P}}$, we define $m_\mathfrak{P}(v)$ to be

$$m_\mathfrak{P}(v) := \begin{cases} \dfrac{1}{\#\mathrm{Aut}_{G_{F_\mathfrak{P}}}(v)} \left(\displaystyle\sum_{i=1}^{k_v} \frac{1}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v_i)} \right)^{-1} & \text{if } \mathrm{inv}(v) \in \mathcal{A}_\mathfrak{P} \text{ and } v \in V_{F_\mathfrak{P}}^{\mathrm{sol}}; \\ 0 & \text{otherwise.} \end{cases} \tag{4.6}$$

Our purpose in the rest of this section is to prove that $m(v) = \prod_{\mathfrak{P}} m_{\mathfrak{P}}(v)$ for all $v \in V_F$.

To this end, let $G_{F_{\mathfrak{P}}}(v)$ be the set of elements $g \in G_{F_{\mathfrak{P}}}$ such that $g \cdot v \in V_{\mathcal{O}_{\mathfrak{P}}}$. Though $G_{F_{\mathfrak{P}}}(v)$ is not a group, $G_{\mathcal{O}_{\mathfrak{P}}}$ acts on it from the left. As before, if $m_{\mathfrak{P}}(v) \neq 0$, then

$$\frac{1}{m(v)} = \#\mathrm{Aut}_{G_{F_{\mathfrak{P}}}}(v) \left(\sum_{i=1}^{k_v} \frac{1}{\#\mathrm{Aut}_{G_{\mathcal{O}_{\mathfrak{P}}}}(v_i)} \right) = \#(G_{\mathcal{O}_{\mathfrak{P}}} \backslash G_{F_{\mathfrak{P}}}(v)). \tag{4.7}$$

We are now in a position to prove the following important theorem:

Theorem 4.3.1. *Let $v \in V_F$ be any element. Then*

$$m(v) = \prod_{\mathfrak{P}} m_{\mathfrak{P}}(v).$$

Proof. We first show that $m(v) = 0$ if and only if $\prod_{\mathfrak{P}} m_{\mathfrak{P}}(v) = 0$. Suppose $v \in V_F$ satisfies $m(v) = 0$. Then either $\mathrm{inv}(v) \notin \mathcal{A}$ or $v \notin V_F^{\mathrm{ls}}$. Since $\mathcal{A}$ is defined by congruence conditions, this implies that either $\mathrm{inv}(v) \notin \mathcal{A}_{\mathfrak{P}}$ for some $\mathfrak{P}$ or $v \notin V_{F_{\mathfrak{P}}}^{\mathrm{sol}}$ for some $\mathfrak{P}$. Thus, it follows that $m_{\mathfrak{P}}(v) = 0$. Conversely, if $\prod_{\mathfrak{P}} m_{\mathfrak{P}}(v) = 0$, then because $m_{\mathfrak{P}}(v) = 1$ for all but finitely many primes $\mathfrak{P}$, we have $m_{\mathfrak{P}}(v) = 0$ for some prime $\mathfrak{P}$. It then follows that $\mathrm{inv}(v) \notin \mathcal{A}_{\mathfrak{P}}$ or $v \notin V_{F_{\mathfrak{P}}}^{\mathrm{sol}}$. In either case, we obtain $m(v) = 0$.

Now suppose that $v \in V_F$ is a locally soluble binary quartic form having invariants in $\mathcal{A}$. Then $m(v) \neq 0$. From (4.5) and (4.7) it suffices to prove that the following equality holds:

$$\sum_{\beta \in \mathrm{Cl}} \#(\Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v)) = \prod_{\mathfrak{P}} \#(G_{\mathcal{O}_{\mathfrak{P}}} \backslash G_{F_{\mathfrak{P}}}(v)).$$

To do this, consider the map

$$\begin{aligned} \phi : \bigcup_{\beta} \Gamma_\beta \backslash G_F(\mathcal{L}_\beta, v) &\to \prod_{\mathfrak{P}} (G_{\mathcal{O}_{\mathfrak{P}}} \backslash G_{F_{\mathfrak{P}}}(v)) \\ \Gamma_\beta \cdot \gamma &\mapsto (G_{\mathcal{O}_{\mathfrak{P}}} \cdot (\beta_{\mathfrak{P}} \gamma))_{\mathfrak{P}}. \end{aligned} \tag{4.8}$$

By definition, $\gamma \cdot v \in \mathcal{L}_\beta$ for $\gamma \in G_F(\mathcal{L}_\beta, v)$, which implies that $\beta_{\mathfrak{P}}\gamma \cdot v \in V_{\mathcal{O}_\mathfrak{P}}$. Thus ϕ is well defined. We now prove that ϕ is a bijection, thereby proving Theorem 4.3.1.

Injectivity of ϕ: If there exists $\beta \in \mathrm{Cl}$ and $\beta' \in \mathrm{Cl}$ along with $\gamma \in G_F(\mathcal{L}_\beta, v)$ and $\gamma' \in G_F(\mathcal{L}'_\beta, v)$ such that $\phi(\Gamma_\beta\gamma) = \phi(\Gamma_{\beta'}\gamma')$, then it follows that $\beta_{\mathfrak{P}}\gamma$ and $\beta'_{\mathfrak{P}}\gamma'$ are $G_{\mathcal{O}_\mathfrak{P}}$-equivalent, for all $\mathfrak{P}$. Therefore, there exist $g_{\mathfrak{P}} \in G_{\mathcal{O}_\mathfrak{P}}$ such that $\beta_{\mathfrak{P}}\gamma = g_{\mathfrak{P}}\beta'_{\mathfrak{P}}\gamma'$ for all primes $\mathfrak{P}$. The strong approximation theorem for G (4.1) now implies that $\beta = \beta'$. Furthermore, we have $\gamma\gamma'^{-1} \in \beta_{\mathfrak{P}}^{-1} G_{\mathcal{O}_\mathfrak{P}} \beta_{\mathfrak{P}}$ for all $\mathfrak{P}$. In other words, $\gamma\gamma'^{-1} \in \Gamma_\beta$ as necessary.

Surjectivity of ϕ: If $(h_{\mathfrak{P}})_{\mathfrak{P}} \in \prod_{\mathfrak{P}}(G_{\mathcal{O}_\mathfrak{P}} \backslash G_{F_\mathfrak{P}}(v))$, then (4.1) implies that we may write $(h_{\mathfrak{P}})_{\mathfrak{P}} = (g_{\mathfrak{P}})_{\mathfrak{P}}\beta\gamma$, where $\gamma \in G_F$, $\beta \in \mathrm{Cl}$, and $g_{\mathfrak{P}} \in G_{\mathcal{O}_\mathfrak{P}}$ for all $\mathfrak{P}$. We claim that $\gamma \in G_F(\mathcal{L}_\beta, v)$, which would show that $\phi(\Gamma_\beta\gamma) = (h_{\mathfrak{P}})_{\mathfrak{P}}$. We know that $h_{\mathfrak{P}} \cdot v \in V_{\mathcal{O}_\mathfrak{P}}$ from which it follows that $\gamma \cdot v \in \beta_{\mathfrak{P}}^{-1} \cdot V_{\mathcal{O}_\mathfrak{P}}$. This implies that $\gamma \in G_F(\mathcal{L}_\beta, v)$ and thus $(h_{\mathfrak{P}})_{\mathfrak{P}}$ is in the image of ϕ. This concludes the proof of Theorem 4.3.1. □

4.4 Evaluating the mass integral

Our aim in this section is to evaluate the mass integral $\int_{V_{\mathcal{O}_\mathfrak{P}}} m_{\mathfrak{P}}(v)dv$.

For each pair $\mathbb{I} = (I, J) \in \mathcal{A}$, let $B_{\mathfrak{P}}(\mathbb{I}) \subset V_{\mathcal{O}_\mathfrak{P}}$ be a set containing one element in each soluble $G_{\mathcal{O}_\mathfrak{P}}$-orbit on the elements in $V_{\mathcal{O}_\mathfrak{P}}$ having invariant $\mathbb{I} \in \mathcal{A}$. The set $G_{\mathcal{O}_\mathfrak{P}} \cdot B_{\mathfrak{P}}(\mathbb{I})$ is a multiset in which every soluble element v with $\mathrm{inv}(v) = \mathbb{I}$ is counted with multiplicity $\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v)$. Consider the multiset $S_{\mathcal{A}_\mathfrak{P}}$ defined by

$$S_{\mathcal{A}_\mathfrak{P}} := \bigcup_{\mathbb{I} \in \mathcal{A}} G_{\mathcal{O}_\mathfrak{P}} \cdot B_{\mathfrak{P}}(\mathbb{I}).$$

We have

$$\int_{V_{\mathcal{O}_\mathfrak{P}}} m_{\mathfrak{P}}(v)dv = \int_{S_{\mathcal{A}_\mathfrak{P}}} \frac{m_{\mathfrak{P}}(v)}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v)} dv.$$

Since $m_{\mathfrak{P}}$ is $G_{\mathcal{O}_\mathfrak{P}}$-invariant (in fact, it is $G_{F_\mathfrak{P}}$-invariant), Proposition 3.6.1 implies

that

$$\int_{S_{\mathcal{A}_\mathfrak{P}}} \frac{m_\mathfrak{P}(v)}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v)} dv = |\mathcal{J}|_\mathfrak{P} \mathrm{Vol}(G_{\mathcal{O}_\mathfrak{P}}) \int_{\mathbb{I}\in\mathcal{A}_\mathfrak{P}} \left(\sum_{v\in B_\mathfrak{P}(\mathbb{I})} \frac{m_\mathfrak{P}(v)}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v)} \right) d\mathbb{I}.$$

For $v \in B_\mathfrak{P}(\mathbb{I})$, let $v = v_1, v_2, \ldots, v_{k(v)}$ be the set of elements in $B_\mathfrak{P}(\mathbb{I})$ that are $G_{F_\mathfrak{P}}$-equivalent to v. Then, from the definition of $m_\mathfrak{P}(v)$, we have

$$\begin{aligned} \sum_{i=1}^{k(v)} \frac{m_\mathfrak{P}(v_i)}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v_i)} &= \frac{1}{\#\mathrm{Aut}_{G_{F_\mathfrak{P}}}(v)} \left(\sum_{i=1}^{k(v)} \frac{1}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v_i)} \right)^{-1} \left(\sum_{i=1}^{k(v)} \frac{1}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v_i)} \right) \\ &= \frac{1}{\#\mathrm{Aut}_{G_{F_\mathfrak{P}}}(v)}. \end{aligned}$$

Therefore, we have

$$\sum_{v\in B_\mathfrak{P}(\mathbb{I})} \frac{m_\mathfrak{P}(v)}{\#\mathrm{Aut}_{G_{\mathcal{O}_\mathfrak{P}}}(v)} = \sum_{v\in B'_\mathfrak{P}(\mathbb{I})} \frac{1}{\#\mathrm{Aut}_{G_{F_\mathfrak{P}}}(v)},$$

where $B'_\mathfrak{P}(\mathbb{I})$ is a set consisting of one element for each $G_{F_\mathfrak{P}}$-equivalence class on the elements in $V_{\mathcal{O}_\mathfrak{P}}$ having invariant $\mathbb{I}$. For $\mathbb{I} \in \mathcal{A}$, we know that every element in $V_{F_\mathfrak{P}}$ having invariant $\mathbb{I}$ is $G_{F_\mathfrak{P}}$-equivalent to an element in $V_{\mathcal{O}_\mathfrak{P}}$. Therefore, we may write

$$\int_{V_{\mathcal{O}_\mathfrak{P}}} m_\mathfrak{P}(v) dv = |\mathcal{J}|_\mathfrak{P} \mathrm{Vol}(G_{\mathcal{O}_\mathfrak{P}}) \int_{\mathbb{I}\in\mathcal{A}_\mathfrak{P}} M_\mathfrak{P}(\mathbb{I}) d\mathbb{I},$$

where $M_\mathfrak{P}(\mathbb{I})$ is given by

$$M_\mathfrak{P}(\mathbb{I}) := \sum_{G_{F_\mathfrak{P}}\backslash V_{F_\mathfrak{P}}^{\mathrm{inv}=\mathbb{I}}} \frac{1}{\#\mathrm{Aut}_{G_{F_\mathfrak{P}}}(v)}.$$

In the above equation, $G_{F_\mathfrak{P}}\backslash V_{F_\mathfrak{P}}^{\mathrm{inv}=\mathbb{I}}$ is a set consisting of representatives for the action of $G_{F_\mathfrak{P}}$ on the set of soluble elements in $V_{F_\mathfrak{P}}$ having invariant $\mathbb{I}$.

To evaluate $M_\mathfrak{P}(\mathbb{I})$, we have the following proposition whose proof is identical to

that of [11, Lemma 3.1].

Proposition 4.4.1. *Let E be an elliptic curve over $F_{\mathfrak{P}}$. We have*

$$\#(E(F_{\mathfrak{P}})/2E(F_{\mathfrak{P}})) = \#E[2](F_{\mathfrak{P}})\#(\mathcal{O}_{\mathfrak{P}}/2\mathcal{O}_{\mathfrak{P}}).$$

Proof. A well-known result of Lutz (see, e.g., [21, Chapter 7, Proposition 6.3] for a proof) asserts that there exists a subgroup $M \subset E(F_{\mathfrak{P}})$ of finite index that is isomorphic to $\mathcal{O}_{\mathfrak{P}}$. Let G denote the finite group $E(F_{\mathfrak{P}})/M$. Then by applying the snake lemma to the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E(F_{\mathfrak{P}}) & \longrightarrow & G & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} & & \downarrow \\ 0 & \longrightarrow & M & \longrightarrow & E(F_{\mathfrak{P}}) & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

we obtain the exact sequence

$$0 \to M[2] \to E(F_{\mathfrak{P}})[2] \to G[2] \to M/2M \to E(F_{\mathfrak{P}})/2E(F_{\mathfrak{P}}) \to G/2G \to 0.$$

Since G is a finite group and M is isomorphic to $\mathcal{O}_{\mathfrak{P}}$, Proposition 4.4.1 follows. □

Fix $\mathbb{I} = (I, J) \in \mathcal{A}$. Theorem 2.2.1 states that if $v \in V_F$ has invariants I and J, then we have

$$\begin{aligned} \#(G_{F_{\mathfrak{P}}} \backslash V_{F_{\mathfrak{P}}}^{\mathrm{inv}=\mathbb{I}}) &= \#(E^{(I,J}(F_{\mathfrak{P}})/2E^{I,J}(F_{\mathfrak{P}})), \\ \#\mathrm{Aut}_{G_{F_{\mathfrak{P}}}}(v) &= \#E^{I,J}[2](F_{\mathfrak{P}}). \end{aligned}$$

Therefore, Proposition 4.4.1 implies that $M_{\mathfrak{P}}(\mathbb{I}) = \#(\mathcal{O}_{\mathfrak{P}}/2\mathcal{O}_{\mathfrak{P}})$. We summarize this section in the following theorem:

Theorem 4.4.2. *With notation as above, we have:*

$$\int_{V_{\mathcal{O}_{\mathfrak{P}}}} m_{\mathfrak{P}}(v)dv = |\mathcal{J}|_{\mathfrak{P}} \cdot \#(\mathcal{O}_{\mathfrak{P}}/2\mathcal{O}_{\mathfrak{P}}) \cdot \mathrm{Vol}(G_{\mathcal{O}_{\mathfrak{P}}}) \cdot \int_{\mathbb{I} \in \mathcal{A}_{\mathfrak{P}}} d\mathbb{I}.$$

Chapter 5

The average number of elements in the 2-Selmer group of elliptic curves over F

Let $\mathcal{A} \subset \mathcal{O}^2$ be a set that is defined via congruence conditions. Recall that this means

$$\mathcal{A} = \cap_{\mathfrak{P}} \mathcal{A}_{\mathfrak{P}}$$

where $\mathcal{A}_{\mathfrak{P}}$ is the completion of $\mathcal{A}$ in $\mathcal{O}_{\mathfrak{P}}^2$. We say that such a family is *nice* if for primes $\mathfrak{P}$ having sufficiently large norm, the set $\mathcal{A}_{\mathfrak{P}}$ contains at least those elements $(I, J) \in \mathcal{O}_{\mathfrak{P}}^2$ such that $\mathfrak{P} \nmid I$ or $\mathfrak{P} \nmid J$. If $\mathfrak{P} \mid (2)$, we further assume that $2^4 \mid I$ and $2^6 \mid J$ for $(I, J) \in \mathcal{A}_{\mathfrak{P}}$.

Let $\mathcal{E}_{\mathcal{A}}$ be the family of elliptic curves over F defined by

$$\mathcal{E}_{\mathcal{A}} := \{E^{I,J} : y^2 = x^3 - \frac{I}{3}x + \frac{B}{27} |\ (I, J) \in \mathcal{A},\ \Delta(I, J) \neq 0\}.$$

We impose the following height on elements in $\mathcal{E}_{\mathcal{A}}$:

$$H(E^{I,J}) := H(I,J),$$

where $H(I,J)$ was defined in (3.2). In this chapter, we prove that the average size of the 2-Selmer group of elliptic curves in $\mathcal{E}_{\mathcal{A}}$, when ordered by height, is at most 3.

5.1 Counting elliptic curves in $\mathcal{E}_{\mathcal{A}}$ having bounded height

Let $N(\mathcal{E}_{\mathcal{A}}; X)$ denote the number of elements in $\mathcal{E}_{\mathcal{A}}$ having height bounded by X. In this section, we obtain asymptotics for $N(\mathcal{E}_{\mathcal{A}})$. Techniques identical to the proof of Theorem 3.7.1 will yield upper bounds on $N(\mathcal{E}_{\mathcal{A}}; X)$. However, obtaining lower bounds is more difficult, and to do so we need the following "uniformity estimate".

Lemma 5.1.1. *For a prime $\mathfrak{P}$, let $\mathcal{W}^{(\mathfrak{P})}(\mathcal{E}_{\mathcal{A}})$ denote the set $E^{I,J} \in \mathcal{E}_{\mathcal{A}}$ such that $\mathfrak{P} \mid I$ and $\mathfrak{P} \mid J$. Then we have*

$$\#\{E \in \mathcal{W}^{(\mathfrak{P})}(\mathcal{E}_{\mathcal{A}}) : H(E) < X\} = O\Big(\frac{X^{5n/6}}{\mathrm{N}(\mathfrak{P})^{5/3}}\Big), \tag{5.1}$$

where the implied constant is independent of $\mathfrak{P}$.

Proof. The left hand side of (5.1) is bounded above by the number of integer pairs $(0,0) \neq (I,J) \in \mathcal{A} \subset \mathcal{O}^2$ with $H(I) \leq X^{1/3}$, $H(J) \leq X^{1/2}$, $\mathfrak{P} \mid I$, and $\mathfrak{P} \mid J$. From Corollary 2.1.2, we obtain that

$$\#\{0 \neq a \in \mathcal{O} : H(a) < Y,\ \mathfrak{P} \mid a\} = \begin{cases} O(Y^n/\mathrm{N}(\mathfrak{P})) & \text{if } \mathrm{N}(\mathfrak{P}) \leq \mathrm{N}(Y) = Y^n; \\ \\ 0 & \text{if } \mathrm{N}(\mathfrak{P}) > Y^n. \end{cases}$$

It therefore follows that

$$\#\{E \in \mathcal{W}^{(\mathfrak{P})}(\mathcal{E}_{\mathcal{A}}) : H(E) < X\} = \begin{cases} O(X^{5n/6}/\mathrm{N}(\mathfrak{P})^2) & \text{if } \mathrm{N}(\mathfrak{P}) \leq X^{n/3}; \\ O(X^{n/2}/\mathrm{N}(\mathfrak{P})) & \text{if } X^{n/3} < \mathrm{N}(\mathfrak{P}) \leq X^{n/2}; \\ 0 & \text{if } \mathrm{N}(\mathfrak{P}) > X^{n/2}. \end{cases} \tag{5.2}$$

Lemma 5.1.1 follows easily from (5.2). □

Recall that we had defined the space $\Sigma_{\mathrm{Inv}_\infty}$ to be $\{-1, 1\}^r$, where r is the number of real embeddings of F. Consider the map

$$\begin{aligned} \mathrm{st} : \mathrm{Inv}_{F_\infty}^{(\Delta \neq 0)} &\rightarrow \Sigma_{\mathrm{Inv}_\infty} \\ (I_i, J_i)_{i \leq r+s} &\mapsto (\mathrm{sign}(\Delta(I_i, J_i)))_{i \leq r} \end{aligned} \tag{5.3}$$

which sends an element of $\mathrm{Inv}_{F_\infty}^{(\Delta \neq 0)}$ to its "splitting type". We had previously used st to write Inv_{F_∞} as a finite union

$$\mathrm{Inv}_{F_\infty}^{(\Delta \neq 0)} = \bigcup_{\alpha \in \Sigma_{\mathrm{Inv}_\infty}} \mathrm{Inv}_{F_\infty}^{(\alpha)},$$

where $\mathrm{Inv}_{F_\infty}^{(\alpha)}$ consists of the elements in $\mathrm{Inv}_{F_\infty}^{(\Delta \neq 0)}$ having splitting type α. We correspondingly write $\mathcal{E}_{\mathcal{A}}$ as a finite union

$$\mathcal{E}_{\mathcal{A}} = \bigcup_{\alpha \in \Sigma_{\mathrm{Inv}_\infty}} \mathcal{E}_{\mathcal{A}}^{(\alpha)},$$

where $\mathcal{E}_{\mathcal{A}}^{(\alpha)}$ is defined to be the set of $E^{I,J}$ in $\mathcal{E}_{\mathcal{A}}$ such that $\mathrm{st}(I, J) = \alpha$. We are now prepared to prove the main theorem of this section.

Theorem 5.1.2. *Let $N(\mathcal{E}_{\mathcal{A}}^{(\alpha)}; X)$ denote the number of elements in $\mathcal{E}_{\mathcal{A}}^{(\alpha)}$ having height*

bounded by X. Then we have

$$N(\mathcal{E}_{\mathcal{A}}^{(\alpha)}; X) = \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{\mathbb{I} \in \mathcal{A}_{\mathfrak{P}}} d\mathbb{I} + o(X^{5n/6}).$$

Proof. By assumption, $\mathcal{A}$ is a subset of $\mathcal{O}^2$ defined by (possibly infinitely many) congruence conditions. For any finite subset S of these conditions, let $\mathcal{A}^{(S)}$ denote the subset of elements in $\mathcal{O}^2$ that satisfy S. Then we have

$$\#\{\mathrm{Inv}_{F_\infty}^{(\alpha)}(X) \cap \mathcal{A}^{(S)}\} = \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{\mathbb{I} \in \mathcal{A}_{\mathfrak{P}}^{(S)}} d\mathbb{I} + O(X^{(5n-2)/6}),$$

where $\mathcal{A}_{\mathfrak{P}}^{(S)}$ denotes the closure of $\mathcal{A}^{(S)}$ in $\mathcal{O}_{\mathfrak{P}}^2$. Taking the limit as S tends towards the set of all congruence conditions that are used to define $\mathcal{A}$, we then obtain

$$\#\{\mathrm{Inv}_{F_\infty}^{(\alpha)}(X) \cap \mathcal{A}\} \leq \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{\mathbb{I} \in \mathcal{A}_{\mathfrak{P}}} d\mathbb{I} + o(X^{5n/6}).$$

We now obtain a lower bound for $\#\{\mathrm{Inv}_{F_\infty}^{(\alpha)}(X) \cap \mathcal{A}\}$. Assume that S contains all the mod $\mathfrak{P}$ congruence conditions used to define $\mathcal{A}$ for $\mathrm{N}(\mathfrak{P}) \leq Y$. Then the uniformity estimate in Lemma 5.1.1 implies that we have

$$\#\{\mathrm{Inv}_{F_\infty}^{(\alpha)}(X) \cap \mathcal{A}^{(S)}\} \leq \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{\mathbb{I} \in \mathcal{A}_{\mathfrak{P}}^{(S)}} d\mathbb{I} + O\Big(\sum_{\mathrm{N}(\mathfrak{P})>Y} \frac{X^{5n/6}}{\mathrm{N}(cp)^{5/3}} \Big).$$

This yields Theorem 5.1.2 because $\sum_{\mathfrak{P}} \mathrm{N}(cp)^{-5/3}$ converges. □

5.2 Proof of the main theorem

We now prove the following theorem from which the main theorems follow.

Theorem 5.2.1. *Let $\mathcal{E}_{\mathcal{A}}^{(\alpha)}$ be as in the previous section. Then we have*

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{E\in\mathcal{E}_{\mathcal{A}}^{(\alpha)}\\ H(E)<X}} \#S_2(E) - 1}{\sum\limits_{\substack{E\in\mathcal{E}_{\mathcal{A}}^{(\alpha)}\\ H(E)<X}} 1} \leq 2. \tag{5.4}$$

Proof. From Theorem 5.1.2, we know that the denominator of the left hand side of (5.4) is equal to

$$\mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \cdot \prod_{\mathfrak{P}} \int_{\mathbb{I}\in\mathcal{A}_{\mathfrak{P}}} d\mathbb{I} + o(X^{5n/6}).$$

From Theorem 2.2.1, we see that the numerator of (5.4) is equal to $N(G_F, V_F^{(\alpha)}; \mathcal{A}(X))$, the number of locally soluble G_F-orbits on V_F having invariants in $\mathcal{A}(X)$ and splitting type σ satisfying $\mathrm{inv}(\sigma) = \alpha$, where each G_F-orbit $G_F \cdot v$ counted with weight $1/\#\mathrm{Stab}_{G_F}(v)$. Let $\Sigma^{(\alpha)} \subset \Sigma_{V,\infty}$ be the set of those soluble splitting types σ such that $\mathrm{inv}(\sigma) = \alpha$. Then (4.4) implies that

$$N(G_F, V_F^{(\alpha)}; \mathcal{A}(X)) = \sum_{\sigma\in\Sigma^{(\alpha)}} \sum_{\beta\in\mathrm{Cl}} N_m(\mathcal{L}_\beta^{(\alpha)}, \Gamma_\beta; X),$$

where m is the mass function defined in (4.3). From Theorem 3.7.1, we then see that the numerator of the left hand side of (5.4) is bounded above by

$$\frac{1}{27^n} \sum_{\sigma\in\Sigma^{(\alpha)}} \frac{1}{\#\mathrm{Aut}(\sigma)} \sum_{\beta\in\mathrm{Cl}} \mathrm{Vol}(\mathcal{F}_{\Gamma_\beta}) \mathrm{Vol}(\mathrm{Inv}_{F_\infty}^{(\alpha)}(X)) \prod_{\mathfrak{P}} \int_{\mathcal{L}_{\beta_{\mathfrak{P}}}} m_{\mathfrak{P}}(v)dv + o(X^{5n/6}).$$

It is easy to compute that $\sum_{\sigma\in\Sigma^{(\alpha)}} \frac{1}{\#\mathrm{Aut}(\sigma)} = \frac{1}{2^n}$ for all α. Since $m_{\mathfrak{P}}$ is $G_{F_{\mathfrak{P}}}$-invariant, we have $\int_{\mathcal{L}_{\beta_{\mathfrak{P}}}} m_{\mathfrak{P}}(v)dv = \int_{\mathcal{O}_{\mathfrak{P}}} m_{\mathfrak{P}}(v)dv$. Therefore, using Theorem 4.4.2 and taking

ratios, we see the left hand side of (5.4) is bounded above by

$$\frac{1}{27^n} \cdot \frac{1}{2^n} \sum_{\beta \in \mathrm{Cl}} \mathrm{Vol}(\mathcal{F}_{\Gamma_\beta}) \prod_{\mathfrak{P}} \left(\left| \frac{1}{27} \right|_{\mathfrak{P}} \#(\mathcal{O}_{\mathfrak{P}}/2\mathcal{O}_{\mathfrak{P}}) \mathrm{Vol}(G_{\mathcal{O}_{\mathfrak{P}}}) \right).$$

Using the product formula and the fact that $\prod_{\mathfrak{P}} \#(\mathcal{O}_{\mathfrak{P}}/2\mathcal{O}_{\mathfrak{P}}) = 2^n$, we see that the above expression is equal to

$$\sum_{\beta \in \mathrm{Cl}} \mathrm{Vol}(\mathcal{F}_{\Gamma_\beta}) \prod_{\mathfrak{P}} \mathrm{Vol}(G_{\mathcal{O}_{\mathfrak{P}}}) = \tau(G_F) = 2,$$

where $\tau(G_F)$ is the Tamagawa number of G_F. This concludes the proof of the theorem.

□

Bibliography

[1] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math **162** (2005), 1031–1063.

[2] ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), 1559—1591.

[3] M. Bhargava and W. Ho, *Coregular representations and genus one curves*, preprint.

[4] ———, *On the average sizes of Selmer groups in families of elliptic curves*, preprint.

[5] M. Bhargava and A. Shankar, *The average number of elements in the* 4*-Selmer groups of elliptic curves is 7*, preprint.

[6] ———, *The average number of elements in the* 5*-Selmer group of elliptic curves*, preprint.

[7] ———, *Binary quartic forms having bounded invariants and the boundedness of the average rank of elliptic curves*, preprint.

[8] ———, *Geometry-of-numbers methods over number fields and function fields*, in progress.

[9] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, preprint.

[10] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves I*, J. Reine Angew. Math. **212** (1963), 7–25.

[11] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math J. **44** (1977), 715–743.

[12] J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94.

[13] J. E. Cremona and T. Fisher, *On the equivalence of binary quartics*, J. of Symbol. Comp. **44** (2009), 673–682.

[14] J. E. Cremona and M. Stoll, *Minimal models for 2-coverings of elliptic curves*, LMS J. Comput. Math. **5** (2002), 220–243 (electronic).

[15] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.

[16] J. Cremona T. Fisher and M. Stoll, *Minimisation and reduction of* 2-, 3- *and* 4-*coverings of elliptic curves*, J. of Alg. Num. Thy. **4** (2010), 763–820.

[17] R. Godement, *Domaines fondamentaus des groupes arithmetiques*, Séminaire Bourbaki (1962), 201–225.

[18] R. P. Langlands, *The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups*, Proc. Sympos. Pure Math., Boulder, Colo. (1965), 143–148.

[19] V. Platonov and A. Rapinchuk (translated from the 1991 Russian original by Rachel Rowen), *Algebraic groups and number theory.*, Pure and Applied Mathematics, Academic Press, Inc., Boston, MA **139** (1994).

[20] B. Poonen, *Average rank of elliptic curves* (*after Manjul Bhargava and Arul Shankar*), Séminaire Bourbaki, to appear in Astérisque.

[21] J. H. Silverman, *The arithmetic of elliptic curves, second edition*, Graduate Texts in Mathematics, Springer, Dordrecht **106** (2009).