



RESEARCH ARTICLE

Average Analytic Ranks of Elliptic Curves over Number Fields

Tristan Phillips 

Department of Mathematics, Dartmouth College, 29 North Main Street, Hanover, NH, 03755-3551, United States;
E-mail: tristanphillips72@gmail.com.

Received: 8 June 2022; **Revised:** 1 October 2024; **Accepted:** 13 October 2024

2020 Mathematics Subject Classification: *Primary* – 11G05; *Secondary* – 11G07, 11G35, 11G50, 11D45, 14G05

Abstract

We give a conditional bound for the average analytic rank of elliptic curves over an arbitrary number field. In particular, under the assumptions that all elliptic curves over a number field K are modular and have L -functions which satisfy the Generalized Riemann Hypothesis, we show that the average analytic rank of isomorphism classes of elliptic curves over K is bounded above by $(9 \deg(K) + 1)/2$, when ordered by naive height. A key ingredient in the proof is giving asymptotics for the number of elliptic curves over an arbitrary number field with a prescribed local condition; these results are obtained by proving general results for counting points of bounded height on weighted projective stacks with a prescribed local condition, which may be of independent interest.

Contents

1	Introduction	2
1.1	Average analytic ranks of elliptic curves	2
1.2	Counting points on weighted projective stacks	4
1.3	Asymptotic notation	4
1.4	Organization	5
2	Preliminaries on weighted projective stacks	5
2.1	Heights on weighted projective stacks	5
3	Weighted geometry of numbers over number fields	6
3.1	O-minimal geometry	7
3.2	Weighted geometry-of-numbers	7
4	Counting points on weighted projective stacks	10
5	Counting elliptic curves	18
5.1	Counting elliptic curves with a prescribed local condition	18
6	Average analytic ranks	22
6.1	L-functions of elliptic curves	22
6.2	Class number estimates	27
6.3	Estimating $S_1(\phi, B)$ and $S_2(\phi, B)$	31
6.4	Bounding the average analytic rank of elliptic curves	32
	References	34

1. Introduction

1.1. Average analytic ranks of elliptic curves

Let E be an elliptic curve over a number field K . The Mordell–Weil theorem states that the set of K -rational points $E(K)$ of E forms a finitely generated abelian group $E(K) \cong E(K)_{\text{tor}} \oplus \mathbb{Z}^r$, where $E(K)_{\text{tor}}$ is the finite *torsion subgroup* and $r \in \mathbb{Z}_{\geq 0}$ is the *rank*. The study of ranks of elliptic curves has become a central topic in number theory. Despite this attention, ranks remain a mystery in many ways.

Birch and Swinnerton-Dyer [BSD65] famously conjectured that the rank of an elliptic curve equals its *analytic rank* (i.e., the order of vanishing of its L -function at $s = 1$).

To get an understanding of ranks of elliptic curves in general, one can hope to determine the average rank of elliptic curves. As there are infinitely many elliptic curves, in order to make sense of this average, one must order elliptic curves in some way. Throughout this article, we order elliptic curves by their *naive height*, as defined at the end of Section 2. The average analytic rank of elliptic curves over the rational numbers was first bounded by Brumer [Bru92], who gave an upper bound of 2.3 under the assumption of the Generalized Riemann Hypothesis for elliptic L -functions.¹ Under the same conditions, this bound was improved to 2 by Heath-Brown [HB04], and then to $25/14 \approx 1.8$ by Young [You06]. In a remarkable series of papers [BS15a, BS15b, BS13a, BS13b], Bhargava and Shankar bounded the average size of 2-, 3-, 4- and 5-Selmer groups of elliptic curves, leading to an unconditional upper bound of 0.885 for the average rank of elliptic curves over \mathbb{Q} .

Surprisingly little is known about average ranks of elliptic curves over number fields beyond \mathbb{Q} . In Shankar’s doctoral thesis [Sha13], he extends his work with Bhargava on bounding 2-Selmer groups to show that the average rank of elliptic curves over number fields is bounded above by 1.5. However, Shankar’s result counts *reduced Weierstrass equations*, which differs from counting isomorphism classes. In particular, counting reduced Weierstrass equations coincides with counting isomorphism classes of elliptic curves only for the finitely many number fields with unit group $\{\pm 1\}$ and class number 1 – namely, \mathbb{Q} and the imaginary quadratic extensions $\mathbb{Q}(\sqrt{-d})$ for $d \in \{2, 7, 11, 19, 43, 67, 163\}$. Outside of these cases, there can be multiple reduced Weierstrass equations within the same isomorphism class of elliptic curves.

In this article, we prove a conditional bound for the average analytic rank of isomorphism classes of elliptic curves over an arbitrary number field. This appears to be the first known bound on average ranks of isomorphism classes of elliptic curves over arbitrary number fields, as well as the first bound for average analytic ranks of elliptic curves over number fields other than \mathbb{Q} .

Theorem 1.1.1. *Let K be a number field of degree d . Assume that all elliptic curves over K are modular and that their L -functions satisfy the Generalized Riemann Hypothesis. Then, the average analytic rank of isomorphism classes of elliptic curves over K , when ordered by naive height, is bounded above by $(9d + 1)/2$.*

One of the main difficulties in extending methods for counting elliptic curves over the rational numbers to elliptic curves over more general number fields is that one may no longer have a bijection between reduced short Weierstrass models and isomorphism classes of elliptic curves. We overcome this difficulty by exploiting the geometry of the moduli stack of elliptic curves. In particular, the (compactified) moduli stack of elliptic curves is isomorphic to the weighted projective stack $\mathcal{P}(4, 6)$. From this perspective, questions about counting elliptic curves of bounded height turn into questions about counting points of bounded height on weighted projective stacks. Such questions can then be studied using various tools from Diophantine geometry.

One of the key ingredients in the proof of Theorem 1.1.1 is estimating the number of elliptic curves with prescribed local conditions over number fields. To state our results on counting elliptic curves, we introduce some notation. Let K be a number field with ring of integers \mathcal{O}_K , discriminant Δ_K , class number h_K , regulator R_K , and which contains ϖ_K roots of unity. Let $\text{Val}(K)$ denote the set of places

¹Brumer also assumed that all elliptic curves over \mathbb{Q} were modular, which was unknown at the time, but later confirmed in a series of papers by Andrew Wiles and his students.

Table 1. Local conditions.

\mathcal{L}	$\kappa_{\mathcal{L}}$	$\epsilon_{\mathcal{L}}$
good	$\frac{q-1}{q} \frac{q^{10}}{q^{10}-1}$	q
bad	$\frac{q^9-1}{q^{10}} \frac{q^{10}}{q^{10}-1}$	q
multiplicative	$\frac{q-1}{q^2} \frac{q^{10}}{q^{10}-1}$	1
split multiplicative	$\frac{q-1}{2q^2} \frac{q^{10}}{q^{10}-1}$	1
nonsplit multiplicative	$\frac{q-1}{2q^2} \frac{q^{10}}{q^{10}-1}$	1
additive	$\frac{q^2-1}{q^{10}} \frac{q^{10}}{q^{10}-1}$	q
I_m	$\frac{q^2-2q+1}{q^{m+2}} \frac{q^{10}}{q^{10}-1}$	q
II	$\frac{q-1}{q^3} \frac{q^{10}}{q^{10}-1}$	1
III	$\frac{q-1}{q^4} \frac{q^{10}}{q^{10}-1}$	1
IV	$\frac{q-1}{q^5} \frac{q^{10}}{q^{10}-1}$	1
I_0^*	$\frac{q-1}{q^6} \frac{q^{10}}{q^{10}-1}$	q
I_m^*	$\frac{q^2-2q+1}{q^{m+7}} \frac{q^{10}}{q^{10}-1}$	q
II^*	$\frac{q-1}{q^{10}} \frac{q^{10}}{q^{10}-1}$	$1/q^2$
III^*	$\frac{q-1}{q^9} \frac{q^{10}}{q^{10}-1}$	$1/q^3$
IV^*	$\frac{q-1}{q^8} \frac{q^{10}}{q^{10}-1}$	$1/q$

of K , let $\text{Val}_0(K)$ denote the set of finite places, and let $\text{Val}_\infty(K)$ denote the set of infinite places. Let ζ_K denote the Dedekind zeta function of K . Let $H(\cdot)$ denote the Hurwitz-Kronecker class number (see Subsection 5.1 for the definition). For a prime $\mathfrak{p} \subset \mathcal{O}_K$, above a rational prime $p \in \mathbb{Z}$, we will write $\deg(\mathfrak{p})$ for the index of fields $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p]$, which we will refer to as the *degree* of \mathfrak{p} .

Theorem 1.1.2. *Let K be a degree d number field, and let \mathfrak{p} be a prime ideal of \mathcal{O}_K of norm q such that $2 \nmid q$ and $3 \nmid q$. Let \mathcal{L} be one of the local conditions listed in Table 1. Then the number of elliptic curves over K with naive height less than B , and which satisfy the local condition \mathcal{L} at \mathfrak{p} , is*

$$\kappa_{\mathcal{L}} B^{5/6} + O\left(\epsilon_{\mathcal{L}} B^{\frac{5}{6} - \frac{1}{3d}}\right),$$

where

$$\kappa = \frac{h_K (2^{r_1+r_2} \pi^{r_2})^2 R_K 10^{r_1+r_2-1} \gcd(2, \varpi_K)}{\varpi_K |\Delta_K| \zeta_K(10)},$$

and where $\kappa_{\mathcal{L}}$ and $\epsilon_{\mathcal{L}}$ are as in Table 1.

We also give asymptotics for counting elliptic curves with a prescribed trace of Frobenius:

Theorem 1.1.3. *Let K be a degree d number field, and let \mathfrak{p} be a degree n prime ideal of \mathcal{O}_K above a rational prime $p > 3$. Set $q = N_{K/\mathbb{Q}}(\mathfrak{p}) = p^n$, the norm of \mathfrak{p} . Let $a \in \mathbb{Z}$ be an integer satisfying $|a| \leq 2\sqrt{q}$. Then, the number of elliptic curves over K with naive height less than B , good reduction at \mathfrak{p} , and which have trace of Frobenius a at \mathfrak{p} , is*

$$\kappa_{n,a} B^{5/6} + O\left(\epsilon_{n,a} B^{\frac{5}{6} - \frac{1}{3d}}\right),$$

Table 2. Constants for Theorem 1.1.3.

n	a	$\kappa_{n,a}$	$\epsilon_{n,a}$
any	$ a < 2\sqrt{q}$ and $p \nmid a$	$\frac{q^{10}}{q^{10}-1}(q-1)H(a^2-4q)/q^2$	$H(a^2-4q)$
odd	$a = 0$	$\frac{q^{10}}{q^{10}-1}(q-1)H(-4p)/q^2$	$H(-4p)$
odd	$a \neq 0$ and $p a$	0	0
even	$a^2 = 4q$	$\frac{q^{10}}{q^{10}-1} \frac{q-1}{12q^2} \left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right) \right)$	$p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)$
even	$a^2 = q$	$\frac{q^{10}}{q^{10}-1}(q-1)\left(1 - \left(\frac{-3}{p}\right)\right)/q^2$	$1 - \left(\frac{-3}{p}\right)$
even	$a^2 = 0$	$\frac{q^{10}}{q^{10}-1}(q-1)\left(1 - \left(\frac{-4}{p}\right)\right)/q^2$	$1 - \left(\frac{-4}{p}\right)$
even	$a^2 \notin \{4q, q, 0\}$ and $p a$	0	0

where

$$\kappa = \frac{h_K(2^{r_1+r_2}\pi^{r_2})^2 R_K 10^{r_1+r_2-1} \gcd(2, \varpi_K)}{\varpi_K |\Delta_K| \zeta_K(10)},$$

and where $\kappa_{n,a}$ and $\epsilon_{n,a}$ are as in Table 2.

Theorem 1.1.2 and Theorem 1.1.3 generalize a result of Cho and Jeong [CJ23b, Theorem 1.4] for elliptic curves over \mathbb{Q} to elliptic curves over arbitrary number fields. For more results on counting elliptic curves with prescribed local conditions, see the work of Cremona and Sadek [CS23].

1.2. Counting points on weighted projective stacks

Our results for counting isomorphism classes of elliptic curves are special cases of a more general theorem for counting points of bounded height on weighted projective stacks.

In [Sch79], Schanuel proved an asymptotic for the number of rational points of bounded height on projective spaces over number fields. This was generalized to weighted projective stacks by Deng [Den98] (see also the work of Darda [Dar21], which gives a proof using height zeta functions). In this paper, we extend these results to count points of bounded height which satisfy finitely many prescribed local conditions (see Theorem 4.0.5).

Remark 1.2.1. Let us briefly mention some additional results related to counting points of bounded height on weighted projective stacks. Recently, Bruin and Manterola Ayala [MA21, BMA23] have generalized Deng’s result to count points whose images, with respect to a morphism of weighted projective stacks, are of bounded height. Using the geometric sieve, Bright, Browning and Loughran [BBL16] have proven a generalization of Schanuel’s theorem which allows one to impose infinitely many local conditions on the points of projective space being counted. In [Phi22], the author combines these results to count points whose images, with respect to a morphism of weighted projective stacks, are of bounded height and satisfy prescribed local conditions. Such a result has applications to counting elliptic curves with certain prescribed level structures and local conditions. Building from this result, Cho, Jeong and Park [CJP23] have given a conditional bound for average analytic ranks of isomorphism classes of elliptic curves over number fields with a prescribed level structure.

1.3. Asymptotic notation

Let $f : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ and $g : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ be real valued functions. Throughout the article, we will write $f = O(g)$ (or $f \ll g$) if there exist constants $C, D \in \mathbb{R}_{>0}$ such that for all $x \geq D$, we have $|f(x)| \leq C \cdot g(x)$. We refer to any such C as the implied constant. If the implied constant depends on a parameter t , then we will write $f = O_t(g)$ (or $f \ll_t g$).

1.4. Organization

In Section 2, we cover basic facts about weighted projective stacks and heights defined on weighted projective stacks. In Section 3, we prove a result for counting points of bounded height satisfying prescribed local conditions on affine spaces over number fields. In Section 4, we prove our main result for counting points of bounded height on weighted projective stacks (Theorem 4.0.5). In Section 5, we apply Theorem 4.0.5 to count elliptic curves with prescribed local conditions. This is where we prove Theorem 1.1.2 and Theorem 1.1.3. Finally, in Section 6, we use the explicit formula for L-functions, together with our results for counting elliptic curves with prescribed local conditions, to bound the average analytic rank of elliptic curves over number fields. This is where we prove Theorem 1.1.1.

2. Preliminaries on weighted projective stacks

In this section, we recall basic facts about weighted projective stacks with an emphasis on heights.

2.1. Heights on weighted projective stacks

Given an $(n + 1)$ -tuple of positive integers $\mathbf{w} = (w_0, \dots, w_n)$, the **weighted projective stack** $\mathcal{P}(\mathbf{w})$ is the quotient stack

$$\mathcal{P}(\mathbf{w}) \stackrel{\text{def}}{=} [(\mathbb{A}^{n+1} - \{0\})/\mathbb{G}_m],$$

where the multiplicative group scheme, \mathbb{G}_m , acts on the punctured affine space, $\mathbb{A}^{n+1} - \{0\}$, as follows:

$$\begin{aligned} \mathbb{G}_m \times (\mathbb{A}^{n+1} - \{0\}) &\rightarrow (\mathbb{A}^{n+1} - \{0\}) \\ (\lambda, (x_0, \dots, x_n)) &\mapsto \lambda *_{\mathbf{w}} (x_0, \dots, x_n) \stackrel{\text{def}}{=} (\lambda^{w_0} x_0, \dots, \lambda^{w_n} x_n). \end{aligned}$$

In the special case when $\mathbf{w} = (1, \dots, 1)$, this recovers the usual projective space \mathbb{P}^n .

The point $[(a_0, \dots, a_n)] \in \mathcal{P}(w_0, \dots, w_n)$ has stabilizer μ_m , where $m = \gcd(w_i : a_i \neq 0)$. When K is a field of characteristic zero, we have that μ_m is finite and reduced over K . It follows that, over fields of characteristic zero, $\mathcal{P}(w_0, \dots, w_n)$ is a Deligne–Mumford stack.

For any field F , let $\mathcal{P}(\mathbf{w})(F)$ denote the set of isomorphism classes of the groupoid of F -points of $\mathcal{P}(\mathbf{w})$. More concretely, $\mathcal{P}(\mathbf{w})(F)$ is in canonical bijection with the quotient

$$(F^{n+1} - \{0\})/F^\times,$$

where F^\times acts on $F^{n+1} - \{0\}$ by the weighted action

$$\begin{aligned} F^\times \times (F^{n+1} - \{0\}) &\rightarrow (F^{n+1} - \{0\}) \\ (\lambda, (a_0, \dots, a_n)) &\mapsto (\lambda^{w_0} a_0, \dots, \lambda^{w_n} a_n). \end{aligned}$$

Throughout this article, unless otherwise stated, we assume all weighted projective stacks $\mathcal{P}(\mathbf{w})$ are defined over a number field K .

For each finite place $v \in \text{Val}_0(K)$, let \mathfrak{p}_v be the corresponding prime ideal, and let π_v be a uniformizer for the completion K_v of K at v . For $x = (x_0, \dots, x_n) \in K^{n+1} - \{0\}$, set $|x_i|_{\mathbf{w},v} \stackrel{\text{def}}{=} |\pi_v|_v^{\lfloor v(x_i)/w_i \rfloor}$, and set

$$|x|_{\mathbf{w},v} \stackrel{\text{def}}{=} \begin{cases} \max_i \{|x_i|_{\mathbf{w},v}\} & \text{if } v \in \text{Val}_0(K) \\ \max_i \{|x_i|_v^{1/w_i}\} & \text{if } v \in \text{Val}_\infty(K). \end{cases}$$

Definition 2.1.1 (Height). The **(exponential) height** of a point $x = [x_0 : \dots : x_n] \in \mathcal{P}(\mathbf{w})(K)$ is defined as

$$\text{Ht}_{\mathbf{w}}(x) \stackrel{\text{def}}{=} \prod_{v \in \text{Val}(K)} |(x_0, \dots, x_n)|_{\mathbf{w}, v}.$$

It is straightforward to check that this height function does not depend on the choice of representative of x .

Definition 2.1.2 (Scaling ideal). Define the **scaling ideal** $\mathfrak{S}_{\mathbf{w}}(x)$ of $x = (x_0, \dots, x_n) \in K^{n+1} - \{0\}$ to be the fractional ideal

$$\mathfrak{S}_{\mathbf{w}}(x) \stackrel{\text{def}}{=} \prod_{v \in \text{Val}_0(K)} \mathfrak{p}_v^{\min_i \{\lfloor v(x_i)/w_i \rfloor\}}.$$

The scaling ideal $\mathfrak{S}_{\mathbf{w}}(x)$ can be characterized as the intersection of all fractional ideals \mathfrak{a} of \mathcal{O}_K such that $x \in \mathfrak{a}^{w_0} \times \dots \times \mathfrak{a}^{w_n} \subseteq K^{n+1}$. It has the property that

$$\mathfrak{S}_{\mathbf{w}}(x)^{-1} = \{a \in K : a^{w_i} x_i \in \mathcal{O}_K \text{ for all } i\}.$$

The height can be written in terms of the scaling ideal as follows:

$$\text{Ht}_{\mathbf{w}}([x_0 : \dots : x_n]) = \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{S}_{\mathbf{w}}(x))} \prod_{v \in \text{Val}_{\infty}(K)} \max_i \{|x_i|_v^{1/w_i}\}.$$

It is straightforward to check that this agrees with the height from Definition 2.1.1.

Remark 2.1.3. The height $\text{Ht}_{\mathbf{w}}$ was first defined by Deng [Den98]. In the case of projective spaces, $\mathbb{P}^n = \mathcal{P}(1, \dots, 1)$, this height corresponds to the usual Weil height. In more geometric terms, this height on weighted projective stacks can be viewed as the ‘stacky height’ associated to the tautological bundle of $\mathcal{P}(\mathbf{w})$ (see [ESZB23, §3.3] for this and much more about heights on stacks).

The (compactified) moduli stack of elliptic curves, $\mathcal{X}_{\text{GL}_2(\mathbb{Z})}$, is isomorphic to the weighted projective stack $\mathcal{P}(4, 6)$. This isomorphism can be given explicitly as

$$\begin{aligned} \mathcal{X}_{\text{GL}_2(\mathbb{Z})} &\xrightarrow{\sim} \mathcal{P}(4, 6) \\ y^2 = x^3 + Ax + B &\mapsto [A : B]. \end{aligned}$$

Under this isomorphism, the tautological bundle on $\mathcal{P}(4, 6)$ corresponds to the Hodge bundle on $\mathcal{X}_{\text{GL}_2(\mathbb{Z})}$. The usual *naive* height of an elliptic curve E over K with a reduced integral short Weierstrass equation $y^2 = x^3 + Ax + B$ is defined as

$$\text{Ht}(E) \stackrel{\text{def}}{=} \prod_{v \in \text{Val}_{\infty}(K)} \max\{|A|_v^3, |B|_v^2\}.$$

One can show that this *naive height* is the same as the *stacky* height on $\mathcal{X}_{\text{GL}_2(\mathbb{Z})}$ with respect to the twelfth power of the Hodge bundle [ESZB23, §3.3]. For any short Weierstrass equation $y^2 = x^3 + ax + b$ of E , the naive height is given by

$$\text{Ht}(E) \stackrel{\text{def}}{=} \text{Ht}_{(4,6)}([a : b])^{12}.$$

3. Weighted geometry of numbers over number fields

Let K be a number field. In this section, we prove asymptotics for the number of K -rational points of bounded height with prescribed local conditions on affine spaces with respect to a weighting. For these asymptotics, we give a power savings error term which is independent of the local conditions.

3.1. O-minimal geometry

We briefly cover the basics of o-minimal geometry which will be needed in this article. A general reference for this subsection is [vdD98, §1]. Let m_L denote Lebesgue measure on \mathbb{R}^n .

Definition 3.1.1 (Semi-algebraic set). A (real) **semi-algebraic subset** of \mathbb{R}^n is a finite union of sets of the form

$$\{x \in \mathbb{R}^n : f_1(x) = \dots = f_k(x) = 0 \text{ and } g_1(x) > 0, \dots, g_l(x) > 0\},$$

where $f_1, \dots, f_k, g_1, \dots, g_l \in \mathbb{R}[X_1, \dots, X_n]$.

Definition 3.1.2 (Structure). A **structure** is a sequence, $\mathcal{S} = (\mathcal{S}_n)_{n \in \mathbb{Z}_{>0}}$, where each \mathcal{S}_n is a set of subsets of \mathbb{R}^n with the following properties:

- (i) If $A, B \in \mathcal{S}_n$, then $A \cup B \in \mathcal{S}_n$ and $\mathbb{R}^n - A \in \mathcal{S}_n$ (i.e., \mathcal{S}_n is a Boolean algebra).
- (ii) If $A \in \mathcal{S}_m$ and $B \in \mathcal{S}_n$, then $A \times B \in \mathcal{S}_{m+n}$.
- (iii) If $\pi : \mathbb{R}^n \rightarrow \mathbb{R}^m$ is the projection to m distinct coordinates and $A \in \mathcal{S}_n$, then $\pi(A) \in \mathcal{S}_m$.
- (iv) All real semi-algebraic subsets of \mathbb{R}^n are in \mathcal{S}_n .

A subset is **definable** in \mathcal{S} if it is contained in some \mathcal{S}_n . Let $D \subseteq \mathcal{S}_n$. A function $f : D \rightarrow \mathbb{R}^m$ is said to be **definable** in \mathcal{S} if its graph, $\Gamma(f) \stackrel{\text{def}}{=} \{(x, f(x)) : x \in D\} \subseteq \mathbb{R}^{m+n}$, is definable in \mathcal{S} .

Note that the intersection of definable sets is definable by property (i).

Definition 3.1.3 (O-minimal structure). An **o-minimal structure** is a structure in which the following additional property holds:

- (v) The boundary of each set in \mathcal{S}_1 is a finite set of points.

The class of semialgebraic sets is an example of an o-minimal structure (see, for example, [vdD98, §2]). The main structure we will use is \mathbb{R}_{exp} , which is defined to be the smallest structure in which the real exponential function, $\exp : \mathbb{R} \rightarrow \mathbb{R}$, is definable. Observe that the function $\log(x)$ is definable in \mathbb{R}_{exp} since its graph,

$$\Gamma(\log(x)) = \{(x, \log(x)) : x \in \mathbb{R}_{>0}\} = \{(\exp(y), y) : y \in \mathbb{R}\} \subset \mathbb{R}^2,$$

is clearly definable in \mathbb{R}_{exp} .

Theorem 3.1.4 [Wil96]. *The structure \mathbb{R}_{exp} is o-minimal.*

From now on, we will call a subset of \mathbb{R}^n **definable** if it is definable in some o-minimal structure.

3.2. Weighted geometry-of-numbers

The following proposition is a version of the Principle of Lipschitz, which gives estimates for the number of lattice points in a weighted homogeneous space.

Proposition 3.2.1. *Let $R \subset \mathbb{R}^n$ be a bounded set definable in an o-minimal structure. Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice with successive minima $\lambda_1, \dots, \lambda_n$ (with respect to the origin-centered unit ball in \mathbb{R}^n). Set*

$$R(B) = B *_w R = \{B *_w x : x \in R\}.$$

Then, for sufficiently large² B ,

$$\#(\Lambda \cap R(B)) = \frac{m_L(R)}{\det \Lambda} B^{|w|} + O\left(\lambda_n \det(\Lambda)^{-1} B^{|w| - w_{\min}}\right),$$

where the implied constant depends only on R and w .

²Here, just how large *sufficiently large* is depends on the lattice Λ .

Proof. This will follow from a general version of the Principle of Lipschitz due to Barroero and Widmer [BW14, Theorem 1.3]. Since $m_L(R(B)) = B^{|\mathbf{w}|} m_L(R)$, [BW14, Theorem 1.3] gives the desired leading term. Let $V_j(R(B))$ denote the sum of the j -dimensional volumes of the orthogonal projections of $R(B)$ onto each j -dimensional coordinate subspace of \mathbb{R}^n . The error term given in [BW14, Theorem 1.3] is

$$O\left(1 + \sum_{j=1}^{n-1} \frac{V_j(R(B))}{\lambda_1 \cdots \lambda_j}\right), \tag{1}$$

where the implied constant depends only on R . In our case, one observes that $V_i(R(B)) = O(V_j(R(B)))$ for all $i \leq j$. Moreover, $V_{n-1}(R(B)) = O(\sum_{i \leq n} B^{|\mathbf{w}| - w_i}) = O(B^{|\mathbf{w}| - w_{\min}})$, where the implied constant depends only on R and \mathbf{w} . By dimension considerations, we see that if $B^{|\mathbf{w}| - w_{\min}} = O(V_i(R(B)))$, then we must have $i \geq n - 1$. From these observations, it follows that

$$O\left(1 + \sum_{j=1}^{n-1} \frac{V_j(R(B))}{\lambda_1 \cdots \lambda_j}\right) = O\left(\frac{V_{n-1}(R(B))}{\lambda_1 \cdots \lambda_{n-1}}\right).$$

By Minkowski’s second theorem [Min07] (for a more modern reference see, for example, [Cas59, p. 203]),

$$\lambda_1 \cdots \lambda_n \geq \frac{2^n}{n! \cdot m_L(\mathcal{B}_n)} \det(\Lambda),$$

where \mathcal{B}_n is the unit ball in \mathbb{R}^n . From this, we obtain the desired expression for the error term,

$$O\left(\frac{V_{n-1}(R(B))}{\lambda_1 \cdots \lambda_{n-1}}\right) = O\left(\frac{\lambda_n B^{|\mathbf{w}| - w_{\min}}}{\det(\Lambda)}\right). \quad \square$$

Definition 3.2.2 (Boxes). A (\mathbb{Z}_p^n) -**box** is a subset $\mathcal{B}_p \subset \mathbb{Z}_p^n$ for which there exist closed balls

$$\mathcal{B}_{p,j} = \{x \in \mathbb{Z}_p : |x - a_j|_p \leq b_{p,j}\} \subset \mathbb{Z}_p,$$

where $a_j \in \mathbb{Z}_p$ and $b_{p,j} \in \{p^{-k} : k \in \mathbb{Z}_{\geq 0}\}$, such that \mathcal{B}_p equals the Cartesian product $\prod_{j=1}^n \mathcal{B}_{p,j}$. Let S be a finite set of primes. An **S-box** is a subset $\mathcal{B} \subset \prod_{p \in S} \mathbb{Z}_p^n$ for which there exist \mathbb{Z}_p^n -boxes \mathcal{B}_p such that

$$\mathcal{B} = \prod_{p \in S} \mathcal{B}_p = \prod_{p \in S} \prod_{j=1}^n \mathcal{B}_{p,j}.$$

Lemma 3.2.3 (Box Lemma). *Let $\Omega_\infty \subset \mathbb{R}^n$ be a bounded subset definable in an o-minimal structure. Let S be a finite set of primes and $\mathcal{B} = \prod_{p \in S} \mathcal{B}_p$ an S-box. Then, for each $B \in \mathbb{R}_{>0}$, we have*

$$\begin{aligned} & \#\left\{x \in \mathbb{Z}^n \cap (B *_w \Omega_\infty) : x \in \prod_{p \in S} \mathcal{B}_p\right\} \\ &= \left(m_L(\Omega_\infty) \prod_{p \in S} m_p(\mathcal{B}_p)\right) B^{|\mathbf{w}|} + O\left(\max_j \left\{\prod_{p \in S} b_{p,j}^{-1}\right\} \left(\prod_{p \in S} m_p(\mathcal{B}_p)\right) B^{|\mathbf{w}| - w_{\min}}\right), \end{aligned}$$

where the implied constant depends only on Ω_∞ and \mathbf{w} .

Proof. We have that $\mathcal{B}_p = \prod_{j=1}^n \mathcal{B}_{p,j}$ with $\mathcal{B}_{p,j} = \{x \in \mathbb{Z}_p : |x - a_j|_p \leq b_{p,j}\}$, where $a_j \in \mathbb{Z}_p$ and $b_{p,j} \in \{p^{-k} : k \in \mathbb{Z}_{\geq 0}\}$. Observe that for each $j \in \{1, \dots, n\}$, the set $\mathbb{Z} \cap \mathcal{B}_{p,j}$ is a translate of the

sublattice $\langle b_{p,j}^{-1} \rangle \subseteq \mathbb{Z}$. By the Chinese Remainder Theorem, the set $\mathbb{Z} \cap \prod_{p \in S} \mathcal{B}_{p,j}$ is a translate of the sublattice $\langle \prod_{p \in S} b_{p,j}^{-1} \rangle \subseteq \mathbb{Z}$. Taking a Cartesian product, we find that the set

$$\prod_{j=1}^n \left(\mathbb{Z} \cap \prod_{p \in S} \mathcal{B}_{p,j} \right) = \mathbb{Z}^n \cap \prod_{p \in S} \mathcal{B}_p$$

is a translate of a sub-lattice of \mathbb{Z}^n whose successive minima are $\prod_{p \in S} b_{p,j}^{-1}$. In particular, the n -th successive minimum of the sublattice is

$$\max_j \left\{ \prod_{p \in S} b_{p,j}^{-1} \right\},$$

and the determinant of the sublattice is

$$\prod_{j=1}^n \prod_{p \in S} b_{p,j}^{-1} = \prod_{p \in S} m_p(\mathcal{B}_p)^{-1}.$$

The lemma then follows from Proposition 3.2.1. □

Let Λ be a free \mathbb{Z} -module of finite rank n . Set $\Lambda_\infty = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ and $\Lambda_p = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Equip Λ_∞ and Λ_p with Haar measures m_∞ and m_p , respectively, normalized so that $m_p(\Lambda_p) = 1$ for all but finitely many primes p . As $\Lambda_p \cong \mathbb{Z}_p^n$, we define a **(Λ_p)-box** to be a subset of Λ_p isomorphic to a (\mathbb{Z}_p^n) -box.

Lemma 3.2.4. *Let Λ be a free \mathbb{Z} -module of finite rank n , let $\Omega_\infty \subset \Lambda_\infty$ be a bounded definable subset, and, for each prime p in a finite subset S , let $\Omega_p = \prod_j \{x \in \mathbb{Z}_p : |x - a_{p,j}|_p \leq \omega_{p,j}\} \subset \Lambda_p$ be a (Λ_p) -box. Let $\mathbf{w} = (w_1, \dots, w_n)$ be an n -tuple of positive integers. Then,*

$$\begin{aligned} & \#\{x \in \Lambda \cap (B *_w \Omega_\infty) : x \in \Omega_p \text{ for all primes } p \in S\} \\ &= \left(\frac{m_\infty(\Omega_\infty)}{m_\infty(\Lambda_\infty/\Lambda)} \prod_{p \in S} \frac{m_p(\Omega_p)}{m_p(\Lambda_p)} \right) B^{|\mathbf{w}|} + O \left(\max_j \left\{ \prod_{p \in S} \omega_{p,j}^{-1} \right\} \left(\prod_{p \in S} \frac{m_p(\Omega_p)}{m_p(\Lambda_p)} \right) B^{|\mathbf{w}| - w_{\min}} \right), \end{aligned}$$

where the implied constant depends only on Λ , Ω_∞ , and \mathbf{w} .

Proof. Fix an isomorphism $\Lambda \cong \mathbb{Z}^n$. The measures m_∞ and m_p on Λ_∞ and Λ_p induce measures on \mathbb{R}^n and \mathbb{Z}_p^n which differ from the usual Haar measures by $m_\infty(\Lambda_\infty/\Lambda)$ and $m_p(\Lambda_p)$, respectively. It therefore suffices to prove the result in the case $\Lambda = \mathbb{Z}^n$, and $m_\infty = m_L$ and m_p are the usual Haar measures; but this case is precisely the Box Lemma (Lemma 3.2.3). □

If K is a number field of degree d over \mathbb{Q} with discriminant Δ_K , then its ring of integers \mathcal{O}_K may naturally be viewed as a rank d lattice in $K_\infty \stackrel{\text{def}}{=} \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} = \prod_{v|\infty} K_v$. This lattice has covolume $|\Delta_K|^{1/2}$ with respect to the usual Haar measure m_∞ on K_∞ (which differs from Lebesgue measure on $K_\infty \cong \mathbb{R}^{r_1+2r_2}$ by a factor of 2^{r_2}) [Neu99, Chapter I Proposition 5.2]. More generally, any nonzero integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ may be viewed as a lattice in K_∞ with covolume $N_{K/\mathbb{Q}}(\mathfrak{a})|\Delta_K|^{1/2}$. For an n -tuple of positive integers $\mathbf{w} = (w_1, \dots, w_n)$, define the lattice

$$\mathfrak{a}^{\mathbf{w}} \stackrel{\text{def}}{=} \mathfrak{a}^{w_1} \times \dots \times \mathfrak{a}^{w_n} \subset K_\infty^n,$$

where we view each \mathfrak{a}^{w_i} as a subset of K_∞ . This lattice has covolume $N_{K/\mathbb{Q}}(\mathfrak{a})^{|\mathbf{w}|} |\Delta_K|^{n/2}$. For example, in the case that $\mathfrak{a} = \mathcal{O}_K$ and $w_i = 1$ for all i , one has the lattice $\mathfrak{a}^{\mathbf{w}} = \mathcal{O}_K^n$ of covolume $|\Delta_K|^{n/2}$.

For any rational prime p , we have $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{\mathfrak{p}|p} \mathcal{O}_{K,\mathfrak{p}}$. Equip each $\mathcal{O}_{K,\mathfrak{p}}$ with the Haar measure $m_{\mathfrak{p}}$, normalized so that $m_{\mathfrak{p}}(\mathcal{O}_{K,\mathfrak{p}}) = 1$. This measure induces a measure on $\mathcal{O}_{K,\mathfrak{p}}^n$, which we will also denote by $m_{\mathfrak{p}}$. Similarly, the measure m_{∞} on K_{∞} induces a measure on K_{∞}^n , which we will denote by m_{∞} .

For $v \in \text{Val}_0(K)$ a finite place, let q_v denote the size of the residue field $\mathcal{O}_K/\mathfrak{p}_v$. Let $\mathfrak{a}_{\mathfrak{p}}$ denote the image of \mathfrak{a} in $\mathcal{O}_{K,\mathfrak{p}}$.

Definition 3.2.5 (Local condition). An **(affine) local condition** at a finite place $v \in \text{Val}_0(K)$ will refer to a subset $\Omega_v \subseteq \mathcal{O}_{K,\mathfrak{p}_v}^n$. We call a local condition Ω_v **irreducible** if it is an $(\mathcal{O}_{K,\mathfrak{p}_v}^n)$ -box – that is, if there exist $a_j \in \mathcal{O}_{K,\mathfrak{p}_v}$ and $\omega_j \in \{q_v^{-k} : k \in \mathbb{Z}_{\geq 0}\}$ such that $\Omega_v = \prod_j \{x \in \mathcal{O}_{K,\mathfrak{p}_v} : |x - a_j|_v \leq \omega_j\} \subset \mathcal{O}_{K,\mathfrak{p}_v}^n$.

Remark 3.2.6. Though our results will mostly concern irreducible local conditions, by taking unions and complements, one can easily extend these results to many other local conditions.

We now apply Lemma 3.2.4 to the rank nd lattice \mathfrak{a}^w , and with the (nd) -tuple of weights $\tilde{w} = (w_1, \dots, w_1, w_2, \dots, w_2, \dots, w_n, \dots, w_n)$, obtained by repeating each of the weights in the n -tuple w exactly d times. Observing that $|\tilde{w}| = d|w|$ and $\tilde{w}_{\min} = w_{\min}$, we obtain the following proposition:

Proposition 3.2.7. Let $\Omega_{\infty} \subset K_{\infty}^n$ be a bounded definable subset. Let S be a finite set of prime ideals of \mathcal{O}_K . For each $\mathfrak{p} \in S$, let $\Omega_{\mathfrak{p}} = \prod_j \{x \in \mathcal{O}_{K,\mathfrak{p}} : |x - a_{\mathfrak{p},j}|_{\mathfrak{p}} \leq \omega_{\mathfrak{p},j}\} \subset \mathcal{O}_{K,\mathfrak{p}}^n$ be an irreducible local condition. Then,

$$\#\{x \in \mathfrak{a}^w \cap (B *_{\mathfrak{w}} \Omega_{\infty}) : x \in \Omega_{\mathfrak{p}} \text{ for all primes } \mathfrak{p} \in S\} = \kappa B^{d|w|} + O\left(\epsilon B^{d|w| - w_{\min}}\right),$$

where

$$\begin{aligned} \kappa &= \frac{m_{\infty}(\Omega_{\infty})}{N_{K/\mathbb{Q}}(\mathfrak{a})^{|\mathfrak{w}|} |\Delta_K|^{n/2}} \left(\prod_{\mathfrak{p} \in S} \frac{m_{\mathfrak{p}}(\Omega_{\mathfrak{p}} \cap \mathfrak{a}_{\mathfrak{p}}^w)}{m_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}}^w)} \right), \\ \epsilon &= \max_j \left\{ \prod_{\mathfrak{p} \in S} \omega_{\mathfrak{p},j}^{-1} \right\} \left(\prod_{\mathfrak{p} \in S} \frac{m_{\mathfrak{p}}(\Omega_{\mathfrak{p}} \cap \mathfrak{a}_{\mathfrak{p}}^w)}{m_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}}^w)} \right), \end{aligned}$$

and where the implied constant depends only on K , Ω_{∞} and w .

4. Counting points on weighted projective stacks

In this section, we prove our results for counting points of bounded height on weighted projective stacks.

Definition 4.0.1 (Local condition). A **(projective) local condition** at a place $v \in \text{Val}(K)$ will refer to a subset $\Omega_v \subseteq \mathcal{P}(w)(K_v)$.

For a projective local condition $\Omega_v \subseteq \mathcal{P}(w)(K_v)$, we denote the affine cone of Ω_v by $\Omega_v^{\text{aff}} \subseteq (\mathbb{A}^{n+1} - \{0\})(K_v)$ (i.e., Ω_v^{aff} is the preimage of Ω with respect to the map $(\mathbb{A}^{n+1} - \{0\}) \rightarrow \mathcal{P}(w)$). For $v \in \text{Val}_0(K)$, the set $\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,\mathfrak{p}_v}^{n+1}$ is an affine local condition, but not an irreducible affine local condition (see Definition 3.2.5).

Example 4.0.2. Let $v \in \text{Val}_0(K)$ be a finite place. Consider the projective local condition

$$\Omega_v = \{[a : b] \in \mathcal{P}(1, 1)(K_v) : v(a) = 0, v(b) = 1\}.$$

Then,

$$\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^2 = \{(\lambda a, \lambda b) \in \mathcal{O}_{K,v}^2 : v(a) = 0, v(b) = 1, \lambda \in K_v^{\times}\}.$$

Though this is not an irreducible affine local condition, it contains the irreducible affine local condition

$$\Omega_{v,0}^{\text{aff}} \stackrel{\text{def}}{=} \{(a, b) \in \mathcal{O}_{K,v}^2 : v(a) = 0, v(b) = 1\}.$$

Letting π_v be a uniformizer of $\mathcal{O}_{K,v}$, we have

$$\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^2 = \bigcup_{t \geq 0} \left(\pi_v^t *_{(1,1)} \Omega_{v,0}^{\text{aff}} \right),$$

where $\pi_v^t *_{(1,1)} \Omega_{v,0}^{\text{aff}}$ is an irreducible affine local condition for each t .

This example motivates the following definition:

Definition 4.0.3 (Irreducible projective local condition). A projective local condition $\Omega_v \subseteq \mathcal{P}(\mathbf{w})(K_v)$ is said to be **irreducible** if there exists an irreducible affine local condition $\Omega_{v,0}^{\text{aff}}$ such that

$$\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1} = \bigcup_{t \geq 0} \left(\pi_v^t *_{\mathbf{w}} \Omega_{v,0}^{\text{aff}} \right).$$

In analogy to the archimedean setting, for any ideal $\mathfrak{a}_v \subseteq \mathcal{O}_{K,v}$, set

$$\mathfrak{a}_v^{\mathbf{w}} \stackrel{\text{def}}{=} \mathfrak{a}_v^{w_0} \times \cdots \times \mathfrak{a}_v^{w_n} \subset K_v^{n+1}.$$

Proposition 4.0.4. Let $\Omega_v \subseteq \mathcal{P}(\mathbf{w})(K_v)$ be a nontrivial irreducible projective local condition with

$$\Omega_{v,0}^{\text{aff}} = \prod_{j=0}^n \{x \in \mathcal{O}_{K,v} : |x - a_j|_v \leq \omega_j\}.$$

For $t \in \mathbb{Z}_{\geq 0}$, set $\Omega_{v,t}^{\text{aff}} = \pi_v^t *_{\mathbf{w}} \Omega_{v,0}^{\text{aff}}$. Then we have the following:

- (a) There exists a j for which $|a_j|_v > \omega_j$.
- (b) For $t \neq s$, we have $\Omega_{v,t}^{\text{aff}} \cap \Omega_{v,s}^{\text{aff}} = \emptyset$.
- (c) For $s, t \in \mathbb{Z}_{\geq 0}$ with $s < t$, we have $\Omega_{v,s}^{\text{aff}} \cap (\pi_v^t)^{\mathbf{w}} = \emptyset$.

Proof. (a) We first prove the contrapositive of part (a). Suppose that $|a_j|_v \leq \omega_j$ for all j . If each $\omega_j = 1$, then $\Omega_{v,0}^{\text{aff}} = \mathcal{O}_{K,v}^{n+1} = \Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1}$, but then $\Omega_v = \mathcal{P}(\mathbf{w})(K_v)$ would be the trivial projective local condition. Therefore, there must exist an index j for which $\omega_j \neq 1$. By possibly reordering, we may assume $\omega_1 \neq 1$. As $|a_1|_v \leq \omega_1 < 1$, we have that $|1 - a_1|_v = 1 > \omega_1$ (by the ultrametric triangle inequality). Let $b \in \mathcal{O}_{K,v} - \{0\}$ be such that $|b - a_1|_v \leq \omega_1$. Then $(b, 0, \dots, 0)$ and $(1, 0, \dots, 0)$ are points in the affine cone $K_v^{n+1} - \{0\}$ of $\mathcal{P}(\mathbf{w})(K_v)$, each above the point $[1 : 0 : \dots : 0] \in \mathcal{P}(\mathbf{w})(K_v)$, but only one is contained in Ω_v^{aff} . We conclude that Ω_v^{aff} cannot be the entire subset of the affine cone above a projective local condition.

(b) We now show that if $|a_j|_v > \omega_j$ for some j , then for $t \neq s$, we have $\Omega_{v,t}^{\text{aff}} \cap \Omega_{v,s}^{\text{aff}} = \emptyset$. Observe that

$$\Omega_{v,t}^{\text{aff}} = \prod_{j=0}^n \{x \in \mathcal{O}_{K,v} : |x - \pi_v^{tw_j} a_j|_v \leq q_v^{-tw_j} \omega_j\}$$

is a product of v -adic balls centered at $\pi_v^{tw_j} a_j$ with radius $q_v^{-tw_j} \omega_j$. Without loss of generality, we may assume $s < t$. Using $|a_j|_v > \omega_j$, we have that

$$|\pi_v^{tw_j} a_j - \pi_v^{sw_j} a_j|_v = q_v^{-sw_j} \cdot |a_j|_v > q_v^{-sw_j} \omega_j > q_v^{-tw_j} \omega_j.$$

In particular, the distance between the centers of the balls

$$\{x \in \mathcal{O}_{K,v} : |x - \pi_v^{tw_j} a_j|_v \leq q_v^{-tw_j} \omega_j\} \text{ and } \{x \in \mathcal{O}_{K,v} : |x - \pi_v^{sw_j} a_j|_v \leq q_v^{-sw_j} \omega_j\}$$

is larger than either of the radii, and thus, the balls must be disjoint (since we are in an ultrametric space).

(c) We will show that if $\Omega_{v,s}^{\text{aff}} \cap (\pi_v^t)^{\mathbf{w}}$ is nonempty, then Ω_v is not a projective local condition. Let $y = (y_0, \dots, y_n) \in \Omega_{v,s}^{\text{aff}} \cap (\pi_v^t)^{\mathbf{w}}$ and let $y' = (y'_0, \dots, y'_n) \in \mathcal{O}_{K,v}^{n+1}$ be such that $y = \pi_v^t *_w y'$. It will suffice to show that y' is not in Ω_v^{aff} .

By part (a), we may choose j to be such that $|a_j|_v > \omega_j$. From this, together with the fact that $y_j \in \pi_v^{tw_j}$ satisfies $|y_j - \pi_v^{sw_j} a_j|_v \leq q_v^{-sw_j} \omega_j$, implies that we must have $|y_j|_v = q_v^{-sw_j} |a_j|_v$. Therefore, $|y'_j|_v = q_v^{(t-s)w_j} |a_j|_v$. Since $s < t$, this implies that $|y'_j|_v \neq |\pi_v^{rw_j} a_j|_v$ for any $r \in \mathbb{Z}_{\geq 0}$, and thus, y' is not contained in $\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1} = \bigcup_t \Omega_{v,t}^{\text{aff}}$. □

For any set of projective local conditions $(\Omega_v)_v$, define the sets

$$\begin{aligned} \Omega &\stackrel{\text{def}}{=} \{x \in \mathcal{P}(\mathbf{w})(K) : x \in \Omega_v \text{ for all } v \in \text{Val}(K)\}, \\ \Omega_\infty &\stackrel{\text{def}}{=} \{x \in \mathcal{P}(\mathbf{w})(K) : x \in \Omega_v \text{ for all } v \in \text{Val}_\infty(K)\}, \\ \Omega_0 &\stackrel{\text{def}}{=} \{x \in \mathcal{P}(\mathbf{w})(K) : x \in \Omega_v \text{ for all } v \in \text{Val}_0(K)\}. \end{aligned}$$

Set $\varpi_{K,\mathbf{w}} \stackrel{\text{def}}{=} \varpi_K / \gcd(\varpi_K, w_0, \dots, w_n)$, where we recall that ϖ_K is the number of roots of unity in K .

Theorem 4.0.5. *Let K be a degree d number field over \mathbb{Q} . Let $S \subset \text{Val}_0(K)$ be a finite set of finite places. For each $v \in \text{Val}_\infty(K) \cup S$, let $\Omega_v \subset \mathcal{P}(\mathbf{w})(K_v)$ be a projective local condition. Suppose that $\Omega_\infty^{\text{aff}}$ is a bounded definable subset of K_∞^{n+1} and that Ω_v is irreducible for all $v \in S$ with*

$$\Omega_{v,0}^{\text{aff}} = \prod_{j=0}^n \{x \in \mathcal{O}_{K,v} : |x - a_{v,j}|_v \leq \omega_{v,j}\},$$

where $a_{v,j} \in \mathcal{O}_{K,v}$ and $\omega_{v,j} \in \{q_v^{-k} : k \in \mathbb{Z}_{\geq 0}\}$ (see Definitions 4.0.3 and 3.2.5). Then,

$$\#\{x \in \mathcal{P}(\mathbf{w})(K) : Ht_{\mathbf{w}}(x) \leq B, x \in \Omega\} = \kappa B^{|\mathbf{w}|} + \begin{cases} O(\epsilon_\Omega B \log(B)) & \text{if } \mathbf{w}=(1,1) \\ & \text{and } K=\mathbb{Q}, \\ O(\epsilon_\Omega B^{\frac{d|\mathbf{w}|-w_{\min}}{d}}) & \text{else,} \end{cases}$$

where the leading coefficient is

$$\kappa = \kappa_\Omega \frac{h_K (2^{r_1+r_2} \pi^{r_2})^{n+1} R_K |\mathbf{w}|^{r_1+r_2-1}}{\varpi_{K,\mathbf{w}} |\Delta_K|^{(n+1)/2} \zeta_K(|\mathbf{w}|)},$$

where

$$\kappa_\Omega = \prod_{v|\infty} \frac{m_v(\{x \in \Omega_v^{\text{aff}} : Ht_{\mathbf{w},v}(x) \leq 1\})}{m_v(\{x \in K_v^{n+1} : Ht_{\mathbf{w},v}(x) \leq 1\})} \prod_{v \in S} m_v(\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1}),$$

where the factor in the error term is

$$\epsilon_\Omega = \sum_{t=0}^\infty \max_j \left\{ \prod_{v \in S} \frac{N_{K/\mathbb{Q}}(\mathfrak{p}_v)^{tw_j}}{\omega_{v,j}} \right\} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p}_v)^{t|\mathbf{w}|}} \prod_{v \in S} m_v(\Omega_{v,0}^{\text{aff}}),$$

and where the implied constant is independent of the local conditions Ω_v with $v \in S$.

Proof. Let $\mathfrak{c}_1, \dots, \mathfrak{c}_h$ be a set of integral ideal representatives of the ideal class group of K . Then, we get the following partition of $\mathcal{P}(\mathbf{w})(K)$ into points whose scaling ideals are in the same ideal class:

$$\mathcal{P}(\mathbf{w})(K) = \bigsqcup_{i=1}^h \{x \in \mathcal{P}(\mathbf{w})(K) : [\mathfrak{S}_{\mathbf{w}}(x)] = [\mathfrak{c}_i]\}.$$

This is well defined since the ideal class of a scaling ideal $[\mathfrak{S}_w(x)]$ does not depend on the representative of x [Den98, Proposition 3.3].

For each $\mathfrak{c} \in \{\mathfrak{c}_1, \dots, \mathfrak{c}_h\}$, consider the counting function

$$M(\Omega, \mathfrak{c}, B) \stackrel{\text{def}}{=} \#\{x \in \mathcal{P}(\mathbf{w})(K) : \text{Ht}_w(x) \leq B, [\mathfrak{S}_w(x)] = [\mathfrak{c}], x \in \Omega\}.$$

Note that

$$\#\{x \in \mathcal{P}(\mathbf{w})(K) : \text{Ht}_w(x) \leq B, x \in \Omega\} = \sum_{i=1}^h M(\Omega, \mathfrak{c}_i, B).$$

Following Schanuel [Sch79], we shall find an asymptotic for $M(\Omega, \mathfrak{c}, B)$ by counting integral points in affine space and then moding out by an action of the unit group, followed by an action of principal ideals.

Consider the (weighted) action of the unit group \mathcal{O}_K^\times on $K^{n+1} - \{0\}$ given by

$$u *_{\mathbf{w}} (x_0, \dots, x_n) = (u^{w_0}x_0, \dots, u^{w_n}x_n),$$

and let $(K^{n+1} - \{0\})/\mathcal{O}_K^\times$ denote the corresponding set of orbits. Let Ω^{aff} be the affine cone of Ω . We may describe $M(\Omega, \mathfrak{c}, B)$ in terms of \mathcal{O}_K^\times -orbits of an affine cone. In particular, there is a bijection between

$$\{[x_0 : \dots : x_n] \in \mathcal{P}(\mathbf{w})(K) : \text{Ht}_w(x) \leq B, [\mathfrak{S}_w(x)] = [\mathfrak{c}], x \in \Omega\}$$

and

$$\left\{ [(x_0, \dots, x_n)] \in (K^{n+1} - \{0\})/\mathcal{O}_K^\times : \frac{\text{Ht}_{w,\infty}(x)}{N_{K/\mathbb{Q}}(\mathfrak{c})} \leq B, \mathfrak{S}_w(x) = \mathfrak{c}, x \in \Omega^{\text{aff}} \right\}$$

given by

$$[x_0 : \dots : x_n] \mapsto [(x_0, \dots, x_n)],$$

and therefore,

$$M(\Omega, \mathfrak{c}, B) = \#\left\{ x \in (K^{n+1} - \{0\})/\mathcal{O}_K^\times : \frac{\text{Ht}_{w,\infty}(x)}{N_{K/\mathbb{Q}}(\mathfrak{c})} \leq B, \mathfrak{S}_w(x) = \mathfrak{c}, x \in \Omega^{\text{aff}} \right\}.$$

Our general strategy will be to first find an asymptotic for the counting function

$$M'(\Omega, \mathfrak{c}, B) \stackrel{\text{def}}{=} \#\left\{ x \in (K^{n+1} - \{0\})/\mathcal{O}_K^\times : \frac{\text{Ht}_{w,\infty}(x)}{N_{K/\mathbb{Q}}(\mathfrak{c})} \leq B, \mathfrak{S}_w(x) \subseteq \mathfrak{c}, x \in \Omega^{\text{aff}} \right\}$$

and then use Möbius inversion to obtain an asymptotic formula for $M(\Omega, \mathfrak{c}, B)$.

We are now going to construct a fundamental domain for the (\mathbf{w} -weighted) action of the unit group \mathcal{O}_K^\times on $K^{n+1} - \{0\}$. This will be done using Dirichlet’s Unit Theorem. Let $\varpi(K)$ denote the set of roots of unity in K .

Theorem 4.0.6 (Dirichlet’s Unit Theorem). *The image Λ of the map*

$$\begin{aligned} \lambda: \mathcal{O}_K^\times &\rightarrow \mathbb{R}^{r_1+r_2} \\ u &\mapsto (\log |u|_v)_{v \in \text{Val}_\infty(K)} \end{aligned}$$

is a rank $r \stackrel{\text{def}}{=} r_1 + r_2 - 1$ lattice in the hyperplane H defined by $\sum_{v \in \text{Val}_\infty(K)} x_v = 0$ and $\ker(\lambda) = \varpi(K)$.

For each $v \in \text{Val}_\infty(K)$, define a map

$$\eta_v : K_v^{n+1} - \{0\} \rightarrow \mathbb{R}$$

$$(x_0, \dots, x_n) \mapsto \log \max_i |x_i|_v^{1/w_i}.$$

Combine these maps to obtain a single map

$$\eta : \prod_{v \in \text{Val}_\infty(K)} (K_v^{n+1} - \{0\}) \rightarrow \mathbb{R}^{r_1+r_2}$$

$$x \mapsto (\eta_v(x_v)).$$

Let H be the hyperplane in Dirichlet’s unit theorem, and let

$$\text{pr} : \mathbb{R}^{r_1+r_2} \rightarrow H$$

be the projection along the vector $(d_v)_{v \in \text{Val}_\infty(K)}$, where $d_v = 1$ if v is real and $d_v = 2$ if v is complex. More explicitly,

$$(\text{pr}(x))_v = x_v - \left(\frac{1}{d} \sum_{v' \in \text{Val}_\infty(K)} x_{v'} \right) d_v.$$

The reason for choosing this projection is to ensure that a certain expanding region (which we are about to construct) will be weighted homogeneous (see Lemma 4.0.7).

Let $\{u_1, \dots, u_r\}$ be a basis for the image of \mathcal{O}_K^\times in the hyperplane H , and let $\{\check{u}_1, \dots, \check{u}_r\}$ be the dual basis. Then the set

$$\tilde{\mathcal{F}} \stackrel{\text{def}}{=} \{y \in H : 0 \leq \check{u}_j(y) < 1 \text{ for all } j \in \{1, \dots, r\}\}$$

is a fundamental domain for H modulo Λ , and $\mathcal{F} \stackrel{\text{def}}{=} (\text{pr} \circ \eta)^{-1} \tilde{\mathcal{F}}$ is a fundamental domain for the (\mathbf{w} -weighted) action of \mathcal{O}_K^\times on $\prod_{v \in \text{Val}_\infty(K)} (K_v^{n+1} - \{0\})$.

Define the sets

$$\mathcal{D}(B) \stackrel{\text{def}}{=} \left\{ x \in \prod_{v \in \text{Val}_\infty(K)} (K_v^{n+1} - \{0\}) : \text{Ht}_{\mathbf{w}, \infty}(x) \leq B \right\}$$

and $\mathcal{F}(B) \stackrel{\text{def}}{=} \mathcal{F} \cap \mathcal{D}(B)$. The sets $\mathcal{D}(B)$ are \mathcal{O}_K^\times -stable, in the sense that if $u \in \mathcal{O}_K^\times$ and $x \in \mathcal{D}(B)$, then $u *_{\mathbf{w}} x \in \mathcal{D}(B)$; this can be seen by the following computation:

$$\begin{aligned} \text{Ht}_{\mathbf{w}, \infty}(u *_{\mathbf{w}} x) &= \prod_{v|\infty} \max_i |u^{w_i} x_{v,i}|_v^{1/w_i} \\ &= \prod_{v|\infty} |u|_v \prod_{v|\infty} \max_i |x_{v,i}|_v^{1/w_i} \\ &= \prod_{v|\infty} \max_i |x_{v,i}|_v^{1/w_i} \\ &= \text{Ht}_{\mathbf{w}, \infty}(x). \end{aligned}$$

Similarly, for any $t \in \mathbb{R}$, we have that

$$\text{Ht}_{\mathbf{w}, \infty}(t *_{\mathbf{w}} x) = \prod_{v|\infty} \max_i |t^{w_i} x_{v,i}|_v^{1/w_i} = \prod_{v|\infty} |t|_v \prod_{v|\infty} \max_i |x_{v,i}|_v^{1/w_i} = |t|^d \text{Ht}_{\mathbf{w}, \infty}(x).$$

This shows that $\mathcal{D}(B) = B^{1/d} \mathcal{D}(1)$ for all $B > 0$.

However, \mathcal{F} is stable under the weighted action of $t \in \mathbb{R}^\times$, in the sense that $t *_{\mathbf{w}} \mathcal{F} = \mathcal{F}$. To see this, note that for any $x \in \prod_{v|\infty} (K_v^{n+1} - \{0\})$,

$$\eta(t *_{\mathbf{w}} x) = (d_v)_{v|\infty} \log(|t|) + \eta(x).$$

Since the projection pr is linear and annihilates the vector $(d_v)_{v|\infty}$, we have that

$$\text{pr} \circ \eta(t *_{\mathbf{w}} x) = \text{pr} \circ \eta(x),$$

as desired. From our observations, we obtain the following lemma:

Lemma 4.0.7. *The regions $\mathcal{F}(B)$ are weighted homogeneous, in the sense that $\mathcal{F}(B) = B^{1/d} *_{\mathbf{w}} \mathcal{F}(1)$ for all $B > 0$.*

We are now going to count lattice points in $\mathcal{F}(B)$. In [Sch79], this is done by using the classical Principle of Lipschitz [Dav51] (see also [Lan94, VI §2 Theorem 2]). One of the cruxes of Schanuel’s argument is verifying that a fundamental domain (analogous to our $\mathcal{F}(1)$) has Lipschitz parameterizable boundary, so that he can apply the Principle of Lipschitz. Though one can modify this part of Schanuel’s argument to work in our case, we will instead take a slightly different route, using an o-minimal version of the Principle of Lipschitz (Proposition 3.2.1). This allows one to give a more streamlined proof of this part of Schanuel’s argument, which may be useful in future generalizations.

Lemma 4.0.8. *The set $\mathcal{F}(1)$ is bounded.*

Proof. Let $\tilde{H} \subset \prod_{v|\infty} \mathbb{R}_v$ be the subset defined by $\sum_{v|\infty} x_v \leq 0$. Note that $\mathcal{F}(1) = \eta^{-1}(\tilde{H} \cap \text{pr}^{-1}(\tilde{\mathcal{F}}))$. It follows from the definition of η that, in order to show $\mathcal{F}(1)$ is bounded, it suffices to show that the set

$$S \stackrel{\text{def}}{=} \tilde{H} \cap \text{pr}^{-1}(\tilde{\mathcal{F}}) \subset \mathbb{R}^{r_1+r_2}$$

is bounded above (i.e., there exist constants $c_1, \dots, c_{r_1+r_2}$ such that for each

$$x = (x_1, \dots, x_{r_1+r_2}) \in S,$$

we have $x_i \leq c_i$ for all i). For this, note that any $x \in S$ can be written as

$$x = \text{pr}(x) + (d_v)_v \frac{1}{d} \sum_{v'|\infty} x_{v'},$$

and thus, the components of S are bounded above, noting that the first term, $\text{pr}(x)$, has components bounded above, and the second term has negative components. □

Lemma 4.0.9. *The set $\mathcal{F}(1)$ is definable in \mathbb{R}_{exp} .*

Proof. We make the following straightforward observations:

- The product $\prod_{v|\infty} (K_v^{n+1} - \{0\})$, viewed as a subset of $\mathbb{R}^{(r_1+2r_2)(n+1)}$, is semi-algebraic since it is clearly the complement of a semi-algebraic set.
- The set $\mathcal{D}(1)$ is semi-algebraic.
- The set

$$\begin{aligned} \mathcal{F} &= \left\{ x \in \prod_{v|\infty} (K_v^{n+1} - \{0\}) : \text{pr} \circ \eta(x) \in \tilde{\mathcal{F}} \right\} \\ &= \left\{ x \in \prod_{v|\infty} (K_v^{n+1} - \{0\}) : 0 \leq \check{u}_j \left(\log(\max_i |x_i|_v^{1/w_i}) - d_v \left(\frac{1}{d} \sum_{v'|\infty} \log(\max_i |x_i|_{v'}^{1/w_i}) \right) \right) < 1 \forall j \right\} \end{aligned}$$

is definable in \mathbb{R}_{exp} since it can be described in terms of polynomials and log, and log is definable in \mathbb{R}_{exp} (as observed in Subsection 3.1).

It follows that the intersection $\mathcal{F}(1) = \mathcal{F} \cap \mathcal{D}(1)$ is definable in \mathbb{R}_{exp} . □

We now analyze $M'(\Omega, \mathfrak{c}, B)$. Note that if $\mathfrak{S}_{\mathbf{w}}(x) \subseteq \mathfrak{c}$, then we must have that x is contained in the lattice

$$\mathfrak{c}^{\mathbf{w}} = \mathfrak{c}^{w_0} \times \dots \times \mathfrak{c}^{w_n}.$$

Therefore, we can write $M'(\Omega, \mathfrak{c}, B)$ as

$$M'(\Omega, \mathfrak{c}, B) = \#\left\{x \in (\mathfrak{c}^{\mathbf{w}} - \{0\})/\mathcal{O}_K^\times : \frac{\text{Ht}_{\mathbf{w},\infty}(x)}{N_{K/\mathbb{Q}}(\mathfrak{c})} \leq B, x \in \Omega^{\text{aff}}\right\}.$$

We now stratify Ω . For each $t \in \mathbb{Z}_{\geq 0}$, set

$$\Omega_{v,t}^{\text{aff}} = \pi_v^t *_{\mathbf{w}} \Omega_{v,0}^{\text{aff}} = \prod_{j=0}^n \{x \in \mathcal{O}_{K,v} : |x - \pi_v^{w_j t} a_{v,j}|_v \leq q_v^{-w_j t} \omega_{v,j}\}.$$

For $\mathbf{t} = (t_v)_{v \in S} \in \mathbb{Z}_{\geq 0}^{\#S}$, set

$$\Omega_{\mathbf{t}}^{\text{aff}} \stackrel{\text{def}}{=} \{x \in \Omega^{\text{aff}} : x \in \Omega_{v,t_v}^{\text{aff}} \text{ for all } v \in S\}.$$

Since each Ω_v is irreducible, we have

$$\Omega^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1} = \bigsqcup_{\mathbf{t} \in \mathbb{Z}_{\geq 0}^{\#S}} \Omega_{\mathbf{t}}^{\text{aff}}.$$

Set

$$\epsilon_{\mathbf{t}} = \max_j \left\{ \prod_{p \in S} q_v^{t_v w_j} \omega_{v,j}^{-1} \right\} \left(\prod_{p \in S} \frac{m_p(\Omega_{v,t_v}^{\text{aff}} \cap \mathfrak{c}_p^{\mathbf{w}})}{m_p(\mathfrak{c}_p^{\mathbf{w}})} \right).$$

Note that each $\varpi(K)$ -orbit (with respect to the \mathbf{w} -weighted action) of an element of $(K - \{0\})^{n+1}$ contains $\varpi_{K,\mathbf{w}}$ elements. Thus,

$$M'(\Omega, \mathfrak{c}, B) = \sum_{\mathbf{t} \in \mathbb{Z}_{\geq 0}^{\#S}} \left(\frac{\#\{\Omega_{\mathbf{t}}^{\text{aff}} \cap \mathcal{F}(N_{K/\mathbb{Q}}(\mathfrak{c})B) \cap \mathfrak{c}^{\mathbf{w}}\}}{\varpi_{K,\mathbf{w}}} + O\left(\epsilon_{\mathbf{t}} B^{|\mathbf{w}|-w_{\min}/d}\right) \right), \tag{2}$$

where each error term accounts for the points of $M'(\Omega, \mathfrak{c}, B)$ contained in the intersection of $\Omega_{\mathbf{t}}^{\text{aff}}$ and the subvariety of the affine cone of $\mathcal{P}(\mathbf{w})(K)$ consisting of points with at least one coordinate equal to zero; by Proposition 3.2.7, this error is at most $O\left(\epsilon_{\mathbf{t}}(B^{1/d})^{d|\mathbf{w}|-w_{\min}}\right)$.

By Lemma 4.0.8 and Lemma 4.0.9, we may apply Proposition 3.2.7, with $\mathfrak{a} = \mathfrak{c}$ and the local conditions $\Omega_v^{\text{aff}} \cap \mathcal{F}(1)$ for $v|\infty$ and $\Omega_{v,t}^{\text{aff}}$ for $v \in S$. Doing so, we have

$$\#\{\Omega_{\mathbf{t}}^{\text{aff}} \cap \mathcal{F}(N_{K/\mathbb{Q}}(\mathfrak{c})B) \cap \mathfrak{c}^{\mathbf{w}}\} = \frac{m_\infty(\Omega_\infty^{\text{aff}} \cap \mathcal{F}(1))}{|\Delta_K|^{(n+1)/2}} \left(\prod_{p \in S} \frac{m_p(\Omega_{v,t_v}^{\text{aff}} \cap \mathfrak{c}_p^{\mathbf{w}})}{m_p(\mathfrak{c}_p^{\mathbf{w}})} \right) B^{|\mathbf{w}|} + O\left(\epsilon_{\mathbf{t}} B^{|\mathbf{w}|-\frac{w_{\min}}{d}}\right).$$

Let $v(\mathfrak{c})$ denote the v -adic valuation of the ideal $\mathfrak{c} \subseteq \mathcal{O}_K$ (i.e., the valuation of any (and all) embeddings of \mathfrak{c} into $\mathcal{O}_{K,v}$). By Proposition 4.0.4(c), if $t < v(\mathfrak{c})$, then $m_p(\Omega_{v,t}^{\text{aff}} \cap \mathfrak{c}_p^{\mathbf{w}}) = 0$. However, when $t \geq v(\mathfrak{c})$, we compute

$$\begin{aligned} \frac{m_{\mathfrak{p}}(\Omega_{v,t}^{\text{aff}} \cap \mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})}{m_{\mathfrak{p}}(\mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})} &= \frac{1}{m_{\mathfrak{p}}(\mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})} m_{\mathfrak{p}}\left(\prod_{j=0}^n \{x \in \mathfrak{c}_{\mathfrak{p}}^{w_j} : |x - \pi_v^{tw_j} a_j|_v \leq q_v^{-tw_j} \omega_j\}\right) \\ &= \frac{1}{m_{\mathfrak{p}}(\mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})} m_{\mathfrak{p}}\left(\prod_{j=0}^n \{x \in \mathcal{O}_{K,\mathfrak{p}} : |\pi_v^{v(c)w_j} x - \pi_v^{tw_j} a_j|_v \leq q_v^{-tw_j} \omega_j\}\right) \\ &= m_{\mathfrak{p}}\left(\Omega_{v,t-v(c)}^{\text{aff}}\right). \end{aligned}$$

By Proposition 4.0.4, we know that the $\Omega_{v,t}^{\text{aff}}$ are disjoint for distinct values of t . Therefore, summing over all $t \in \mathbb{Z}_{\geq 0}$, it follows that

$$\sum_{t \geq 0} \frac{m_{\mathfrak{p}}(\Omega_{v,t}^{\text{aff}} \cap \mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})}{m_{\mathfrak{p}}(\mathfrak{c}_{\mathfrak{p}}^{\mathfrak{w}})} = \sum_{s \geq 0} m_{\mathfrak{p}}(\Omega_{v,s}^{\text{aff}}) = m_{\mathfrak{p}}(\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1}),$$

and we obtain the asymptotic

$$M'(\Omega, \mathfrak{c}, B) = \frac{m_{\infty}(\Omega_{\infty}^{\text{aff}} \cap \mathcal{F}(1))}{\varpi_{K,\mathfrak{w}} |\Delta_K|^{(n+1)/2}} \left(\prod_{\mathfrak{p} \in S} m_{\mathfrak{p}}(\Omega_v^{\text{aff}} \cap \mathcal{O}_{K,v}^{n+1}) \right) B^{|\mathfrak{w}|} + O\left(\epsilon_{\Omega} B^{|\mathfrak{w}| - w_{\min}/d}\right). \tag{3}$$

Note that as m_{∞} is the product of measures $(m_v)_{v|\infty}$, one has

$$\frac{m_{\infty}(\Omega_{\infty}^{\text{aff}} \cap \mathcal{F}(1))}{m_{\infty}(\mathcal{F}(1))} = \prod_{v|\infty} \frac{m_v(\{x \in \Omega_v^{\text{aff}} : \text{Ht}_v(x) \leq 1\})}{m_v(\{x \in K_v^{n+1} : \text{Ht}_v(x) \leq 1\})},$$

and thus,

$$m_{\infty}(\Omega_{\infty}^{\text{aff}} \cap \mathcal{F}(1)) = m_{\infty}(\mathcal{F}(1)) \prod_{v|\infty} \frac{m_v(\{x \in \Omega_v^{\text{aff}} : \text{Ht}_v(x) \leq 1\})}{m_v(\{x \in K_v^{n+1} : \text{Ht}_v(x) \leq 1\})}. \tag{4}$$

Computing the volume of $\mathcal{F}(1)$ as in [Den98, Proposition 5.3], we obtain

$$m_{\infty}(\mathcal{F}(1)) = (2^{r_1+r_2} \pi^{r_2})^{n+1} R_K |\mathfrak{w}|^{r_1+r_2-1}.$$

This differs by a factor of $2^{(n+1)r_2}$ from Deng’s result since we are using the usual Haar measure on K_{∞} , rather than the Lebesgue measure.

Observe that the leading coefficient of the asymptotic (3) equals $\zeta_K(|\mathfrak{w}|)\kappa/h_K$, where κ is as in the statement of Theorem 4.0.5.

Note that for $x \in \mathfrak{c}^{\mathfrak{w}}$, $\mathfrak{I}_{\mathfrak{w}}(x) = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{a} \subseteq \mathcal{O}_K$. Then, $\text{Ht}_{\mathfrak{w}}(x) = \text{Ht}_{\mathfrak{w},\infty}(x)/N_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{c})$. Therefore,

$$M'(\Omega, \mathfrak{c}, B) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} M(\Omega, \mathfrak{a}\mathfrak{c}, B/N_{K/\mathbb{Q}}(\mathfrak{a})) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}(\mathfrak{a}) \leq B}} M(\Omega, \mathfrak{a}\mathfrak{c}, B/N_{K/\mathbb{Q}}(\mathfrak{a})),$$

where the inequality $N_{K/\mathbb{Q}}(\mathfrak{a}) \leq B$ comes from the fact that $M(\Omega, \mathfrak{c}, B) = 0$ if $B < 1$, since all points have height greater than or equal to 1.

Since the ideals of \mathcal{O}_K form a poset (ordered by inclusion), we may use Möbius inversion (see, for example, [Sta97, §3.7] for details about Möbius inversion for posets). Applying Möbius inversion, and using our asymptotic (3) for $M'(\Omega, \mathfrak{c}, B)$, we have that

$$\begin{aligned}
 M(\Omega, \mathfrak{c}, B) &= \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}(\mathfrak{a}) \leq B}} \mu(\mathfrak{a}) \left(\frac{\zeta_K(|\mathbf{w}|)\kappa}{h_K} \left(\frac{B}{N_{K/\mathbb{Q}}(\mathfrak{a})} \right)^{|\mathbf{w}|} + O \left(\epsilon_\Omega \left(\frac{B}{N_{K/\mathbb{Q}}(\mathfrak{a})} \right)^{|\mathbf{w}| - w_{\min}/d} \right) \right) \\
 &= \frac{\zeta_K(|\mathbf{w}|)\kappa}{h_K} B^{|\mathbf{w}|} \left(\sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \mu(\mathfrak{a}) \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^{|\mathbf{w}|}} - \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}(\mathfrak{a}) > B}} \mu(\mathfrak{a}) \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^{|\mathbf{w}|}} \right) \\
 &\quad + O \left(\epsilon_\Omega B^{|\mathbf{w}| - w_{\min}/d} \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ N_{K/\mathbb{Q}}(\mathfrak{a}) \leq B}} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^{|\mathbf{w}| - w_{\min}/d}} \right) \\
 &= \frac{\zeta_K(|\mathbf{w}|)\kappa}{h_K} B^{|\mathbf{w}|} \left(\frac{1}{\zeta_K(|\mathbf{w}|)} - O \left(B^{-|\mathbf{w}|+1} \right) \right) + \begin{cases} O(\epsilon_\Omega B \log(B)) & \text{if } \mathbf{w}=(1,1) \\ & \text{and } K=\mathbb{Q}, \\ O(\epsilon_\Omega B^{|\mathbf{w}| - w_{\min}/d}) & \text{else,} \end{cases} \\
 &= \frac{\kappa}{h_K} B^{|\mathbf{w}|} + \begin{cases} O(\epsilon_\Omega B \log(B)) & \text{if } \mathbf{w} = (1, 1) \text{ and } K = \mathbb{Q}, \\ O(\epsilon_\Omega B^{|\mathbf{w}| - w_{\min}/d}) & \text{else.} \end{cases}
 \end{aligned}$$

Summing over the h_K ideal class representatives \mathfrak{c}_i , we arrive at Theorem 4.0.5. □

5. Counting elliptic curves

In this section, we apply Theorem 4.0.5 to the moduli stack of elliptic curves.

5.1. Counting elliptic curves with a prescribed local condition

An application of Theorem 4.0.5 gives the following result:

Corollary 5.1.1. *Let $\mathcal{E}_K(B)$ denote the set of isomorphism classes of elliptic curves over K with height less than B . Then,*

$$\#\mathcal{E}_K(B) = \kappa B^{5/6} + O(B^{5/6-1/3d}),$$

where

$$\kappa = \frac{h_K (2^{r_1+r_2} \pi^{r_2})^2 R_K 10^{r_1+r_2-1} \gcd(2, \varpi_K)}{\varpi_K |\Delta_K| \zeta_K(10)}.$$

Proof. Recall that the moduli stack of elliptic curves, $\mathcal{X}_{\text{GL}_2(\mathbb{Z})}$, is isomorphic to the weighted projective stack $\mathcal{P}(4, 6)$. Also recall that the naive height on $\mathcal{X}_{\text{GL}_2(\mathbb{Z})}$ corresponds to the twelfth power of the height on $\mathcal{P}(4, 6)$ with respect to the tautological bundle (i.e., the height $\text{Ht}_{(4,6)}$). Therefore, the desired result follows from applying Theorem 4.0.5 to $\mathcal{P}(4, 6)$ with trivial local conditions (i.e., $S = \emptyset$). □

We now use Theorem 4.0.5 to count elliptic curves with a prescribed local condition.

Theorem 1.1.2. *Let K be a degree d number field, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal of norm q such that $2 \nmid q$ and $3 \nmid q$. Let \mathcal{L} be one of the local conditions listed in Table 1. Then the number of elliptic curves over K with naive height less than B and which satisfy the local condition \mathcal{L} at \mathfrak{p} is*

$$\kappa K_{\mathcal{L}} B^{5/6} + O \left(\epsilon_{\mathcal{L}} B^{\frac{5}{6} - \frac{1}{3d}} \right),$$

where

$$\kappa = \frac{h_K (2^{r_1+r_2} \pi^{r_2})^2 R_K 10^{r_1+r_2-1} \gcd(2, \varpi_K)}{\varpi_K |\Delta_K| \zeta_K(10)},$$

and where $\kappa_{\mathcal{E}}$ and $\epsilon_{\mathcal{E}}$ are as in Table 1.

Proof. Good reduction case. Note that the number of elliptic curves over \mathbb{F}_q with good reduction is

$$\#\{(a, b) \in \mathbb{F}_q \times \mathbb{F}_q : 4a^3 + 27b^2 \not\equiv 0 \pmod{q}\} = q^2 - q.$$

For each pair (a, b) in the above set, fix a lift in $\mathcal{O}_{K,v}^2$, which, by an abuse of notation, we will also denote (a, b) . Then, consider the irreducible local condition

$$\Omega_{\mathfrak{p},0}^{\text{aff}}(a, b) \stackrel{\text{def}}{=} \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - a|_v \leq \frac{1}{q}, |x_1 - b|_v \leq \frac{1}{q} \right\}.$$

We find the \mathfrak{p} -adic measure

$$m_{\mathfrak{p}}(\Omega_{\mathfrak{p},0}^{\text{aff}}(a, b)) = \frac{1}{q^2}.$$

For $t \in \mathbb{Z}_{\geq 0}$, the sets

$$\Omega_{\mathfrak{p},t}^{\text{aff}}(a, b) = \pi_v^t *_{(4,6)} \Omega_{\mathfrak{p},0}^{\text{aff}}(a, b) = \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - q^{4t} a|_v \leq \frac{1}{q^{4t+1}}, |x_1 - q^{6t} b|_v \leq \frac{1}{q^{6t+1}} \right\}$$

each have \mathfrak{p} -adic measure

$$m_{\mathfrak{p}}(\Omega_{\mathfrak{p},t}^{\text{aff}}(a, b)) = \frac{1}{q^{10t+2}}.$$

Applying Theorem 4.0.5 to each $\Omega_{\mathfrak{p},0}^{\text{aff}}(a, b)$, and summing over all the $q^2 - q$ possible (a, b) pairs, it follows that the number of elliptic curves of bounded height over K with good reduction at \mathfrak{p} is

$$\kappa_{\mathcal{E}} B^{5/6} + O\left(\epsilon B^{\frac{5}{6} - \frac{1}{3d}}\right), \tag{5}$$

where

$$\kappa_{\mathcal{E}} = \sum_{(a,b)} \sum_{t=0}^{\infty} m_{\mathfrak{p}}(\Omega_{\mathfrak{p},t}^{\text{aff}}(a, b)) = (q^2 - q) \sum_{t=0}^{\infty} \frac{1}{q^{10t+2}} = (q^2 - q) \frac{1}{q^2} \frac{q^{10}}{q^{10} - 1} = \frac{q-1}{q} \frac{q^{10}}{q^{10} - 1},$$

and

$$\epsilon = \sum_{(a,b)} \sum_{t=0}^{\infty} \max\{q^{4t+1}, q^{6t+1}\} m_{\mathfrak{p}}(\Omega_{\mathfrak{p},t}^{\text{aff}}(a, b)) = (q^2 - q) \sum_{t=0}^{\infty} \frac{q^{6t+1}}{q^{10t+2}} = \frac{q^5 - q^4}{q^4 - 1}.$$

As the error term can be rewritten as $O(qB^{\frac{5}{6} - \frac{1}{3d}})$, we may replace the coefficient ϵ in the asymptotic (5) with $\epsilon_{\mathcal{E}} = q$.

Kodaira type III* case. By Tate’s algorithm [Tat75], an elliptic curve over $K_{\mathfrak{p}}$ given in short Weierstrass form, $E : y^2 = x^3 + ax + b$, has type III* reduction if and only if $v_{\mathfrak{p}}(a) = 3$ and $v_{\mathfrak{p}}(b) \geq 5$. Observe that

$$\#\{(a, b) \in \mathcal{O}_K/\mathfrak{p}^5 \times \mathcal{O}_K/\mathfrak{p}^5 : v_{\mathfrak{p}}(a) = 3, v_{\mathfrak{p}}(b) \geq 5\} = q(q - 1).$$

For each pair (a, b) in the above set, fix a lift in $\mathcal{O}_{K,v}^2$, which, by an abuse of notation, we will also denote (a, b) . Then, consider the irreducible local condition

$$\Omega_{p,0}^{\text{aff}}(a, b) \stackrel{\text{def}}{=} \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - a|_v \leq \frac{1}{q^5}, |x_1 - b|_v \leq \frac{1}{q^5} \right\}.$$

We find that the p -adic measure of this set is

$$m_p(\Omega_{p,0}^{\text{aff}}(a, b)) = \frac{1}{q^{10}}.$$

The sets

$$\Omega_{p,t}^{\text{aff}}(a, b) = \pi_v^t *_{(4,6)} \Omega_{p,0}^{\text{aff}}(a, b) = \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - q^{4t}a|_v \leq \frac{1}{q^{4t+5}}, |x_1 - q^{6t}b|_v \leq \frac{1}{q^{6t+5}} \right\}$$

each have p -adic measure

$$m_p(\Omega_{p,t}^{\text{aff}}(a, b)) = \frac{1}{q^{10t+10}}.$$

Applying Theorem 4.0.5 to each $\Omega_{p,0}^{\text{aff}}(a, b)$, and summing over all pairs (a, b) , yields the following asymptotic for the number of elliptic curves of bounded height over K with reduction of Kodaira type III* at p :

$$\kappa_{\mathcal{L}} B^{5/6} + O\left(\epsilon B^{\frac{5}{6} - \frac{1}{3d}}\right), \tag{6}$$

where

$$\kappa_{\mathcal{L}} = \sum_{(a,b)} \sum_{t=0}^{\infty} m_p(\Omega_{p,t}^{\text{aff}}(a, b)) = q(q-1) \sum_{t=0}^{\infty} \frac{1}{q^{10t+10}} = (q^2 - q) \frac{1}{q^{10}} \frac{q^{10}}{q^{10} - 1} = \frac{q-1}{q^9} \frac{q^{10}}{q^{10} - 1},$$

and

$$\epsilon = \sum_{(a,b)} \sum_{t=0}^{\infty} \max\{q^{4t+5}, q^{6t+5}\} m_p(\Omega_{p,t}^{\text{aff}}(a, b)) = (q^2 - q) \sum_{t=0}^{\infty} \frac{q^{6t+5}}{q^{10t+10}} = \frac{q-1}{q^4 - 1}.$$

As the error term can be rewritten as $O(q^{-3} B^{\frac{5}{6} - \frac{1}{3d}})$, we may replace the coefficient ϵ in the asymptotic (6) with $\epsilon_{\mathcal{L}} = 1/q^3$.

The other cases can be proven similarly to those given above. □

We now turn to estimating the number of elliptic curves with a prescribed trace of Frobenius. For $b, c \in \mathbb{F}_q$, let $E_{b,c}$ denote the short Weierstrass model $y^2 = x^3 + bx + c$, with discriminant $\Delta(b, c) = -16(4b^3 + 27c^2)$ and trace of Frobenius $a_q(E_{b,c})$. We study the counting function

$$H(a, q) \stackrel{\text{def}}{=} \#\{(b, c) \in \mathbb{F}_q \times \mathbb{F}_q : \Delta(b, c) \neq 0, a_q(E_{b,c}) = a\}. \tag{7}$$

This function is closely related to *Hurwitz-Kronecker class numbers*, which we now recall. Let K be an imaginary quadratic field with ring of integers \mathcal{O}_K , and let \mathcal{O} be an order in K with class number $h(\mathcal{O})$. The **Hurwitz-Kronecker class number** of \mathcal{O} , denoted $H(\text{disc}(\mathcal{O}))$, is defined as

$$H(\text{disc}(\mathcal{O})) \stackrel{\text{def}}{=} \sum_{\mathcal{O}' \subset \mathcal{O}_K} \frac{h(\mathcal{O}')}{\#\mathcal{O}'^\times}. \tag{8}$$

This definition of the Hurwitz-Kronecker class number agrees with the definition given in [Len87] but is half as large as it is sometimes defined (such as in [Cox89]). Let $q = p^n$ be a power of a prime $p > 3$. Then, a beautiful result, following largely from work of Deuring [Deu41], expresses the number of elliptic curves over a finite field \mathbb{F}_q with a prescribed trace of Frobenius in terms of Hurwitz-Kronecker class numbers:

$$H(a, q) = \begin{cases} (q - 1)H(a^2 - 4q) & \text{if } |a| < 2\sqrt{q} \text{ and } p \nmid a \\ (q - 1)H(-4p) & \text{if } n \text{ is odd and } a = 0 \\ \frac{q-1}{12} \left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right) \right) & \text{if } n \text{ is even and } a^2 = 4q \\ (q - 1) \left(1 - \left(\frac{-3}{p}\right) \right) & \text{if } n \text{ is even and } a^2 = q \\ (q - 1) \left(1 - \left(\frac{-4}{p}\right) \right) & \text{if } n \text{ is even and } a = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

This formula can be derived from [Sch87, Theorem 4.6], which counts the number of isomorphism classes of elliptic curves over \mathbb{F}_q with a prescribed trace of Frobenius. From this, one can deduce formula (9) by noting that the isomorphism class of each $E_{b,c}$ contains exactly $q - 1$ elliptic curves. To see that each isomorphism class contains exactly $q - 1$ elliptic curves, note that $E_{b,c} \cong E_{d,e}$ if and only if $(d, e) = (\lambda^4 b, \lambda^6 c)$ for some $\lambda \in \mathbb{F}_q^\times$, and since $p > 3$, the pairs $(\lambda^4 b, \lambda^6 c)$ will be distinct for distinct $\lambda \in \mathbb{F}_q^\times$. (See [Cox89, Theorem 14.18] for a proof of formula (9) in the case that $q = p$ is a prime.)

Theorem 1.1.3. *Let K be a degree d number field, and let \mathfrak{p} be a prime ideal of \mathcal{O}_K of degree n above a rational prime $p > 3$. Set $q = p^n$. Let $a \in \mathbb{Z}$ be an integer satisfying $|a| \leq 2\sqrt{q}$. Then, the number of elliptic curves over K with naive height less than B , good reduction at \mathfrak{p} , and which have trace of Frobenius a at \mathfrak{p} is*

$$\kappa \kappa_{n,a} B^{5/6} + O\left(\epsilon_{n,a} B^{\frac{5}{6} - \frac{1}{3d}}\right),$$

where

$$\kappa = \frac{h_K (2^{r_1+r_2} \pi^{r_2})^2 R_K 10^{r_1+r_2-1} \gcd(2, \varpi_K)}{\varpi_K |\Delta_K| \zeta_K(10)},$$

and where $\kappa_{n,a}$ and $\epsilon_{n,a}$ are as in Table 2.

Proof. For each of the $H(a, q)$ pairs (b, c) in the set

$$\{(b, c) \in \mathbb{F}_q \times \mathbb{F}_q : \Delta(b, c) \neq 0, a_q(E_{b,c}) = a\},$$

fix a lift in $\mathcal{O}_{K,v}^2$, which, by an abuse of notation, we will also denote (b, c) . Then consider the irreducible local condition

$$\Omega_{\mathfrak{p},0}^{\text{aff}}(b, c) \stackrel{\text{def}}{=} \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - b|_v \leq \frac{1}{q}, |x_1 - c|_v \leq \frac{1}{q} \right\}.$$

We find that the \mathfrak{p} -adic measure of each of these local conditions is

$$m_{\mathfrak{p}}(\Omega_{\mathfrak{p},0}^{\text{aff}}(b, c)) = \frac{1}{q^2}.$$

More generally, for $t \in \mathbb{Z}_{\geq 0}$, the sets

$$\Omega_{\mathfrak{p},t}^{\text{aff}}(b, c) = \pi_v^t *_{(4,6)} \Omega_{\mathfrak{p},0}^{\text{aff}}(b, c) = \left\{ (x_0, x_1) \in \mathcal{O}_{K,v}^2 : |x_0 - q^{4t} b|_v \leq \frac{1}{q^{4t+1}}, |x_1 - q^{6t} c|_v \leq \frac{1}{q^{6t+1}} \right\}$$

each have p -adic measure

$$m_p(\Omega_{p,t}^{\text{aff}}(b, c)) = \frac{1}{q^{10t+2}}.$$

Applying Theorem 4.0.5 to each $\Omega_{p,0}^{\text{aff}}(b, c)$, and summing over all the $H(a, q)$ possible (b, c) pairs, it follows that the number of elliptic curves of bounded height over K with good reduction at p and trace of Frobenius a at p is

$$\kappa \kappa' B^{5/6} + O\left(\epsilon B^{\frac{5}{6} - \frac{1}{3d}}\right), \tag{10}$$

where

$$\kappa' = \sum_{(b,c)} \sum_{t=0}^{\infty} m_p(\Omega_{p,t}^{\text{aff}}(b, c)) = H(a, q) \sum_{t=0}^{\infty} \frac{1}{q^{10t+2}} = H(a, q) \frac{1}{q^2} \frac{q^{10}}{q^{10} - 1},$$

and

$$\epsilon = \sum_{(b,c)} \sum_{t=0}^{\infty} \max\{q^{4t+1}, q^{6t+1}\} m_p(\Omega_{p,t}^{\text{aff}}(b, c)) = H(a, q) \sum_{t=0}^{\infty} \frac{q^{6t+1}}{q^{10t+2}} = H(a, q) \frac{q^3}{q^4 - 1}.$$

From this, the desired asymptotics can now be derived using (9).

For example, in the case that a is an integer satisfying $|a| < 2\sqrt{q}$ and $p \nmid a$, we have that $H(a, q) = (q - 1)H(a^2 - 4q)$. Thus,

$$\kappa' = \frac{H(a, q)}{q^2} \frac{q^{10}}{q^{10} - 1} = \frac{(q - 1)H(a^2 - 4q)}{q^2} \frac{q^{10}}{q^{10} - 1} = \kappa_{n,a}$$

and

$$\epsilon = (q - 1)H(a^2 - 4q) \frac{q^3}{q^4 - 1}.$$

As the error term can be rewritten as $O\left(H(a^2 - 4q)B^{\frac{5}{6} - \frac{1}{3d}}\right)$, we may replace the coefficient ϵ in the asymptotic (10) with $\epsilon_{n,a} = H(a^2 - 4q)$. □

6. Average analytic ranks

In this section, we use our results from the previous section on counting elliptic curves with prescribed local conditions in order to give a bound for the average analytic rank of elliptic curves over number fields. Our strategy will mainly follow that of Cho and Jeong [CJ23b, CJ23a] and is related to Brumer’s strategy (see Remark 6.1.3).

6.1. *L*-functions of elliptic curves

In this subsection, we recall basic facts about *L*-functions of elliptic curves. Our exposition mostly follows [Mil02, Appendix A].

Let E be an elliptic curve of discriminant Δ_E over a number field K . For each finite place $v \in \text{Val}_0(K)$, let E_v denote the reduction of E at v , let q_v be the order of the residue field k_v of K at v , let $N_v = \#E_v(\mathbb{F}_{q_v})$, and let $a_v = q_v + 1 - N_v$. If E has bad reduction at v , set

$$b_v \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } v, \\ -1 & \text{if } E \text{ has nonsplit multiplicative reduction at } v, \\ 0 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

For each $v \in \text{Val}_0(K)$, define a polynomial $L_v(E/K, T)$ by

$$L_v(E/K, T) \stackrel{\text{def}}{=} \begin{cases} 1 - a_v T + q_v T^2 & \text{if } E \text{ has good reduction at } v, \\ 1 - b_v T & \text{if } E \text{ has bad reduction at } v. \end{cases}$$

The **Hasse–Weil L-function** $L(E/K, s)$ of E over K is defined as the Euler product

$$L(E/K, s) \stackrel{\text{def}}{=} \prod_{v \in \text{Val}_0(K)} L_v(E/K, q_v^{-s})^{-1}.$$

The logarithmic derivative of $L(E/K, s)$ is

$$\frac{L'}{L}(E/K, s) = - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) > 0}} \frac{d}{ds} (\log(1 - b_v q_v^{-s})) - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) = 0}} \frac{d}{ds} (\log(1 - a_v q_v^{-s} + q_v^{1-2s})).$$

The first sum can be rewritten as

$$- \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) > 0}} \frac{d}{ds} (\log(1 - b_v q_v^{-s})) = \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) > 0}} \frac{d}{ds} \left(\sum_{k=1}^{\infty} \frac{b_v^k}{k q_v^{ks}} \right) = - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) > 0}} \sum_{k=1}^{\infty} \frac{b_v^k \log(q_v)}{q_v^{ks}}.$$

For the second sum, factor $1 - a_v T + q_v T^2$ as $(1 - \alpha_v T)(1 - \beta_v T)$, where $\alpha_v + \beta_v = a_v$ and $\alpha_v \beta_v = q_v$. Then,

$$- \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) = 0}} \frac{d}{ds} (\log(1 - a_v q_v^{-s} + q_v^{1-2s})) = - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) = 0}} \sum_{k=1}^{\infty} \frac{(\alpha_v^k + \beta_v^k) \log(q_v)}{q_v^{ks}}.$$

We thus obtain the following expression for the logarithmic derivative of $L(E/K, s)$:

$$\frac{L'}{L}(E/K, s) = - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) > 0}} \sum_{k=1}^{\infty} \frac{b_v^k \log(q_v)}{q_v^{ks}} - \sum_{\substack{v \in \text{Val}_0(K) \\ v(\Delta_E) = 0}} \sum_{k=1}^{\infty} \frac{(\alpha_v^k + \beta_v^k) \log(q_v)}{q_v^{ks}}.$$

Define the **von Mangoldt function** on integral ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ as

$$\Lambda_K(\mathfrak{a}) \stackrel{\text{def}}{=} \begin{cases} \log(q_v) & \text{if } \mathfrak{a} = \mathfrak{p}_v^k \text{ for some } k, \\ 0 & \text{otherwise.} \end{cases}$$

For prime powers, set

$$\widehat{a}_E(\mathfrak{p}_v^k) = \begin{cases} \alpha_v^k + \beta_v^k & \text{if } E \text{ has good reduction at } \mathfrak{p}_v, \\ b_v^k & \text{if } E \text{ has bad reduction at } \mathfrak{p}_v, \end{cases}$$

and for \mathfrak{a} not a power of a prime, set $\widehat{a_E}(\mathfrak{a}) = 0$. Then our expression for the logarithmic derivative of $L(E/K, s)$ becomes

$$\frac{L'}{L}(E/K, s) = - \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a_E}(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})^s}, \tag{11}$$

where the sum is over the nonzero integral ideals of \mathcal{O}_K .

Let $\Gamma(s) \stackrel{\text{def}}{=} \int_0^\infty t^{s-1} e^{-t} dt$ be the usual gamma function. Let $\Gamma_K(s)$ be the gamma factor

$$\Gamma_K(s) \stackrel{\text{def}}{=} ((2\pi)^{-s} \Gamma(s))^{[K:\mathbb{Q}]}$$

Let $\mathfrak{f}_{E/K}$ be the conductor of E over K , and define a constant

$$A_{E/K} \stackrel{\text{def}}{=} N_{K/\mathbb{Q}}(\mathfrak{f}_{E/K}) \Delta_K^2.$$

Define the **completed Hasse–Weil L-function**, $\Lambda(E/K, s)$, as

$$\Lambda(E/K, s) \stackrel{\text{def}}{=} A_{E/K}^{s/2} \Gamma_K(s) L(E/K, s).$$

We now assume that our elliptic curve E is modular over K , so that the L -function $L(E/K, s)$ is automorphic. This implies that the Hasse–Weil conjecture holds true for E , and thus,

$$\Lambda(E/K, s) = \epsilon(E) \Lambda(E/K, 2 - s),$$

where $\epsilon(E) \in \{\pm 1\}$ is the root number. We see that the logarithmic derivative of $\Lambda(E/K, s)$ is

$$\frac{\Lambda'}{\Lambda}(E/K, s) = \frac{\log(A_{E/K})}{2} + \frac{\Gamma'_K}{\Gamma_K}(s) + \frac{L'}{L}(E/K, s) = -\frac{\Lambda'}{\Lambda}(E/K, 2 - s). \tag{12}$$

We now state the explicit formula for L -functions of elliptic curves over number fields:

Proposition 6.1.1 (Explicit Formula). *Let $\phi: \mathbb{C} \rightarrow \mathbb{C}$ be a partial function that is even and analytic in the strip $|\text{Im}(s)| \leq \frac{1}{2} + \epsilon$ for some $\epsilon > 0$, and assume that on this strip $|\phi(s)| \ll (1 + |s|)^{-(1+\delta)}$ for some $\delta > 0$ as $|\text{Re}(s)| \rightarrow \infty$. For $x \in \mathbb{R}$, assume that $\phi(x) \in \mathbb{R}$, and set*

$$\widehat{\phi}(t) \stackrel{\text{def}}{=} \int_{\mathbb{R}} \phi(x) e^{-2\pi i t x} dx,$$

the Fourier transform. Let E be a modular elliptic curve over a number field K . Suppose that the L -function $L(E/K, s)$ associated to E satisfies the Generalized Riemann Hypothesis, so that all nontrivial zeros ρ_j of $L(E/K, s)$ are of the form

$$\rho_j = 1 + i\gamma_j \text{ for some } \gamma_j \in \mathbb{R}.$$

Let $r(E) \stackrel{\text{def}}{=} \text{ord}_{s=1}(L(E/K, s))$ be the analytic rank of E . Then, we have

$$\begin{aligned} & r(E)\phi(0) + \sum_{\rho_j \neq 1} \phi(\gamma_j) \\ &= \frac{\widehat{\phi}(0)}{2\pi} \log(A_{E/K}) + \frac{1}{\pi} \int_{\mathbb{R}} \frac{\Gamma'_K}{\Gamma_K}(1 + iy) \phi(y) dy - \frac{1}{\pi} \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a_E}(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})} \cdot \widehat{\phi}\left(\frac{\log(N_{K/\mathbb{Q}}(\mathfrak{a}))}{2\pi}\right), \end{aligned}$$

where the sum on the left-hand side is over the zeros $\rho_j \neq 1$ with relevant multiplicity.

Proposition 6.1.1 is a slight generalization of [IK04, Theorem 5.12] (see also [Mes86] and [Mil02, Appendix A] for the specific case of L -functions of elliptic curves). In [IK04], the condition on the test function ϕ is that it is a Schwartz function. However, as observed in [GG07, Lemma 1], the proof of [IK04, Theorem 5.12] can be adapted to work for the set of functions ϕ satisfying the conditions in Proposition 6.1.1. We will use the following modified version of the explicit formula:

Corollary 6.1.2 (Modified Explicit Formula). *Maintaining the notation from Proposition 6.1.1 and letting X be a parameter, we have that*

$$\begin{aligned}
 & r(E)\phi(0) + \sum_{\gamma_j \neq 0} \phi\left(\gamma_j \frac{\log(X)}{2\pi}\right) \\
 &= \frac{\widehat{\phi}(0) \log(A_{E/K})}{\log(X)} - \frac{2}{\log(X)} \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a}_E(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})} \cdot \widehat{\phi}\left(\frac{\log(N_{K/\mathbb{Q}}(\mathfrak{a}))}{\log(X)}\right) + O\left(\frac{1}{\log(X)}\right).
 \end{aligned} \tag{13}$$

Proof. From the explicit formula (Proposition 6.1.1), it follows that

$$\begin{aligned}
 r(E)\phi(0) + \sum_{\gamma_j \neq 0} \phi\left(\gamma_j \frac{\log(X)}{2\pi}\right) &= \frac{\widehat{\phi}(0) \log(A_{E/K})}{\log(X)} + \frac{1}{\pi} \int_{\mathbb{R}} \frac{\Gamma'_K}{\Gamma_K}(1+iy) \phi\left(y \frac{\log(X)}{2\pi}\right) dy \\
 &\quad - \frac{2}{\log(X)} \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a}_E(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})} \cdot \widehat{\phi}\left(\frac{\log(N_{K/\mathbb{Q}}(\mathfrak{a}))}{\log(X)}\right).
 \end{aligned} \tag{14}$$

A classical estimate for the logarithmic derivative of the gamma function is

$$\left| \frac{\Gamma'}{\Gamma}(1+iy) \right| = O(\log(|y|+2)).$$

From this, and the fact that ϕ is absolutely integrable (since $|\phi(s)| \ll (1+|s|)^{-(1+\delta)}$), it follows that

$$\int_{\mathbb{R}} \frac{\Gamma'_K}{\Gamma_K}(1+iy) \phi\left(y \frac{\log(X)}{2\pi}\right) dy = O\left(\frac{1}{\log(X)}\right).$$

Substituting this into (14) gives the modified explicit formula. □

We now use the modified explicit formula to obtain an expression that bounds the analytic rank. Let E be an elliptic curve with minimal discriminant $\mathfrak{D}_{E/K}$ and of height less than or equal to X . For each such E , we have that $N_{K/\mathbb{Q}}(\mathfrak{D}_{E/K}) \ll X$, and therefore,

$$\log(N_{K/\mathbb{Q}}(\mathfrak{D}_{E/K})) \leq \log(X) + O(1).$$

But since the conductor $\mathfrak{f}_{E/K}$ divides the minimal discriminant $\mathfrak{D}_{E/K}$, one has $N_{K/\mathbb{Q}}(\mathfrak{f}_{E/K}) \leq N_{K/\mathbb{Q}}(\mathfrak{D}_{E/K})$, and thus,

$$\log(N_{K/\mathbb{Q}}(\mathfrak{f}_{E/K}))/\log(X) \leq 1 + O(1/\log X).$$

It follows that $\log(A_{E/K})/\log(X) \leq 1 + O(1/\log X)$. By Corollary 6.1.2, this observation gives the inequality

$$\begin{aligned}
 & r(E)\phi(0) + \sum_{\gamma_j \neq 0} \phi\left(\gamma_j \frac{\log(X)}{2\pi}\right) \\
 &\leq \widehat{\phi}(0) - \frac{2}{\log(X)} \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a}_E(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})} \cdot \widehat{\phi}\left(\frac{\log(N_{K/\mathbb{Q}}(\mathfrak{a}))}{\log(X)}\right) + O\left(\frac{1}{\log X}\right).
 \end{aligned}$$

We further simplify by rewriting the sum on the right-hand side as

$$\sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\widehat{a}_E(\mathfrak{a}) \Lambda_K(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})} \cdot \widehat{\phi}\left(\frac{\log(N_{K/\mathbb{Q}}(\mathfrak{a}))}{\log(X)}\right) = \sum_{v \in \text{Val}_0(K)} \sum_{k \geq 1} \frac{\widehat{a}_E(\mathfrak{p}_v^k) \log(q_v)}{q_v^k} \cdot \widehat{\phi}\left(\frac{k \log(q_v)}{\log(X)}\right).$$

By the Weil Conjectures for Elliptic curves, $|\alpha_v| = |\beta_v| = \sqrt{q_v}$ (see, for example, [Sil09, §V Theorem 2.3.1(a)]). From this, and the fact that $|b_v| \leq 1$, we have $|\widehat{a}_E(\mathfrak{p}_v^k)| \leq 2q_v^{k/2}$. Using this, we bound the $k \geq 3$ part of the sum:

$$\begin{aligned} \sum_{v \in \text{Val}_0(K)} \sum_{k \geq 3} \frac{\widehat{a}_E(\mathfrak{p}_v^k) \log(q_v)}{q_v^k} \cdot \widehat{\phi}\left(\frac{k \log(q_v)}{\log(X)}\right) &\leq \sum_{v \in \text{Val}_0(K)} \sum_{k \geq 3} \frac{2 \log(q_v)}{q_v^{k/2}} \|\widehat{\phi}\|_\infty \\ &\leq \sum_{v \in \text{Val}_0(K)} \frac{2 \log(q_v)}{q_v^{3/2} (1 - q_v^{-1/2})} \|\widehat{\phi}\|_\infty \\ &= O(1), \end{aligned}$$

where $\|f\|_\infty$ is the usual L^∞ -norm defined as

$$\|f\|_\infty \stackrel{\text{def}}{=} \inf\{a \geq 0 : m_L(\{x : |f(x)| > a\}) = 0\},$$

where m_L is the Lebesgue measure on \mathbb{R} . Also note that for any finite set of places $S \subset \text{Val}_0(K)$, we clearly have

$$\sum_{v \in S} \sum_{k=1}^2 \frac{\widehat{a}_E(\mathfrak{p}_v^k) \log(q_v)}{q_v^k} \cdot \widehat{\phi}\left(\frac{k \log(q_v)}{\log(X)}\right) = O(1).$$

Therefore, setting

$$U_k(E, \phi, X) \stackrel{\text{def}}{=} \sum_{\substack{v \in \text{Val}_0(K) \\ 2 \nmid q_v, 3 \nmid q_v}} \frac{\widehat{a}_E(\mathfrak{p}_v^k) \log(q_v)}{q_v^k} \cdot \widehat{\phi}\left(\frac{k \log(q_v)}{\log(X)}\right),$$

we have

$$r(E)\phi(0) + \sum_{\gamma_j \neq 0} \phi\left(\gamma_j \frac{\log(X)}{2\pi}\right) \leq \widehat{\phi}(0) - \frac{2}{\log(X)} (U_1(E, \phi, X) + U_2(E, \phi, X)) + O\left(\frac{1}{\log X}\right).$$

We now average over isomorphism classes of elliptic curves. For each elliptic curve E , let $\rho_{E,j} = 1 + i\gamma_{E,j}$ be the nontrivial zeros of the L-function $L(E/K, s)$. Let $\mathcal{E}_K(B)$ denote the set of isomorphism classes of elliptic curves over K with height bounded by B . Setting

$$\begin{aligned} S_k(\phi, B) &\stackrel{\text{def}}{=} \frac{2}{\log(B) \#\mathcal{E}_K(B)} \sum_{E \in \mathcal{E}_K(B)} U_k(E, \phi, B) \\ &= \frac{2}{\log(B) \#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2 \nmid q_v, 3 \nmid q_v}} \frac{\log(q_v)}{q_v^k} \cdot \widehat{\phi}\left(\frac{k \log(q_v)}{\log(B)}\right) \sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}_v^k), \end{aligned}$$

we have that

$$\begin{aligned} &\phi(0) \frac{1}{\#\mathcal{E}_K(B)} \sum_{E \in \mathcal{E}_K(B)} r(E) + \frac{1}{\#\mathcal{E}_K(B)} \sum_{E \in \mathcal{E}_K(B)} \sum_{\gamma_{E,j} \neq 0} \phi\left(\gamma_{E,j} \frac{\log(B)}{2\pi}\right) \\ &\leq \widehat{\phi}(0) - S_1(\phi, B) - S_2(\phi, B) + O\left(\frac{1}{\log(B)}\right). \end{aligned} \tag{15}$$

Remark 6.1.3. So far, we have followed the same strategy as Brumer [Bru92]. The main difficulty in estimating the $S_k(\phi, B)$ is estimating the sums of the $\widehat{a_E}(\mathfrak{p}_v^k)$. Brumer does this by relating the sums to certain exponential sums. Following Cho and Jeong [CJ23b, CJ23a], we will take a slightly different approach, instead estimating the sums using our estimates for the number of elliptic curves with a prescribed trace of Frobenius (Theorem 1.1.3).

For our applications, we shall use the test function

$$\phi(y) = \begin{cases} \left(\frac{\sin(\pi \nu y)}{2\pi y}\right)^2 & \text{if } y \neq 0, \\ \nu^2/4 & \text{if } y = 0, \end{cases}$$

whose Fourier transform is

$$\widehat{\phi}(t) = \begin{cases} \frac{1}{2} \left(\frac{\nu}{2} - \frac{|t|}{2}\right) & \text{for } |t| \leq \nu \\ 0 & \text{for } |t| > \nu. \end{cases}$$

Observe that this test function satisfies the conditions of Proposition 6.1.1 (despite not being a Schwartz function).

Our strategy will be to show that

$$-S_1(\phi, B) - S_2(\phi, B) = \frac{\phi(0)}{2} + o(1).$$

This will imply the following upper bound for the average analytic rank of elliptic curves over the number field K :

$$\frac{\widehat{\phi}(0)}{\phi(0)} + \frac{1}{2} = \frac{1}{\nu} + \frac{1}{2}.$$

6.2. Class number estimates

In this subsection, we give some estimates for the counting functions $H(a, q)$, which were defined in Subsection 5.1 equation (7). These results will be used in the next subsection.

Proposition 6.2.1. *For any $a \in \mathbb{Z}$, we have*

$$H(a, q) \ll_{\epsilon} q^{3/2+\epsilon},$$

as a function of q for any $\epsilon > 0$.

Proof. By formula (9) for $H(a, q)$, it suffices to show $H(a^2 - 4q) \ll_{\epsilon} q^{1/2+\epsilon}$ and $H(-4p) \ll_{\epsilon} q^{1/2+\epsilon}$, and for this, it will suffice to show that for all possible n , we have $H(n) \ll_{\epsilon} |n|^{1/2+\epsilon}$. As n must be the discriminant of an order in an imaginary quadratic field, it must be negative, non-square and congruent to 0 or 1 modulo 4.

Let $\text{sqf}(n)$ denote the squarefree part of n (e.g., $\text{sqf}(12) = 3$), and let $\text{sq}(n)$ be such that $n = \text{sqf}(n) \cdot \text{sq}(n)^2$ (e.g., $\text{sq}(12) = 2$). For non-square negative integers D that are congruent to

0 or 1 modulo 4, let \mathcal{O}_D denote the imaginary quadratic order of discriminant D . We can rewrite equation (8) as

$$H(n) = \sum_{\substack{d|\text{sq}(n) \\ n/d^2 \equiv 0,1 \pmod{4}}} \frac{h(\mathcal{O}_{n/d^2})}{\#\mathcal{O}_{n/d^2}^\times}.$$

Define a quadratic character

$$\begin{aligned} \chi_D : \mathbb{Z} &\rightarrow \mathbb{C}^\times \\ m &\mapsto \left(\frac{D}{m}\right). \end{aligned}$$

Observe that

$$\lim_{s \rightarrow 1} (s - 1)\zeta_{\mathcal{O}_D}(s) = \sum_{m=1}^\infty \frac{\chi_D(m)}{m} = \sum_{m=1}^\infty \chi_D(m) \int_m^\infty \frac{1}{x^2} dx. \tag{16}$$

For any positive integer $r \in \mathbb{Z}_{\geq 1}$, the Pólya–Vinogradov inequality gives

$$\left| \sum_{m=1}^r \chi_D(m) \right| \leq 2\sqrt{|D|} \log(|D|).$$

In particular, the functions $f_r(x) = \sum_{m=1}^r \chi_D(m)/x^2$ are dominated by $2\sqrt{|D|} \log(|D|)/x^2$ on $\mathbb{R}_{\geq 1}$. Therefore, by the dominated convergence theorem, we may switch the sum and integral in (16), so that

$$\sum_{m=1}^\infty \chi_D(m) \int_m^\infty \frac{1}{x^2} dx = \int_1^\infty \left(\sum_{m=1}^x \chi_D(m) \right) \frac{1}{x^2} dx.$$

Splitting this integral and again applying the Pólya–Vinogradov inequality, we find that for any $\epsilon > 0$,

$$\begin{aligned} \lim_{s \rightarrow 1} (s - 1)\zeta_{\mathcal{O}_D}(s) &= \int_1^{\sqrt{|D|}} \left(\sum_{m=1}^x \chi_D(m) \right) \frac{1}{x^2} dx + \int_{\sqrt{|D|}}^\infty \left(\sum_{m=1}^x \chi_D(m) \right) \frac{1}{x^2} dx \\ &\ll \int_1^{\sqrt{|D|}} \frac{x}{x^2} dx + \int_{\sqrt{|D|}}^\infty \frac{\sqrt{|D|} \log(|D|)}{x^2} dx \\ &\ll \log(|D|) + \log(|D|) \\ &\ll |D|^\epsilon. \end{aligned}$$

From this and the analytic class number formula [JP20, Theorem 1.1], we have the following upper bound for class numbers of orders in imaginary quadratic fields:

$$h(\mathcal{O}_D) \ll |D|^{1/2+\epsilon}.$$

Let $\tau(n)$ denote the number of divisors of n , and recall that $\tau(n) \ll_\epsilon |n|^\epsilon$ for any $\epsilon > 0$. Combining the above observations, we have

$$H(n) \leq \sum_{\substack{d|\text{sq}(n) \\ n/d^2 \equiv 0,1 \pmod{4}}} h(\mathcal{O}_{n/d^2}) \ll \tau(\text{sq}(n)) |n|^{1/2+\epsilon} \ll_\epsilon |n|^{1/2+\epsilon}. \quad \square$$

The next proposition gives estimates for certain sums involving $H(a, q)$.

Proposition 6.2.2. *Let q be a power of a prime $p > 3$. For any $\epsilon > 0$, we have the following estimates:*

$$\begin{aligned} \sum_{|a| \leq 2\sqrt{q}} H(a, q) &= q^2 - q, \\ \sum_{|a| \leq 2\sqrt{q}} aH(a, q) &= 0, \\ \sum_{|a| \leq 2\sqrt{q}} a^2H(a, q) &= q^3 + O\left(q^{\frac{5}{2} + \epsilon}\right). \end{aligned}$$

Proof. The first sum: We have that

$$\sum_{|a| \leq 2\sqrt{q}} H(a, q) = \#\{(b, c) \in \mathbb{F}_q \times \mathbb{F}_q : \Delta(b, c) \neq 0\} = q^2 - q.$$

The second sum: Pairing positive and negative terms, we have that

$$\sum_{|a| \leq 2\sqrt{q}} aH(a, q) = \sum_{0 < a \leq 2\sqrt{q}} (aH(a, q) - aH(a, q)) = 0,$$

where we have used that $H(a, q) = H(-a, q)$.

The third sum: This sum is the most subtle. As observed in Subsection 5.1, each isomorphism class of elliptic curves over \mathbb{F}_q contains exactly $q - 1$ elliptic curves, which can be thought of as the size of the orbit of an elliptic curve E with respect to the weighted $\mathbb{G}_m(\mathbb{F}_q)$ action, with weights 4 and 6. Let $\mathcal{E}_{\mathbb{F}_q}$ denote the set of isomorphism classes of elliptic curves over \mathbb{F}_q . By the orbit stabilizer theorem,

$$H(a, q) = \sum_{\substack{E \in \mathcal{E}_{\mathbb{F}_q} \\ a_q(E) = a}} \frac{q - 1}{\#\text{Aut}_{\mathbb{F}_q}(E)}.$$

Therefore, we can rewrite the third sum as

$$\sum_{|a| \leq 2\sqrt{q}} a^2H(a, q) = (q - 1) \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_{\mathbb{F}_q} \\ a_q(E) = a}} \frac{a^2}{\#\text{Aut}_{\mathbb{F}_q}(E)} = (q - 1) \sum_{E \in \mathcal{E}_{\mathbb{F}_q}} \frac{a_q(E)^2}{\#\text{Aut}_{\mathbb{F}_q}(E)}.$$

The final sum can be estimated using work of Birch [Bir68] and Ihara [Iha67], as we now explain. Write $q = p^r$. Define an indicator function

$$\delta_{2\mathbb{Z}}(r) = \begin{cases} 1 & \text{if } r \text{ is even} \\ 0 & \text{if } r \text{ is odd.} \end{cases}$$

Let $T_k(m)$ be the m -th Hecke operator on the space of weight k cusp forms of level 1, and let $\text{Tr}(T_k(m))$ denote the trace of $T_k(m)$.

The following result is due to Birch (in the $r = 1$ case) [Bir68] and Ihara (for $r > 1$) [Iha67] (see [KP17, Theorem 2]):

Theorem 6.2.3 (Birch-Ihara). *With notation as above, we have that*

$$\frac{1}{q} \sum_{E \in \mathcal{E}_{\mathbb{F}_q}} \frac{a_q(E)^2}{\#\text{Aut}_{\mathbb{F}_q}(E)}$$

equals

$$\begin{aligned} & \frac{1}{q} \left(p^3 \text{Tr}(T_4(p^{r-2})) - \text{Tr}(T_4(q)) + \frac{1}{2} \left(p^3 \sum_{i=0}^{r-2} \min\{p^i, p^{r-2-i}\}^3 - \sum_{i=0}^r \min\{p^i, p^{r-i}\}^3 \right) \right) \\ & + p \text{Tr}(T_2(p^{r-2})) - \text{Tr}(T_2(q)) + \frac{1}{2} \left(p \sum_{i=0}^{r-2} \min\{p^i, p^{r-2-i}\} - \sum_{i=0}^r \min\{p^i, p^{r-i}\} \right) \\ & + \sum_{i=0}^r p^i - p \sum_{i=0}^{r-2} p^i. \end{aligned}$$

We now show that for any $\epsilon > 0$,

$$\sum_{E \in \mathcal{E}_{\mathbb{F}_q}} \frac{a_q(E)^2}{\#\text{Aut}_{\mathbb{F}_q}(E)} = q^2 + O(q^{3/2+\epsilon}).$$

Using the Ramanujan–Peterson–Deligne bound for Hecke eigenvalues [Del74], one can show that for any prime power p^s and any $\epsilon > 0$,

$$\text{Tr}(T_k(p^s)) \ll_k p^{s(k-1)/2} \ll_k p^{s((k-1)/2+\epsilon)}$$

(see, for example, the introduction of [Pet18]). In particular,

$$p^3 \text{Tr}(T_4(p^{r-2})) - \text{Tr}(T_4(q)) \ll p^3 p^{(r-2)(3/2+\epsilon)} + q^{3/2+\epsilon} \ll q^{3/2+\epsilon}$$

and

$$p \text{Tr}(T_2(p^{r-2})) - \text{Tr}(T_2(q)) \ll p p^{(r-2)(1/2+\epsilon)} + q^{1/2+\epsilon} \ll q^{1/2+\epsilon}.$$

We now estimate the sums in Theorem 6.2.3. As a function of q , the sum $\sum_{i=0}^r \min\{p^i, p^{r-i}\}^3$ has on the order of $\log(q)$ terms, and each term is bounded above by $(p^{r/2})^3 = q^{3/2}$. Therefore,

$$\sum_{i=0}^r \min\{p^i, p^{r-i}\}^3 \ll q^{3/2} \log(q) \ll q^{3/2+\epsilon}.$$

Similar reasoning shows that

$$p^3 \sum_{i=0}^{r-2} \min\{p^i, p^{r-2-i}\}^3 \ll p^3 \log(q) p^{3(r-2)/2} \ll q^{3/2+\epsilon}.$$

We also compute

$$p \sum_{i=0}^{r-2} \min\{p^i, p^{r-2-i}\} - \sum_{i=0}^r \min\{p^i, p^{r-i}\} = - \sum_{i \in \{0,r\}} \min\{p^i, p^{r-i}\} = -2,$$

and

$$\sum_{i=0}^r p^i - p \sum_{i=0}^{r-2} p^i = \sum_{i \in \{0,r\}} p^i = 1 + q.$$

Combining the above estimates, we find that

$$\frac{1}{q} \sum_{E \in \mathcal{E}_{\mathbb{F}_q}} \frac{a_q(E)^2}{\#\text{Aut}_{\mathbb{F}_q}(E)} = O\left(\frac{q^{3/2+\epsilon}}{q}\right) + O(q^{1/2+\epsilon}) - \frac{2}{2} + (1+q) = q + O(q^{1/2+\epsilon}).$$

From this, we obtain

$$\sum_{|a| \leq 2\sqrt{q}} a^2 H(a, q) = (q-1) \left(q^2 + O(q^{3/2+\epsilon}) \right) = q^3 + O(q^{5/2+\epsilon}). \quad \square$$

6.3. Estimating $S_1(\phi, B)$ and $S_2(\phi, B)$

Lemma 6.3.1. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal of norm $N_{K/\mathbb{Q}}(\mathfrak{p}) = q$ such that $2 \nmid q$ and $3 \nmid q$. Then, for any $\epsilon > 0$, we have the following upper bound:*

$$\sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}) \ll_{\epsilon} \frac{1}{q} B^{5/6} + q^{3/2+\epsilon} B^{5/6-1/3d}.$$

Proof. Let $\mathcal{E}_K^{\text{mult}}(B)$ denote the set of elliptic curves over K of naive height bounded by B and multiplicative reduction at \mathfrak{p} . Then, we have

$$\sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}) = \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K(B) \\ a_{\mathfrak{p}}(E)=a}} \widehat{a}_E(\mathfrak{p}) + \sum_{E \in \mathcal{E}_K^{\text{mult}}(B)} \widehat{a}_E(\mathfrak{p}).$$

By Theorem 1.1.2, we have that

$$\left| \sum_{E \in \mathcal{E}_K^{\text{mult}}(B)} \widehat{a}_E(\mathfrak{p}) \right| \ll \#\mathcal{E}_K^{\text{mult}}(B) \ll \frac{1}{q} B^{5/6} + B^{5/6-1/3d}. \quad (17)$$

By Proposition 6.2.2, Proposition 6.2.1 and the proof of Theorem 1.1.3, we have that

$$\begin{aligned} \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K(B) \\ a_{\mathfrak{p}}(E)=a}} \widehat{a}_E(\mathfrak{p}) &= \sum_{|a| \leq 2\sqrt{q}} a \left(\kappa \frac{H(a, q)}{q^2} \frac{q^{10}}{q^{10}-1} B^{5/6} + O\left(q^{-1} H(a, q) B^{5/6-1/3d} \right) \right) \\ &= 0 + \sum_{|a| \leq 2\sqrt{q}} O\left(a q^{-1} H(a, q) B^{5/6-1/3d} \right) \\ &\ll \max_{|a| \leq 2\sqrt{q}} \{H(a, q)\} B^{5/6-1/3d} \\ &\ll_{\epsilon} q^{3/2+\epsilon} B^{5/6-1/3d}. \end{aligned}$$

This, together with the bound (17), implies the lemma. □

Lemma 6.3.2. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal with norm $N_{K/\mathbb{Q}}(\mathfrak{p}) = q$ such that $2 \nmid q$ and $3 \nmid q$. Then, we have the following estimate:*

$$\sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}^2) = -\kappa q B^{5/6} + O\left(q^{1/2+\epsilon} B^{\frac{5}{6}} + q^2 B^{\frac{5}{6}-\frac{1}{3d}} \right),$$

where the implied constant does not depend on q .

Proof. Let $\mathcal{E}_K^{\text{good}}(B)$ (resp. $\mathcal{E}_K^{\text{mult}}(B)$) denote the set of elliptic curves over K with good reduction (resp. multiplicative reduction) at \mathfrak{p} and height bounded by B . In this case, we have that

$$\sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}^2) = \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K^{\text{good}}(B) \\ a_{\mathfrak{p}}(E)=a}} \widehat{a}_E(\mathfrak{p}^2) + \sum_{E \in \mathcal{E}_K^{\text{mult}}(B)} \widehat{a}_E(\mathfrak{p}^2).$$

Since $\widehat{a}_E(\mathfrak{p}^2) = \widehat{a}_E(\mathfrak{p})^2 = 1$ for all $E \in \mathcal{E}_K^{\text{mult}}(B)$, we have, by Theorem 1.1.2, that

$$\left| \sum_{E \in \mathcal{E}_K^{\text{mult}}(B)} \widehat{a}_E(\mathfrak{p}^2) \right| = \#\mathcal{E}_K^{\text{mult}}(B) = \kappa \frac{q-1}{q^2} \frac{q^{10}}{q^{10}-1} B^{5/6} + O(B^{5/6-1/3d}) = O(B^{5/6}). \tag{18}$$

In the case that E has good reduction at \mathfrak{p} , a straightforward computation shows that $\widehat{a}_E(\mathfrak{p}^2)$ equals $a_{\mathfrak{p}}(E)^2 - 2q$. Therefore, by Proposition 6.2.2 and the proof of Theorem 1.1.3, we have that

$$\begin{aligned} \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K^{\text{good}}(B) \\ a_{\mathfrak{p}}(E)=a}} \widehat{a}_E(\mathfrak{p}^2) &= \sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K^{\text{good}}(B) \\ a_{\mathfrak{p}}(E)=a}} (a_{\mathfrak{p}}(E)^2 - 2q) \\ &= \sum_{|a| \leq 2\sqrt{q}} (a^2 - 2q) \left(\kappa \frac{H(a, q)}{q^2} \frac{q^{10}}{q^{10}-1} B^{5/6} + O\left(q^{-1} H(a, q) B^{5/6-1/3d}\right) \right) \\ &= \frac{\kappa q^8}{q^{10}-1} \left(\sum_{|a| \leq 2\sqrt{q}} a^2 H(a, q) - 2q \sum_{|a| \leq 2\sqrt{q}} H(a, q) \right) B^{5/6} + O\left(q^2 B^{5/6-\frac{1}{3d}}\right) \\ &= \frac{-\kappa q^{11}}{q^{10}-1} B^{5/6} + O\left(q^{1/2+\epsilon} B^{5/6} + q^2 B^{5/6-\frac{1}{3d}}\right). \end{aligned}$$

Observe that

$$\frac{q^{10}}{q^{10}-1} = \sum_{k=0}^{\infty} q^{-10k} = 1 + O(q^{-10}).$$

Therefore,

$$\sum_{|a| \leq 2\sqrt{q}} \sum_{\substack{E \in \mathcal{E}_K^{\text{good}}(B) \\ a_{\mathfrak{p}}(E)=a}} \widehat{a}_E(\mathfrak{p}^2) = -\kappa q B^{5/6} + O\left(q^{1/2+\epsilon} B^{5/6} + q^2 B^{5/6-\frac{1}{3d}}\right).$$

This, together with the bound (18), implies the lemma. □

6.4. Bounding the average analytic rank of elliptic curves

We now prove our main result.

Theorem 1.1.1. *Let K be a number field of degree d . Assume that all elliptic curves over K are modular and that their L -functions satisfy the Riemann-Hypothesis. Then the average analytic rank of isomorphism classes of elliptic curves over K , when ordered by naive height, is bounded above by $(9d + 1)/2$.*

Proof. By Lemma 6.3.1 and the observation that $\widehat{\phi}$ is supported on the interval $[-\nu, \nu]$, we have that

$$\begin{aligned} S_1(\phi, B) &= \frac{2}{\log(B)\#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v} \cdot \widehat{\phi}\left(\frac{\log(q_v)}{\log(B)}\right) \sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}_v) \\ &\ll_{\epsilon} \frac{2}{\log(B)\#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v} \cdot \widehat{\phi}\left(\frac{\log(q_v)}{\log(B)}\right) \left(\frac{1}{q_v} B^{5/6} + q_v^{3/2+\epsilon} B^{5/6-1/3d}\right) \\ &\ll \frac{2}{\log(B)\#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq B^\nu \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v} \left(\frac{1}{q_v} B^{5/6} + q_v^{3/2+\epsilon} B^{5/6-1/3d}\right). \end{aligned}$$

By Corollary 5.1.1, we know that $\#\mathcal{E}_K(B) = \kappa B^{5/6} + O(B^{5/6-1/3d})$. Using this and the prime ideal theorem, we have that

$$S_1(\phi, B) \ll_{\epsilon} \frac{2}{\log(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq B^\nu \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v} \left(\frac{1}{q_v} + q_v^{3/2+\epsilon} B^{-1/3d}\right) \ll \frac{1 + B^{(3/2+\epsilon)\nu-1/3d}}{\log(B)}. \tag{19}$$

By Lemma 6.3.2, we have

$$\begin{aligned} S_2(\phi, B) &= \frac{2}{\log(B)\#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v^2} \cdot \widehat{\phi}\left(\frac{2\log(q_v)}{\log(B)}\right) \sum_{E \in \mathcal{E}_K(B)} \widehat{a}_E(\mathfrak{p}_v^2) \\ &= \frac{2}{\log(B)\#\mathcal{E}_K(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v^2} \cdot \widehat{\phi}\left(\frac{2\log(q_v)}{\log(B)}\right) \left(-\kappa q_v B^{5/6} + O(q_v^{1/2+\epsilon} B^{5/6} + q_v^2 B^{5/6-1/3d})\right). \end{aligned}$$

Assuming $\epsilon < 1/4$ and using $\#\mathcal{E}_K(B) = \kappa B^{5/6} + O(B^{5/6-1/3d})$, we have

$$\begin{aligned} S_2(\phi, B) &= \frac{2}{\log(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v^2} \cdot \widehat{\phi}\left(\frac{2\log(q_v)}{\log(B)}\right) \left(-q_v + O(q_v^{1/2+\epsilon} + q_v^2 B^{-1/3d})\right) \\ &= \frac{-2}{\log(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ 2\uparrow q_v, 3\uparrow q_v}} \frac{\log(q_v)}{q_v} \cdot \widehat{\phi}\left(\frac{2\log(q_v)}{\log(B)}\right) + O\left(\frac{1}{\log B} \sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq B^{\nu/2}}} \left(\frac{1}{q_v^{3/2-\epsilon}} + \log(q_v) B^{-1/3d}\right)\right) \\ &= \frac{-1}{\log(B)} \sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq B^{\nu/2} \\ 2\uparrow q_v, 3\uparrow q_v}} \left(\frac{\nu \log(q_v)}{2q_v} - \frac{\log(q_v)^2}{q_v \log(B)}\right) + O\left(\frac{1 + B^{\nu/2-1/3d}}{\log(B)}\right). \end{aligned}$$

Arguments using the prime ideal theorem show that

$$\sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq X}} \frac{\log(q_v)}{q_v} = \log(X) + O(1)$$

and

$$\sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq X}} \frac{\log(q_v)^2}{q_v} = \frac{\log(X)^2}{2} + O(\log \log(X)).$$

From this, it follows that

$$\begin{aligned} & \sum_{\substack{v \in \text{Val}_0(K) \\ q_v \leq B^{v/2} \\ 2 \nmid q_v, 3 \nmid q_v}} \left(\frac{v \log(q_v)}{2q_v} - \frac{\log(q_v)^2}{q_v \log(B)} \right) \\ &= \frac{v}{2} (\log(B^{v/2}) + O(1)) - \frac{1}{\log(B)} \left(\frac{\log(B^{v/2})^2}{2} + O(\log \log(B^{v/2})) \right) \\ &= \left(\frac{v^2}{4} \log(B) + O(1) \right) - \left(\frac{v^2}{8} \log(B) + O(1) \right) \\ &= \frac{v^2}{8} \log(B) + O(1). \end{aligned}$$

Therefore,

$$S_2(\phi, B) = \frac{-\phi(0)}{2} + O\left(\frac{1 + B^{v/2-1/3d}}{\log(B)}\right).$$

Taking $v = (3d(3/2 + \epsilon))^{-1}$ and combining the above estimate for S_2 with our bound (19) for S_1 , we obtain

$$-S_1(\phi, B) - S_2(\phi, B) = \frac{\phi(0)}{2} + o(1).$$

Substituting this into (15) and taking the limit superior as B goes to infinity gives the following upper bound for the average analytic rank of elliptic curves over K :

$$\frac{1}{v} + \frac{1}{2} = 3d(3/2 + \epsilon) + \frac{1}{2},$$

for any $0 < \epsilon < 1/4$. Since the limit superior exists, and since ϵ can be taken arbitrarily small, we obtain the bound $(9d + 1)/2$. \square

Acknowledgements. The author thanks Brandon Alberts, Peter Bruin, Peter Cho, Jordan Ellenberg, Ben Kane, Irati Manterola Ayala, Steven Miller, Grant Molnar, Filip Najman, Junyeong Park, John Voight and David Zureick-Brown for helpful conversations and comments on this work. Special thanks to Bryden Cais and Doug Ulmer for their encouragement throughout this project. The author is especially grateful to Keunyoung Jeong for providing thoughtful feedback and corrections. Finally, a huge thank you to the anonymous referee for thoroughly reading this article multiple times and pointing out countless corrections and suggestions that greatly improved the accuracy and readability of the article.

Competing interest. The authors have no competing interest to declare.

Funding statement. During the completion of this work, the author was supported by the National Science Foundation, via grant DMS-2303011.

References

- [BBL16] M. J. Bright, T. D. Browning and D. Loughran, ‘Failures of weak approximation in families’, *Compos. Math.* **152**(7) (2016), 1435–1475.
- [Bir68] B. J. Birch, ‘How the number of points of an elliptic curve over a fixed prime field varies’, *J. London Math. Soc.* **43** (1968), 57–60.

- [BMA23] P. Bruin and I. M. Ayala, ‘Counting rational points on weighted projective spaces over number fields’, Preprint, 2023, [arXiv:2302.10967](https://arxiv.org/abs/2302.10967).
- [Bru92] A. Brumer, ‘The average rank of elliptic curves. I’, *Invent. Math.* **109**(3) (1992), 445–472.
- [BS13a] M. Bhargava and A. Shankar, ‘The average number of elements in the 4-selmer groups of elliptic curves is 7’, Preprint, 2023, [arXiv:1312.7333](https://arxiv.org/abs/1312.7333).
- [BS13b] M. Bhargava and A. Shankar, ‘The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1’, Preprint, 2013, [arXiv:1312.7859](https://arxiv.org/abs/1312.7859).
- [BS15a] M. Bhargava and A. Shankar, ‘Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves’, *Ann. of Math. (2)* **181**(1) (2015), 191–242.
- [BS15b] M. Bhargava and A. Shankar, ‘Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0’, *Ann. of Math. (2)* **181**(2) (2015), 587–621.
- [BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, ‘Notes on elliptic curves. II’, *J. Reine Angew. Math.* **218** (1965), 79–108.
- [BW14] F. Barroero and M. Widmer, ‘Counting lattice points and O-minimal structures’, *Int. Math. Res. Not. IMRN* (**18**) (2014), 4932–4957.
- [Cas59] J. W. S. Cassels, *An Introduction to the Geometry of Numbers* (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete) vol. 99 (Springer-Verlag, Berlin-Göttingen-Heidelberg, 1959).
- [CJ23a] P. J. Cho and K. Jeong, ‘The average analytic rank of elliptic curves with prescribed torsion’, *J. Lond. Math. Soc. (2)* **107**(2) (2023), 616–657.
- [CJ23b] P. J. Cho and K. Jeong, ‘On the distribution of analytic ranks of elliptic curves’, *Math. Z.* **305**(3) (2023), Paper No. 42, 20 pp.
- [CJP23] P. J. Cho, K. Jeong and J. Park, ‘The average analytic rank of elliptic curves with prescribed level structure’, Preprint, 2023, [arXiv:2312.05817](https://arxiv.org/abs/2312.05817).
- [Cox89] D. A. Cox, *Primes of the Form $x^2 + ny^2$* . (A Wiley-Interscience Publication) (John Wiley & Sons, Inc., New York, 1989). Fermat, class field theory and complex multiplication.
- [CS23] J. E. Cremona and M. Sadek, ‘Local and global densities for Weierstrass models of elliptic curves’, *Math. Res. Lett.* **30**(2) (2023), 413–461.
- [Dar21] R. Darda, ‘Rational points of bounded height on weighted projective stacks’, PhD thesis, Université Paris Cité, 2021.
- [Dav51] H. Davenport, ‘On a principle of Lipschitz’, *J. London Math. Soc.* **26** (1951), 179–183.
- [Del74] P. Deligne, ‘La conjecture de Weil. I’, *Inst. Hautes Études Sci. Publ. Math.* (**43**) (1974), 273–307.
- [Den98] A.-W. Deng, ‘Rational points on weighted projective spaces’, Preprint, 1998, [arXiv:9812082](https://arxiv.org/abs/9812082).
- [Deu41] M. Deuring, ‘Die Typen der Multiplikatorenringe elliptischer Funktionenkörper’, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.
- [ESZB23] J. S. Ellenberg, M. Satriano and D. Zureick-Brown, ‘Heights on stacks and a generalized Batyrev-Manin-Malle conjecture’, *Forum Math. Sigma* **11** (2023), Paper No. e14, 54 pp.
- [GG07] D. A. Goldston and S. M. Gonek, ‘A note on $S(t)$ and the zeros of the Riemann zeta-function’, *Bull. Lond. Math. Soc.* **39**(3) (2007), 482–486.
- [HB04] D. R. Heath-Brown, ‘The average analytic rank of elliptic curves’, *Duke Math. J.* **122**(3) (2004), 591–623.
- [Iha67] Y. Ihara, ‘Hecke Polynomials as congruence ζ functions in elliptic modular case’, *Ann. of Math. (2)* **85** (1967), 267–295.
- [IK04] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society Colloquium Publications) vol. 53 (American Mathematical Society, Providence, RI, 2004).
- [JP20] B. W. Jordan and B. Poonen, ‘The analytic class number formula for 1-dimensional affine schemes’, *Bull. Lond. Math. Soc.* **52**(5) (2020), 793–806.
- [KP17] N. Kaplan and I. Petrow, ‘Elliptic curves over a finite field and the trace formula’, *Proc. Lond. Math. Soc. (3)* **115**(6) (2017), 1317–1372.
- [Lan94] S. Lang, *Algebraic Number Theory* (Graduate Texts in Mathematics) vol. 110, second edn. (Springer-Verlag, New York, 1994).
- [Len87] H. W. Lenstra, Jr. ‘Factoring integers with elliptic curves’, *Ann. of Math. (2)* **126**(3) (1987), 649–673.
- [MA21] I. M. Ayala, ‘Counting rational points on weighted projective spaces over number fields’, Master’s thesis, University of Zurich, 2021.
- [Mes86] J.-F. Mestre, ‘Formules explicites et minorations de conducteurs de variétés algébriques’, *Compos. Math.* **58**(2) (1986), 209–232.
- [Mil02] S. J. Miller, ‘1- and 2-level densities for families of elliptic curves: Evidence for the underlying group symmetries’, PhD thesis, Princeton University, ProQuest LLC, Ann Arbor, MI, 2002.
- [Min07] H. Minkowski, *Diophantische Approximationen. Eine Einführung in die Zahlentheorie. Mathematische Vorlesungen an der Universität Göttingen. II.* Leipzig: B. G. Teubner. viii, 235 S. Mit 82 Fig., 1907.
- [Neu99] J. Neukirch, *Algebraic Number Theory* (Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]) vol. 322 (Springer-Verlag, Berlin, 1999). Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

- [Pet18] I. Petrow, 'Bounds for traces of Hecke operators and applications to modular and elliptic curves over a finite field', *Algebra Number Theory* **12**(10) (2018), 2471–2498.
- [Phi22] T. Phillips, 'Rational points of bounded height on some genus zero modular curves over number fields', Preprint, 2022, [arXiv:2201.10624](https://arxiv.org/abs/2201.10624).
- [Sch79] S. H. Schanuel, 'Heights in number fields', *Bull. Soc. Math. France* **107**(4) (1979), 433–449.
- [Sch87] R. Schoof, 'Nonsingular plane cubic curves over finite fields', *J. Combin. Theory Ser. A* **46**(2) (1987), 183–211.
- [Sha13] A. Shankar, 'The average rank of elliptic curves over number fields', PhD thesis, Princeton University, 2013.
- [Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics) vol. 106, second edn. (Springer, Dordrecht, 2009).
- [Sta97] R. P. Stanley, *Enumerative Combinatorics. Vol. 1* (Cambridge Studies in Advanced Mathematics) vol. 49 (Cambridge University Press, Cambridge, 1997). With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.
- [Tat75] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', in *Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)* (Lecture Notes in Math.) vol. 476 (1975), 33–52.
- [vdD98] L. van den Dries, *Tame Topology and o-minimal Structures* (London Mathematical Society Lecture Note Series) vol. 248 (Cambridge University Press, Cambridge, 1998).
- [Wil96] A. J. Wilkie, 'Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function', *J. Amer. Math. Soc.* **9**(4) (1996), 1051–1094.
- [You06] M. P. Young, 'Low-lying zeros of families of elliptic curves', *J. Amer. Math. Soc.* **19**(1) (2006), 205–250.