DIOPHANTINE APPROXIMATION FOR ALGEBRAIC POINTS ON CURVES

By

Thomas Plante

A DISSERTATION

Submitted
to Michigan State University
in partial fulfillment of the requirements
for the degree of

Mathematics – Doctor of Philosophy

2020

ABSTRACT

DIOPHANTINE APPROXIMATION FOR ALGEBRAIC POINTS ON CURVES

By

Thomas Plante

A foundational result in Diophantine approximation is Roth's theorem, which asserts that for a given algebraic number α and $\varepsilon > 0$, the inequality $|\alpha - p/q| < 1/q^{2+\varepsilon}$ has only finitely many solutions in rational numbers $p/q \in \mathbb{Q}$. Ridout and Lang subsequently proved a general form of Roth's theorem allowing for arbitrary absolute values (including p-adic absolute values) and permitting arbitrary (fixed) number fields k in place of the rational numbers. Wirsing proved a generalization of Roth's theorem, where the approximating elements are taken from varying number fields of degree d, and the quantity $2+\varepsilon$ in Roth's theorem is replaced by $2d+\varepsilon$. As a consequence of a deep inequality of Vojta, Wirsing's theorem, appropriately formulated, may be extended to a Diophantine approximation result for algebraic points of degree d on a nonsingular projective curve.

The main theorem of this thesis improves on this general form of Wirsing's theorem further, but only in the cases where $d = 2$ and $d = 3$. More specifically, if we let C be a nonsingular projective curve over a number field k, S a finite set of places of k and $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$, then letting $R \in C(k)$ and $\varepsilon > 0$, we get

$$m_{D,S}(P) \leq (N_d(D) + \varepsilon) h_R(P) + O(1)$$

for all $P \in C(\overline{k})$ with $[k(P) : k] = d \in \{2, 3\}$, where $m_{D,S}(P)$ is a sum of local heights associated to D and S, h_R is a global height associated to R, and

$$N_d(D) := \max \left\{ \left| \left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty) \right) \cap \mathrm{Supp}(D) \right| \right\}$$

taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree d. As $N_d(D) \leq 2d$, the main result gives a refinement of Wirsing's theorem depending on the divisor D.

In much the same way that Roth's theorem can be used to prove Siegel's Theorem about integral points on a genus-0 affine curve, the main theorem of this dissertation implies Levin's generalization of Siegel's theorem for algebraic points of degree d in the cases $d = 2, 3$.

After a review of some properties of global heights and local heights, we also show that the main theorem is sharp, in the sense that counterexamples exist when $N_d(D) + \varepsilon$ is replaced with $N_d(D) - \varepsilon$.

To prove the main theorem, we first show that for curves of large enough genus, the number of morphisms $\sigma : C \to \mathbb{P}^1$ of degree $d = 2, 3$ defined over k is finite. We then prove that curves for which the number of such morphisms is finite satisfy the main theorem. Finally, we prove the main theorem for the remaining small genus curves on a case by case basis.

We transfer the Diophantine approximation problem for points of degree d on C to a Diophantine approximation problem for rational points on $\mathrm{Sym}^d(C)$ (the dth symmetric power of C). We exploit the map from $\mathrm{Sym}^d(C)$ to $\mathrm{Jac}(C)$, the Jacobian of C, and its associated geometry. We use Diophantine approximation results for abelian varieties (when we're on $\mathrm{Jac}(C)$), Diophantine approximation results for projective spaces (fibers of $\mathrm{Sym}^d(C) \mapsto \mathrm{Jac}(C)$), and Diophantine approximation results on $\mathrm{Sym}^d(C)$ directly, plus algebraic geometry to connect all of these. In the course of the proof we make use of Schmidt's subspace theorem and its generalizations due to Ru-Wong and Evertse-Ferretti as well as a version of Roth's theorem for nonreduced divisors and Faltings' approximation theorem for rational points on abelian varieties.

TABLE OF CONTENTS

CHAPTER 1 AN INTRODUCTION TO DIOPHANTINE APPROXIMATION 1
1.1 The Road to Roth's Theorem 1
1.2 Further Approximation Results 4
1.3 Integral Points on Curves 7

CHAPTER 2 REVIEW OF HEIGHTS 11
2.1 Heights on Projective Spaces 11
2.2 Heights on Projective Varieties 14
2.3 Heights on Closed Subschemes 18

CHAPTER 3 PREPARATION 22
3.1 Useful Results 22
3.2 Sharpness of the Main Result 25
3.3 Facts on Trigonal Maps 27

CHAPTER 4 PROOF OF THE MAIN THEOREM 31
4.1 Algebraic Points on Curves 31
4.2 Quadratic Points on Elliptic Curves 37
4.3 Cubic Points on Curves of Low Genus 45

BIBLIOGRAPHY 63

CHAPTER 1

AN INTRODUCTION TO DIOPHANTINE APPROXIMATION

1.1 The Road to Roth's Theorem

An important question in Diophantine approximation is how closely a given real number $\alpha \in \mathbb{R}$ can be approximated by rational numbers $p/q \in \mathbb{Q}$; in particular, that to approximate α closely both the numerator, p, and denominator, q, must be large. A typical way of expressing this is to ask, for a given $\alpha \in \mathbb{R}$ and $e > 0$, whether or not the inequality

$$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{|q|^e}$$

has infinitely many solutions $p/q \in \mathbb{Q}$. In 1842, it was shown by Dirichlet that

Theorem 1.1.1. *For each $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ the inequality*

$$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^2}$$

has infinitely many solutions $p/q \in \mathbb{Q}$.

Meanwhile, in 1844, Liouville showed that

Theorem 1.1.2 (Liouville)**.** *If α is an algebraic number of degree d and if $e > d$, then the inequality*

$$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{|q|^e}$$

has at most finitely many solutions $p/q \in \mathbb{Q}$.

In fact, given an algebraic number α of degree d, you can find an **effective** (explicitly described) constant $C = C(\alpha) > 0$ such that the inequality

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{|q|^d}$$

holds for all $p/q \in \mathbb{Q} \setminus \{\alpha\}$.

Example 1.1.3. Let $\alpha = \sum_{i=1}^{\infty} 10^{-i!}$. Then the partial sums $\sum_{i=1}^{n} 10^{-i!}$ are solutions to $\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{|q|^e}$ as long as $n \geq e$. By Liouville's theorem, α is transcendental.

In order to start getting nice applications to Diophantine equations, however, one needs an exponent of $d - \varepsilon$.

Theorem 1.1.4 (Thue, 1909)**.** *Let $\alpha \in \overline{\mathbb{Q}}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Let $\varepsilon > 0$. Then there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{d}{2}+1+\varepsilon}}.$$

Example 1.1.5. Consider integer solutions to the equation $x^3 - 2y^3 = 1$. Then

$$\frac{1}{y^3} = \left(\frac{x}{y}\right)^3 - 2 = \left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\left(\frac{x}{y}\right)^2 + \frac{x}{y}\sqrt[3]{2} + \sqrt[3]{4}\right)$$

Which implies $\left|\frac{x}{y} - \sqrt[3]{2}\right| < \frac{C}{y^3}$ for some constant $C > 0$. By Thue's theorem, there are only finitely many solutions $x, y \in \mathbb{Z}$.

More generally, Thue proved that if $f \in \mathbb{Z}[x, y]$ is an irreducible binary form with $\deg(f) \geq 3$, and $r \in \mathbb{Z}$, $f(x, y) = r$ has only finitely many integer solutions x and y.

The exponent $\frac{d}{2} + 1$ in Thue's theorem was subsequently improved to $2\sqrt{d}$ by Siegel (1921) and $\sqrt{2d}$ by Dyson and Gelfond (independently) (1947). In 1955 Roth managed to eliminate the dependence on d altogether.

Theorem 1.1.6 (Roth's Theorem)**.** *For every algebraic number α and every $\varepsilon > 0$, the inequality*

$$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{|q|^{2+\varepsilon}}$$

has only finitely many solutions $p/q \in \mathbb{Q}$.

Equivalently, for every real algebraic number α and every $\varepsilon > 0$, there exists a constant $C = C(\alpha, \varepsilon) > 0$ such that for all $p/q \in \mathbb{Q} \setminus \{\alpha\}$

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{|q|^{2+\varepsilon}}.$$

note here that Roth's Theorem only asserts the existence of such a constant C and provides no way of calculating it, that is, C is not effective. Another equivalent expression of Roth's Theorem is that for every real algebraic number α and every $\varepsilon > 0$, there exists a constant $C = C(\alpha, \varepsilon) > 0$ such that for all $p/q \in \mathbb{Q} \setminus \{\alpha\}$

$$\log \max \left\{ \left| \frac{p}{q} - \alpha \right|^{-1}, 1 \right\} \leq (2 + \varepsilon) \log \max \{|p|, |q|\} + C.$$

This form is significant, because it is written in terms of functions called heights. The left hand side of the inequality is what's known as a local height of p/q, relative to the algebraic number α, which for now we denote $\lambda_\alpha(p/q)$. note that the closer p/q gets to α, the larger the local height becomes, so we think of local height like an inverse distance function. The height of a rational number p/q, with $\gcd(p, q) = 1$, is $h(p/q) := \log \max \{|p|, |q|\}$. Height can be thought of as a measure of the arithmetic complexity of a number. Thus, using big-O notation, we may restate Roth's theorem: For every algebraic number α and every $\varepsilon > 0$, the inequality

$$\lambda_\alpha(\beta) \leq (2 + \varepsilon) h(\beta) + O(1)$$

holds for all $\beta \in \mathbb{Q}$.

Generalizing to an arbitrary absolute value $|\cdot|_v$ on a number field k (normalized as in Definition 2.1.3), we define the following:

Definition 1.1.7. Let k be a number field. Given $\alpha \in \overline{k}$ and an absolute value $|\cdot|_v$ on k (with some fixed extension to $\overline{k}$), define the local height associated to α at v by

$$\lambda_{\alpha,v}(\beta) := \log \max \left\{ \left| \frac{1}{\beta - \alpha} \right|_v, 1 \right\}$$

for all $\beta \in k$.

Similarly, we may define the (global) height of an algebraic number (see Definition 2.1.6).

1.2 Further Approximation Results

In 1958, Ridout generalized Roth's theorem to p-adic absolute values on $\mathbb{Q}$ and soon after Lang generalized the result to an arbitrary number field.

Theorem 1.2.1 (Roth's Theorem, General Form)**.** *Let S be a finite set of absolute values on a number field k. For each $v \in S$, let $\alpha_v \in \overline{k}$ and fix an extension of $|\cdot|_v$ to $\overline{k}$. Let $\varepsilon > 0$. Then for all $\beta \in k \setminus \{\alpha_v | v \in S\}$*

$$\sum_{v \in S} \lambda_{\alpha_v, v}(\beta) \leq (2 + \varepsilon) h(\beta) + O(1).$$

We can also view Roth's Theorem as a statement about k-rational points on the projective line by defining local heights $\lambda_{D,v}$ with respect to a divisor D on $\mathbb{P}^1(k)$ (see Definition 2.2.1). Then we get the following:

Theorem 1.2.2 (Roth's Theorem on $\mathbb{P}^1$)**.** *Let S be a finite set of places of a number field k. Let $P_1, \ldots, P_q \in \mathbb{P}^1(k)$ be distinct points, $D = \sum_{i=1}^{q} P_i$, and $\varepsilon > 0$. Then for all $P \in \mathbb{P}^1(k) \setminus \{P_1, \ldots, P_q\}$*

$$m_{D,S}(P) := \sum_{v \in S} \lambda_{D,v}(P) \leq (2 + \varepsilon) h(P) + O(1).$$

We will study throughout inequalities of this form, where a sum of local heights, with respect to some divisor, is bounded by a constant multiple of a global height (where the constant may depend on the divisor). For curves of genus greater than one, such inequalities are uninteresting (for rational points) due to Faltings' theorem:

Theorem 1.2.3 (Faltings' Theorem)**.** *Let C be a smooth projective curve of genus $g \geq 2$, defined over a number field k. Then the number of k-rational points of C is finite.*

Proof. See [8, Part E]. □

This is exactly the statement that, given any finite set S of absolute values on a number field k and distinct points $P_1, \ldots, P_q \in C(k)$, $m_{D,S}(P) \leq O(1)$ for all $P \in C(k) \setminus \{P_1, \ldots, P_q\}$, where $D = \sum_{i=1}^{q} P_i$.

It remains to ask what happens on curves of genus one, i.e. elliptic curves. The answer for this case is due to Siegel. It requires the notion of a global height associated to a divisor on a curve C (see Definition 3.8). In the case of curves, we will typically take the divisor D to consist of a single point $R \in C(k)$. By Theorem 2.2.12, if $R, R' \in C(k)$, then for any $\varepsilon > 0$, $|h_R(P) - h_{R'}(P)| \leq \varepsilon h_R(P) + O(1)$, so that the choice of the point R will not be significant in our inequalities.

Theorem 1.2.4 (Siegel)**.** *Let C be a smooth projective curve of genus one, defined over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_q \in C(k)$ be distinct points and let $D = \sum_{i=1}^{q} P_i$. Let $R \in C(k)$ and let $\varepsilon > 0$. Then for all $P \in C(k) \setminus \{P_1, \ldots, P_q\}$*

$$m_{D,S}(P) \leq \varepsilon h_R(P) + O(1).$$

Another way to generalize Roth's theorem is to consider, instead of k-rational points, algebraic points in $C(\overline{k})$ of degree d over k. We denote the support of a divisor D by $\mathrm{Supp}(D)$.

Theorem 1.2.5 (Wirsing's Theorem)**.** *Let S be a finite set of places of a number field k. Let $P_1, \ldots, P_q \in \mathbb{P}^1(k)$ be distinct points and let $D = \sum_{i=1}^{q} P_i$. Let $\varepsilon > 0$ and let d be a positive integer. Then for all points $P \in \mathbb{P}^1(\overline{k}) \setminus \mathrm{Supp}(D)$ satisfying $[k(P) : k] \leq d$,*

$$m_{D,S}(P) \leq (2d + \varepsilon)h(P) + O(1).$$

Theorem 1.2.6 (Vojta's Inequality)**.** *Let C be a nonsingular projective curve defined over a number field k with canonical divisor K. Let S be a finite set of places of k. Let $P_1, \ldots, P_q \in C(k)$ be distinct points and let $D = \sum_{i=1}^{q} P_i$. Let A be an ample divisor on C. Let $\varepsilon > 0$. If r is a positive integer then*

$$m_{D,S}(P) + h_K(P) \leq d_a(P) + \varepsilon h_A(P) + O(1)$$

for all points $P \in C(\overline{k}) \setminus \mathrm{Supp}(D)$ for which $[k(P) : k] \leq r$, where d_a is the arithmetic discriminant (a value defined by Vojta using Arakelov theory).

Proof. See [17]. □

Vojta's inequality implies many important results in Diophantine Geometry, including Faltings's theorem and Wirsing's theorem. Vojta also conjectured that the arithmetic discriminant in the inequality could be replaced by the smaller geometric (logarithmic) discriminant $d(P) := \log |D_{k(p)}|/[k : \mathbb{Q}]$. The relationship between these discriminants is similar to that between the arithmetic and geometric genus. Vojta's conjecture implies many other famous conjectures, such as the famous ABC conjecture.

We can use Vojta's inequality to generalize Wirsing's theorem to curves.

Theorem 1.2.7. *Let C be a nonsingular projective curve over a number field k. Let S be a finite set of places of k and let $R \in C(k)$. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$ and let d be a positive integer. Then*

$$m_{D,S}(P) \leq (2d + \varepsilon)h_R(P) + O(1)$$

for all $P \in C(\overline{k})$ with $[k(P) : k] = d$.

Proof. Follows from Vojta's inequality. See [14, Equation (2.0.3)]. □

Song and Tucker show that this result is sharp in the following sense.

Theorem 1.2.8. *Let C be a nonsingular projective curve over a number field k and let $\varphi : C \to \mathbb{P}^1$ be a nonconstant morphism of degree d. Let S be a finite set of places of k and let $R \in C(k)$. Let $\varepsilon > 0$. Then there exists a choice of D such that there is an infinite set of points $P \in C(\overline{k})$ with $[k(P) : k] \leq d$ satisfying*

$$m_{D,S}(P) \geq (2d - \varepsilon)h_R(P) + O(1).$$

Proof. See [14, Theorem 2.3]. □

However, by replacing $2d$ with a constant depending on the divisor D, we found we could improve on Theorem 1.2.7 as follows:

Theorem 1.2.9 (The Main Theorem)**.** *Let C be a nonsingular projective curve over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i \in \mathrm{Div}(C)$. Let $R \in C(k)$ and let $\varepsilon > 0$. Then if $d \in \{2, 3\}$,*

$$m_{D,S}(Q) \leq (N_d(D) + \varepsilon) h_R(Q) + O(1)$$

for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$, where

$$N_d(D) := \max \left\{ \left| \left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty) \right) \cap \mathrm{Supp}(D) \right| \right\}$$

taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree d.

note that the most that $N_d(D)$ could ever be is $2d$, which agrees with Theorem 1.2.7. These diophantine approximation inequalities are closely related to qualitative results for integral points on curves.

1.3 Integral Points on Curves

Let k be a number field and let S be a finite set of places of k containing all archimedean places. The ring of S-integers, denoted $\mathcal{O}_{k,S}$, is defined to be the set of all $\beta \in k$ such that $|\beta|_v \leq 1$ for all $v \notin S$.

Theorem 1.3.1 (Siegel's Theorem, 1929)**.** *Let $C \subset \mathbb{A}^n$ be a nonsingular affine curve over a number field k and let S be a finite set of places of k containing the archimedean places. An **S-integral point** of C is a point whose affine coordinates are all in the ring $\mathcal{O}_{k,S}$. If C has genus $g > 0$, or if C has at least three distinct points at infinity, then C has only finitely many S-integral points.*

Proof. See [1, Theorem 7.3.9]. □

Although this qualitative result preceded the above diophantine approximation inequalities on projective curves, they are related in the following way:

Let $C \subset \mathbb{A}^n$ be a nonsingular affine curve over a number field k. Let $\tilde{C}$ be the nonsingular projective completion of C and let D be the very ample divisor on $\tilde{C}$ consisting of the points at infinity of C. Let $R \in \tilde{C}(k)$ and let $\varepsilon > 0$. By Lemma 3.1.7, the set of S-integral points on C corresponds (up to a finite number of points) to the set of points $P \in \tilde{C}(k) \setminus \mathrm{Supp}(D)$ satisfying $m_{D,S}(P) = h_D(P) + O(1)$. If C has genus $g = 0$ and $\deg(D) \geq 3$, then $\tilde{C}$ is birationally equivalent to $\mathbb{P}^1$ and

$$\begin{aligned}
\deg(D)h_R(P) &= h_{\deg(D)R}(P) \\
&\leq (1+\varepsilon)h_D(P) + O(1) \text{ by Theorem 2.2.12} \\
&= (1+\varepsilon)m_{D,S}(P) + O(1) \\
&\leq (1+\varepsilon)(2+\varepsilon)h_R(P) + O(1) \text{ by Theorem 1.2.2,}
\end{aligned}$$

implying $h_R(P) \leq O(1)$. By Theorem 2.2.11, there are only finitely many such points. If C has genus $g = 1$, then Theorem 1.2.4 says $m_{D,S}(P) \leq \varepsilon h_D(P) + O(1)$ for all $P \in \tilde{C} \setminus \mathrm{Supp}(D)$. But if $m_{D,S}(P) = h_D(P) + O(1)$, then this implies $h_D(P) \leq O(1)$ and once again Theorem 2.2.11 implies there are only finitely many such points. And of course if C has genus $g \geq 2$ then Theorem 1.2.3 implies $m_{D,S}(P) \leq O(1)$. So if $m_{D,S}(P) = h_D(P) + O(1)$, then $h_D(P) \leq O(1)$ and there are only finitely such points. Thus these three results together imply Siegel's theorem.

In this way diophantine approximation inequalities for rational points on projective varieties can be thought of as more precise statements of qualitative results for integral points on affine varieties.

Similar to how Roth's theorem implies the genus-0 case of Siegel's theorem, the main theorem can be used to show the $d = 2, 3$ cases of the following qualitative result on integral points.

Theorem 1.3.2 (Levin)**.** *Let $C \subset \mathbb{A}^n$ be a nonsingular affine curve over a number field k and let S be a finite set of places of k containing the archimedean places. Let $\tilde{C}$ be a nonsingular projective completion of C and let $(\tilde{C} \setminus C)(\overline{k}) = \{P_1, \ldots, P_q\}$. Let d be a positive integer. Let $\overline{O}_{k,S}$ denote the integral closure of $O_{k,S}$ in $\overline{k}$. Then there exists a finite extension L of k such that the set*

$$\{P \in C(\overline{O}_{L,S}) \mid [L(P) : L] \leq d\}$$

is infinite if and only if there exists a morphism $\varphi : \tilde{C} \to \mathbb{P}^1$*, over* $\overline{k}$ *with* $\deg(\varphi) \leq d$ *and* $\varphi(\{P_1, \ldots, P_q\}) \subset \{0, \infty\}$.

Proof. See [10, Theorem 1.9] □

To see how this is implied by the main theorem, let $C \subset \mathbb{A}^n$ be a nonsingular affine curve over a number field k and let S be a finite set of places of k containing the archimedean places. Let $\tilde{C}$ be a nonsingular projective completion of C and let $(\tilde{C} \setminus C)(\overline{k}) = \{P_1, \ldots, P_q\}$. Let $d \in \{2, 3\}$. Let $D = P_1 + \ldots + P_q$ be a divisor on $\tilde{C}$ and let $R \in \tilde{C}(k)$. Then for all $P \in \tilde{C}(\overline{O}_{L,S}) \setminus \{P_1, \ldots, P_q\}$ with $[k(P) : k] = d$,

$$\begin{aligned}
\deg(D)h_R(P) &= h_{\deg(D)R}(P) \\
&\leq (1+\varepsilon)h_D(P) + O(1) \text{ by Theorem 2.2.12} \\
&= (1+\varepsilon)m_{D,S}(P) + O(1) \\
&\leq (1+\varepsilon)(N_d(D) + \varepsilon)h_R(P) + O(1) \text{ by Theorem 1.2.2,}
\end{aligned}$$

where

$$N_d(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$$

taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree d. But if there does not exist a morphism $\varphi : \tilde{C} \to \mathbb{P}^1$, over $\overline{k}$ with $\deg(\varphi) \leq d$ and $\varphi(\{P_1, \ldots, P_q\}) \subset \{0, \infty\}$ then $N < \deg(D)$, and so the above inequality implies $h_R(P) \leq O(1)$ and by Theorem 2.2.11, there are only finitely many such points P.

The main idea behind this result and the main theorem is that we expect almost all of the degree d points on a curve are coming from pulling back rational points on $\mathbb{P}^1$ by maps of degree d. The following are two other results that are closely related to this heuristic approach.

C is called **hyperelliptic** (respectively **bielliptic**) if it admits a map $\varphi : C \to X$ of degree 2 onto a curve X of genus zero (respectively one).

Theorem 1.3.3 (Harris-Silverman)**.** *Let C be a nonsingular projective curve over a number field k. Suppose C has genus $g \geq 2$. Assume that C is neither hyperelliptic nor bielliptic. Then the set of points $P \in C(\overline{k})$ with $[k(P) : k] \leq 2$ is finite.*

Proof. See [6, Corollary 3] □

Theorem 1.3.4 (Corvaja-Zannier)**.** *Let $C \subset \mathbb{A}^n$ be a nonsingular affine curve over a number field k and let S be a finite set of places of k containing the archimedean places. Let $\tilde{C}$ be a nonsingular projective completion of C and let $(\tilde{C} \setminus C)(\overline{k}) = \{P_1, \ldots, P_q\}$.*

(a) *If $q \geq 5$, then C contains only finitely many quadratic (over k) S-integral points.*

(b) *If $q \geq 4$, then there exists a finite set of rational maps $\varphi : \tilde{C} \to \mathbb{P}^1$ of degree 2 such that all but finitely many of the quadratic S-integral points on C are sent to $\mathbb{P}^1_k$ by some of the mentioned maps.*

Proof. See [2, Corollary 1] □

CHAPTER 2

REVIEW OF HEIGHTS

2.1 Heights on Projective Spaces

The height of a rational number p/q is defined to be $h(p/q) = \log \max\{|p|, |q|\}$. Similarly the height of a point $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(\mathbb{Q})$, with coordinates chosen so that $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, is defined to be $h(P) = \log \max\{|x_0|, \ldots, |x_n|\}$. One of the key features of heights is that, given a bound, the number of points of bounded height is finite, that is the set

$$\left\{P \in \mathbb{P}^n(\mathbb{Q}) \mid h(P) \leq B\right\}$$

is finite for any $B > 0$.

In order to generalize the concept of heights to number fields other than $\mathbb{Q}$, we recall some properties of absolute values on fields. An absolute value on a field k is a map $|\cdot| : k \to \mathbb{R}$ satisfying the following.

- $|\alpha| \geq 0$ for all $\alpha \in k$.
- $|\alpha| = 0$ if and only if $\alpha = 0$.
- $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in k$.
- $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in k$.

We say two absolute values on a field k are **equivalent** if they induce the same topology on k. It can be shown that

Proposition 2.1.1. *Two absolute values $|\cdot|_1, |\cdot|_2$ on a field k are equivalent if and only if there is a positive real number s such that*

$$|x|_1 = |x|_2^s$$

for all $x \in k$.

Proof. See [11, Proposition 3.3]. □

We denote the set of equivalence classes of non-trivial absolute values on a field k by M_k and call its elements places. If k' is an extension of k and v is a place of k, we say a place w of k' **extends** v, denoted $w|v$, if the restriction to k of any representative of w is a representative of v.

Definition 2.1.2. The completion of k with respect to the place v is an extension field k_v, with a place w such that:

(a) $w|v$

(b) The topology of k_v induced by w is complete.

(c) k is a dense subset of k_v in the above topology.

The completion exists and is unique up to isometric isomorphisms. By abuse of notation, we shall denote the unique place w also by v.

The standard absolute values on $\mathbb{Q}$ are the (usual) archimedean absolute value $|\cdot|_\infty = |\cdot|$ and the p-adic absolute values $|\cdot|_p = p^{-\mathrm{ord}_p(\cdot)}$ for each prime p. By Ostrowski's Theorem, this is a complete list of all absolute values on $\mathbb{Q}$ up to equivalence.

Definition 2.1.3. Let p be a place on $\mathbb{Q}$. We consider a number field k and a place v of k extending p. For any $x \in k$, we define

$$|x|_v = |N_{k_v/\mathbb{Q}_p}(x)|_p^{1/[k:\mathbb{Q}]}$$

where $N_{k_v/\mathbb{Q}_p}$ is the norm from k_v to $\mathbb{Q}_p$.

note that $|\cdot|_v$ is an extension to k of $|\cdot|_p^{[k_v:\mathbb{Q}_p]/[k:\mathbb{Q}]}$ on $\mathbb{Q}$, an absolute value that by Proposition 2.1 is equivalent to $|\cdot|_p$. That is $v|p$.

These normalized absolute values satisfy the following.

Lemma 2.1.4. *Let k be a number field with a place $v \in M_k$. We consider a finite-dimensional extension field k' of k. For any $x \in k^*$,*

$$\prod_{\substack{w \in M_{k'} \\ w|v}} |x|_w = |x|_v.$$

Proof. See [1, Lemma 1.3.7]. □

Proposition 2.1.5 (The Product Formula)**.** *Let k be a number field. For any $x \in k^*$,*

$$\prod_{v \in M_k} |x|_v = 1.$$

Proof. See [1, Proposition 1.4.4]. □

Definition 2.1.6. The (absolute) height of a point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ with homogeneous coordinates $(x_0, \ldots, x_n)$ is defined to be

$$h(P) = \sum_{v \in M_k} \max_{0 \le i \le n} \log |x_i|_v$$

where k is some number field containing $x_0, \ldots, x_n$. We also define the height of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ to be the height of the point $(\alpha, 1) \in \mathbb{P}^1(\overline{\mathbb{Q}})$

$$h(\alpha) := h((\alpha, 1)) = \sum_{v \in M_k} \log \max \{|\alpha|_v, 1\}.$$

Proposition 2.1.7. *The height, so defined, is independent of the choice of homogeneous coordinates for P and the choice of number field k containing them.*

Proof. See [1, Lemmas 1.5.2 and 1.5.3]. □

One reason for studying heights is because they satisfy the following.

Theorem 2.1.8 (Northcott's Theorem)**.** *For any numbers $B, d \ge 0$, the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid h(P) \le B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \le d\}$$

is finite. In particular, for any fixed number field k, the set

$$\{P \in \mathbb{P}^n_k \mid h(P) \leq B\}$$

is finite.

Proof. See [1, Theorem 1.6.8]. □

Another important property of heights is preservation under Galois action.

Proposition 2.1.9. *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $h(P) = h(\sigma(P))$ for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, where $\sigma\left((x_i)_{i=1}^n\right) := (\sigma(x_i))_{i=1}^n$*

Proof. See [1, Proposition 1.5.17]. □

2.2 Heights on Projective Varieties

Let X be a projective variety over a number field k. We denote the set of divisors on X by Div(X). We consider a divisor D on X with associated line bundle $\mathcal{O}(D)$ and rational section s_D. There are base-point-free line bundles L, M on X such that $\mathcal{O}(D) \cong L \otimes M^{-1}$. Now choose generating global sections $s_0, \ldots, s_m$ of L and $t_0, \ldots, t_n$ of M, and call the data

$$\mathcal{D} = (s_D; L, \mathbf{s}; M, \mathbf{t})$$

a **presentation** of the divisor D. We denote the support of the divisor D by $\mathrm{Supp}(D)$.

Definition 2.2.1. Let $v \in M_k$. For $P \in X(k) \setminus \mathrm{Supp}(D)$, we define the **local height** of P relative to the presentation $\mathcal{D}$ at the place v to be

$$\lambda_{\mathcal{D},v}(P) := \log \max_k \min_l \left| \frac{s_k}{t_l s_D}(P) \right|_v .$$

Definition 2.2.2. If D_1 and D_2 are divisors with presentations $\mathcal{D}_i = (s_{D_i}; L_i, \mathbf{s}_i; M_i, \mathbf{t}_i)$, then we define the presentation $\mathcal{D}_1 + \mathcal{D}_2$ of the divisor $D_1 + D_2$ to be

$$\mathcal{D}_1 + \mathcal{D}_2 := (s_{D_1} s_{D_2}; L_1 \otimes L_2, \mathbf{s}_1\mathbf{s}_2; M_1 \otimes M_2, \mathbf{t}_1\mathbf{t}_2).$$

Similarly, if a divisor D has presentation $\mathcal{D} = (s_D; L, \mathbf{s}; M, \mathbf{t})$, we define the presentation $-\mathcal{D}$ of the divisor $-D$ to be

$$-\mathcal{D} := (s_D^{-1}; M, \mathbf{t}; L, \mathbf{s}).$$

Furthermore, if $\pi : Y \to X$ is a morphism of projective varieties such that $\pi(Y)$ is not contained in $\mathrm{Supp}(D)$, then we define the presentation $\pi^*\mathcal{D}$ of the divisor π^*D on Y to be

$$\pi^*\mathcal{D} := (\pi^* s_D; \pi^* L, \pi^* \mathbf{s}; \pi^* M, \pi^* \mathbf{t}).$$

With these definitions, it is immediate that the corresponding local heights satisfy

$$\lambda_{\mathcal{D}_1+\mathcal{D}_2,v} = \lambda_{\mathcal{D}_1,v} + \lambda_{\mathcal{D}_2,v}, \qquad \lambda_{-\mathcal{D},v} = -\lambda_{\mathcal{D},v}, \qquad \text{and} \qquad \lambda_{\pi^*\mathcal{D},v} = \lambda_{\mathcal{D},v} \circ \pi$$

for all $v \in M_k$.

Definition 2.2.3. An M_k**-constant** is a map $\gamma : M_k \to \mathbb{R}$ with the property that $\gamma_v = 0$ for all but finitely many $v \in M_k$.

Theorem 2.2.4. *Let $\mathcal{D}$ and $\mathcal{D}'$ be two presentations of the divisor D. Then there is an M_k-constant γ such that*

$$|\lambda_{\mathcal{D},v} - \lambda_{\mathcal{D}',v}| \leq \gamma_v.$$

Proof. See [1, Theorem 2.2.11]. □

For this reason, whenever an inequality holds only up to the addition of a bounded function, we will omit the presentation $\mathcal{D}$ and, by abuse of notation, denote a local height relative to D at a place v by $\lambda_{D,v}$.

Proposition 2.2.5. *Let D be an effective divisor on X. Then there is a presentation $\mathcal{D}$ of D such that for any $P \notin \mathrm{Supp}(D)$ and for any field extension $k \subset k' \subset \overline{k}$ such that $P \in X(k')$ and any place $v \in M_{k'}$, it holds that $\lambda_{\mathcal{D},v}(P) \geq 0$.*

Proof. See [1, Proposition 2.3.9]. □

Example 2.2.6. Let $\alpha \in k$. The point $(\alpha, 1)$ in $\mathbb{P}^1_k$ has the presentation

$$\mathcal{A} = (x_0 - \alpha x_1; \mathcal{O}_{\mathbb{P}^1}(1), (x_1, x_0 - \alpha x_1); \mathcal{O}_{\mathbb{P}^1}, 1).$$

For $\beta \in k \setminus \{\alpha\}$ and $v \in M_k$ the corresponding local height is

$$\lambda_{\alpha,v}(\beta) := \lambda_{\mathcal{A},v}((\beta, 1)) = \log \max \left\{ \left| \frac{1}{\beta - \alpha} \right|_v, 1 \right\}$$

which is the local height we described in Definition 1.1.7.

Example 2.2.7. The hyperplane $\{x_0 = 0\}$ in $\mathbb{P}^n_k$ has the presentation

$$\mathcal{D} = (x_0; \mathcal{O}_{\mathbb{P}^n}(1), (x_0, x_1, \ldots, x_n); \mathcal{O}_{\mathbb{P}^n}, 1).$$

For $P \in \mathbb{P}^n_k$ with $x_0(P) \neq 0$ and $v \in M_k$ the corresponding local height is

$$\lambda_{\mathcal{D},v}(P) = \log \max_i \left\{ \left| \frac{x_i}{x_0}(P) \right|_v \right\}$$

and the product formula becomes

$$h(P) = \sum_{v \in M_k} \lambda_{\mathcal{D},v}(P).$$

For this reason we make the following definition.

Definition 2.2.8. Let $\mathcal{D} = (s_D; L, \mathbf{s}; M, \mathbf{t})$ be a presentation of a divisor D on X. For $P \in X(\overline{k})$ there are s_i and t_j such that $s_i(P) \neq 0$, $t_j(P) \neq 0$ by definition of base point free line bundles. Thus we can find a non-zero rational section s of $\mathcal{O}(D)$ such that P is not contained in the support of the divisor $D(s)$. Then $\mathcal{D}(s) = (s; L, \mathbf{s}; M, \mathbf{t})$ is a presentation of $D(s)$. If k' is a finite extension $k \subset k' \subset \overline{k}$ such that $P \in X(k')$, then we define the **global height** of P relative to $\mathcal{D}$ by

$$h_{\mathcal{D}}(P) = \sum_{v \in M_{k'}} \lambda_{\mathcal{D}(s),v}(P).$$

Proposition 2.2.9. *The global height $h_{\mathcal{D}}$ is independent of the choices of k' and of the section s.*

Proof. See [1, Proposition 2.3.4]. □

It is immediately clear by the definition and the above discussion that, given presentations $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}$ of divisors D_1, D_2, D respectively and a morphism of projective varieties $\pi : X \to Y$, the corresponding global heights also satisfy

$$h_{\mathcal{D}_1+\mathcal{D}_2} = h_{\mathcal{D}_1} + h_{\mathcal{D}_2}, \;\; h_{-\mathcal{D}} = -h_{\mathcal{D}}, \;\; \text{and} \;\; h_{\pi^*\mathcal{D}} = h_{\mathcal{D}} \circ \pi.$$

Furthermore, by Proposition 3.2, if $D \in \mathrm{Div}(X)$ is effective, then there exists a presentation $\mathcal{D}$ of D such that $h_{\mathcal{D}}(P) \geq 0$ for all $P \in X(\overline{k})$.

For two divisors D_1 and D_2, we write $D_1 \sim D_2$ if D_1 is linearly equivalent to D_2, i.e. the difference $D_2 - D_1$ is a principal divisor.

Theorem 2.2.10. *Let $\mathcal{D}_1$, $\mathcal{D}_2$ be presentations of divisors D_1, $D_2 \in \mathrm{Div}(X)$ with $D_1 \sim D_2$. Then there is a constant $\gamma > 0$ such that*

$$|h_{\mathcal{D}_2} - h_{\mathcal{D}_1}| \leq \gamma.$$

Proof. See [1, Theorem 2.3.6]. □

Similarly to local heights, whenever an inequality holds only up to the addition of a bounded function, we will omit the presentation $\mathcal{D}$ and, by abuse of notation, denote a global height relative to D by h_D. Furthermore, in the special case where the divisor D is an effective divisor of degree 1 on a curve and $\mathrm{Supp}(D) = \{R\}$, we define $h_R := h_D$.

Global heights also satisfy Northcott's theorem.

Theorem 2.2.11 (Northcott's Theorem)**.** *Let D be an ample divisor on X and let $\mathcal{D}$ be a presentation of D. Then the set*

$$\{P \in X(\overline{k}) \mid h_{\mathcal{D}}(P) \leq B, \;\; [k(P) : k] \leq d\}$$

is finite for any constants $B, d \in \mathbb{R}$.

Proof. See [1, Theorem 2.4.9]. □

Recall that two divisors $D_1, D_2 \in \mathrm{Div}(X)$ are **algebraically equivalent** if there exists a connected algebraic set T, two points $t_1, t_2 \in T(k)$ and a line bundle L on $X \times T$ such that

$\mathcal{O}(D_1) \cong L|_{X\times\{t_1\}}$ and $\mathcal{O}(D_2) \cong L|_{X\times\{t_2\}}$. In particular if X is a curve, then any two points on X are algebraically equivalent.

Theorem 2.2.12. *Let $A, B \in \mathrm{Div}(X)$ be algebraically equivalent divisors with A ample. Let $\varepsilon > 0$ and d a positive integer. Then for all $P \in X(\overline{k})$ with $[k(P) : k] \leq d$ we have*

$$|h_A(P) - h_B(P)| \leq \varepsilon h_A(P) + O(1).$$

Proof. Follows from [8, Theorem B.5.9] and Theorem 2.2.11. □

Given a presentation $\mathcal{D} = (s_D; L, \mathbf{s}; M, \mathbf{t})$ of a divisor $D \in \mathrm{Div}(X)$, we have the morphisms

$$\varphi : X \to \mathbb{P}^m_k, \qquad P \mapsto (s_0(P), s_1(P), \ldots, s_m(P))$$

and

$$\psi : X \to \mathbb{P}^n_k, \qquad P \mapsto (t_0(P), t_1(P), \ldots, t_n(P)).$$

By the product formula we see that $h_{\mathcal{D}}(P) = h(\varphi(P)) - h(\psi(P))$. Therefore, by Proposition 2.1.9, for any $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we have $h_{\mathcal{D}}(\sigma(P)) = h_{\mathcal{D}}(P)$.

2.3 Heights on Closed Subschemes

We identify a closed subscheme X of a nonsingular projective variety V with its ideal sheaf $\mathcal{I}_X$. Then for closed subschemes X and Y we define the following:

$$\mathcal{I}_{X+Y} = \mathcal{I}_X \mathcal{I}_Y$$

$$\mathcal{I}_{X\cap Y} = \mathcal{I}_X + \mathcal{I}_Y$$

$$\mathcal{I}_{X\cup Y} = \mathcal{I}_X \cap \mathcal{I}_Y.$$

We say $X \subset Y$ if $\mathcal{I}_Y \subset \mathcal{I}_X$. Let $f : V \to W$ be a morphism of projective varieties. Then for any closed subscheme $X \subset V$ and $Z \subset W$ we define the scheme-theoretic image $f(X)$ by $\mathcal{I}_{f(X)} = \mathrm{Ker}(\mathcal{O}_W \to f_*\mathcal{O}_X)$ and the scheme theoretic inverse image f^*Z by $\mathcal{I}_{f^*Z} = f^{-1}\mathcal{I}_Z \cdot \mathcal{O}_V$.

Lemma 2.3.1. *Let $f : V \to W$ be a morphism of projective varieties and let $Z \subset W$ be a closed subscheme. The scheme theoretic inverse image f^*Z is the fibered product*

$$\begin{array}{ccc} f^*Z & \longrightarrow & V \\ \downarrow & & \downarrow f \\ Z & \longrightarrow & W \end{array}$$

of Z and V over W, that is $f^*Z = Z \times_W V$.

Proof. See Tag 01JU on The Stacks Project [15, Lemma 01JU]. □

Lemma 2.3.2. *Let $f : V \to W$ be a morphism of projective varieties. Then for any Zariski-closed subschemes $X \subset V$ and $Z \subset W$,*

(a) $X \subset f^*(f(X))$

(b) $f(f^*Z) \subset Z$

Proof. (a) By definition of $f(X)$ we get a commutative diagram of sheaves,

$$\begin{array}{ccc} f_*\mathcal{O}_X & \longleftarrow & f_*\mathcal{O}_V \\ \uparrow & & \uparrow f^\# \\ \mathcal{O}_W/\mathcal{I}_{f(X)} & \longleftarrow & \mathcal{O}_W \end{array}$$

to which the corresponding commutative diagram of schemes is as follows.

$$\begin{array}{ccc} X & \longrightarrow & V \\ \downarrow & & \downarrow f \\ f(X) & \longrightarrow & W \end{array}$$

By the universal property of the fibered product, there exists a unique morphism $X \to f(X) \times_W V$ such that the following diagram commutes.

$$\begin{array}{ccc} X & \longrightarrow & f(X) \times_W V \\ & \searrow & \downarrow \varphi \\ & & V \end{array}$$

By Lemma 2.3.1, $f(X) \times_W V$ is the inverse image $f^*(f(X))$ and the map φ is a closed immersion. Thus we also get the commutative diagram of structure sheaves,

$$\begin{array}{ccc} \mathcal{O}_V/\mathcal{I}_X & \longleftarrow & \mathcal{O}_V/\mathcal{I}_{f^*(f(X))} \\ & \nwarrow & \uparrow{\scriptstyle \varphi^\#} \\ & & \mathcal{O}_V \end{array}$$

which implies that $\mathcal{I}_{f^*(f(X))} \subset \mathcal{I}_X$, that is $X \subset f^*(f(X))$.

(b) By Lemma 2.3.1, we know that $f^*Z = Z \times_W V$. Thus we get the corresponding commutative diagram of sheaves,

$$\begin{array}{ccc} f_*\mathcal{O}_{f^*Z} & \longleftarrow & f_*\mathcal{O}_V \\ \uparrow & & \uparrow{\scriptstyle f^\#} \\ \mathcal{O}_W/\mathcal{I}_Z & \longleftarrow & \mathcal{O}_W \end{array}$$

from which it follows that $\mathcal{I}_Z \subset \mathrm{Ker}(\mathcal{O}_W \to f_*\mathcal{O}_{f^*Z}) = \mathcal{I}_{f(f^*Z)}$, that is $f(f^*Z) \subset Z$.

□

Lemma 2.3.3. *Let $X \subset V$ be a closed subscheme. There exist effective divisors $D_1, \ldots, D_r$ such that $X = \bigcap D_i$.*

Proof. See [13, Lemma 2.2]. □

Given such $D_1, \ldots, D_r$, we define the local heights corresponding to the closed subscheme X to be $\lambda_{X,v} := \min_i\{\lambda_{D_i,v}\}$, for all places $v \in M_k$. note that on $\mathrm{Supp}(D_i)$ we may think of $\lambda_{D_i,v}$ as having value ∞ so that $\lambda_{X,v}$ is defined (up to a bounded function) outside $\bigcap \mathrm{Supp}(D_i) = \mathrm{Supp}(X)$.

Theorem 2.3.4. *Let V be a projective variety defined over a number field k and let $v \in M_k$. Then up to a bounded function we have the following:*

(a) For all closed subschemes $X \subset V$ and places $v \in M_k$, the local height $\lambda_{X,v}$ is well-defined, up to a bounded function, independent of the choice of effective divisors $D_1, \ldots, D_r$.

(b) For all closed subschemes $X, Y \subset V$,

$$\lambda_{X\cap Y,v} = \min\{\lambda_{X,v}, \lambda_{Y,v}\}.$$

(c) For all closed subschemes $X, Y \subset V$,

$$\lambda_{X+Y,v} = \lambda_{X,v} + \lambda_{Y,v}.$$

(d) If closed subschemes $X, Y \subset V$ satisfy $X \subset Y$, then

$$\lambda_{X,v} \leq \lambda_{Y,v}.$$

(e) For all closed subschemes $X, Y \subset V$,

$$\max\{\lambda_{X,v}, \lambda_{Y,v}\} \leq \lambda_{X\cup Y,v} \leq \lambda_{X,v} + \lambda_{Y,v}.$$

(f) If closed subschemes $X, Y \subset V$ satisfy $\mathrm{Supp}(X) \subset \mathrm{Supp}(Y)$, then there exists a constant $c \geq 0$ such that

$$\lambda_{X,v} \leq c\lambda_{Y,v}.$$

(g) Let $\varphi : W \to V$ be a morphism of varieties, and let $X \subset V$ be a closed subscheme. Then

$$\lambda_{W,\varphi^* X,v} = \lambda_{V,X,v} \circ \varphi.$$

Proof. See [13, Theorem 2.1]. □

CHAPTER 3

PREPARATION

3.1 Useful Results

Given a nonsingular variety V defined over a number field k and a closed subscheme X, and given $D_1, \ldots, D_r$ such that $X = \bigcap_{i=1}^{r} D_i$, we define the local heights corresponding to the closed subscheme X to be

$$\lambda_{X,v}(P) := \min_{1 \le i \le r} \{\lambda_{D_i,v}(P)\}$$

for all points $P \in V \setminus X$ and all places $v \in M_k$. These are well-defined by Theorem 2.3.4. For a set of places $S \subset M_k$ we similarly define

$$m_{X,S}(P) := \sum_{v \in S} \lambda_{X,v}(P).$$

Faltings generalized Siegel's approximation result on elliptic curves to abelian varieties as follows.

Theorem 3.1.1. *Let V be an abelian variety over a number field k. Let S be a finite set of places of k. Let $X \subset V$ be a closed subscheme and A an ample divisor on V. Let $\varepsilon > 0$. Then for any $P \in V(k) \setminus \mathrm{Supp}(X)$*

$$m_{X,S}(P) \le \varepsilon h_A(P) + O(1).$$

Proof. See [5, Theorem 2]. □

Roth's theorem was also generalized to higher dimensional projective spaces.

Theorem 3.1.2 (Schmidt's Subspace Theorem)**.** *Let k be a number field. Let S be a finite set of places of k. For each $v \in S$ let $\{L_{0v}, \ldots, L_{nv}\}$ be a linearly independent set of linear forms in the variables $x_0, \ldots, x_n$, with coefficients in k and let H_{iv} be the hyperplane in $\mathbb{P}^n$ associated with the linear form L_{iv}. Let $\varepsilon > 0$. Then there exists a finite set $\mathcal{H}$ of hyperplanes of $\mathbb{P}^n_k$ such that for all $P \in \mathbb{P}^n_k \setminus \bigcup_{H \in \mathcal{H}} H$*

$$\sum_{v \in S} \sum_{i=0}^{n} \lambda_{H_{iv},v}(P) \le (N_d(D) + 1 + \varepsilon) h(P).$$

Proof. See [1, Chapter 7]. □

We say a set of $m+1$ hyperplanes in $\mathbb{P}^n$ is in j**-subgeneral position** if $n \leq j \leq m$ and any subset of size $j+1$ of the hyperplanes will have empty intersection. In this case we get the following result of Ru and Wong.

Theorem 3.1.3. *Let k be a number field. Let S be a finite set of places of k. Let $\{H_0, \ldots, H_m\}$ be a set of hyperplanes in $\mathbb{P}^n$ in d-subgeneral position. Let $\varepsilon > 0$. Then there exists a finite set $\mathcal{H}$ of hyperplanes of $\mathbb{P}^n_k$ such that for all $P \in \mathbb{P}^n_k \setminus \bigcup_{H\in\mathcal{H}} H$*

$$\sum_{i=0}^{m} m_{H_i,S}(P) \leq (2d - N_d(D) + 1 + \varepsilon)h(P).$$

Proof. See [12, Theorem 3.5]. □

Generalizations of the subspace theorem to projective varieties have been given, independently, by Corvaja and Zannier [3, Theorem 3] and by Evertse and Ferretti, whose version we state.

Theorem 3.1.4 (Evertse-Ferretti)**.** *Let X be a projective subvariety of $\mathbb{P}^N$ of dimension $n \geq 1$ defined over a number field k. Let S be a finite set of places of k. For all $v \in S$, let $H_{0,v}, \ldots, H_{n,v} \in \mathbb{P}^N$ be hypersurfaces over k such that*

$$X \cap H_{0,v} \cap \cdots \cap H_{n,v} = \emptyset$$

Let $\varepsilon > 0$. Then there exists a proper Zariski-closed subscheme $Z \subset X$ such that, for all points $P \in X(k) \setminus Z$,

$$\sum_{v\in S} \sum_{i=0}^{n} \frac{\lambda_{H_{i,v},v}(P)}{\deg H_{i,v}} < (N_d(D) + 1 + \varepsilon)h(P).$$

Proof. See [4, Theorem 1.1] □

This may be reformulated in terms of divisors as follows.

Theorem 3.1.5 (Evertse-Ferretti, reformulated)**.** *Let X be a projective variety of dimension n defined over a number field k. Let S be a finite set of places of k. For each $v \in S$ let $D_{0,v}, \ldots, D_{n,v}$ be effective divisors on X, defined over k, in general position. Suppose there exists an ample divisor*

A and positive integers $d_{i,v}$ such that $D_{i,v}$ is linearly equivalent to $d_{i,v}A$ for all i and for all $v \in S$. Let $\varepsilon > 0$. Then there exists a proper Zariski-closed subscheme $Z \subset X$ such that for all points $P \in X(k) \setminus Z$,

$$\sum_{v \in S} \sum_{i=0}^{n} \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq (N_d(D) + 1 + \varepsilon) h_A(P) + O(1).$$

Proof. See [9, Theorem 3.1] □

Levin proved that the linear equivalence in this reformulation may be replaced by numerical equivalence.

Theorem 3.1.6. *Let X be a projective variety of dimension n defined over a number field k. Let S be a finite set of places of k. For each $v \in S$ let $D_{0,v}, \ldots, D_{n,v}$ be effective divisors on X, defined over k, in general position. Suppose there exists an ample divisor A and positive integers $d_{i,v}$ such that $D_{i,v}$ is numerically equivalent to $d_{i,v}A$ for all i and for all $v \in S$. Let $\varepsilon > 0$. Then there exists a proper Zariski-closed subscheme $Z \subset X$ such that for all points $P \in X(k) \setminus Z$,*

$$\sum_{v \in S} \sum_{i=0}^{n} \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq (N_d(D) + 1 + \varepsilon) h_A(P) + O(1).$$

Proof. See [9, Theorem 3.2]. □

Let k be a number field and let S be a finite set of places of k containing all archimedean places. The ring of S-integers, denoted $\mathcal{O}_S$, is defined to be the set of all $x \in k$ such that $|x|_v \leq 1$ for all $v \notin S$. If S consists of only the archimedean places, we call these the ring of integers of k, denoted $\mathcal{O}_k$. If V is a projective variety over k and D a very ample effective divisor on V with $\mathbf{x} = (x_0 = 1, x_1, \ldots, x_n)$ a basis for $\mathcal{L}(D)$, then the map $P \mapsto (x_1(P), x_2(P), \ldots, x_n(P))$ defines an embedding of $V \setminus \mathrm{Supp}(D)$ into $\mathbb{A}^n$. We say a point $P \in V(k) \setminus \mathrm{Supp}(D)$ is $(D, \mathbf{x}, S)$-**integral** if $x_i(P) \in \mathcal{O}_S$ for $0 \leq i \leq n$. note that for any point $P \in V(k) \setminus \mathrm{Supp}(D)$, we may choose a $b \in \mathcal{O}_k$ which clears the denominators of $x_i(P)$, $1 \leq i \leq n$, so that $\mathbf{x}' = (x_0 = 1, bx_1, \ldots, bx_n)$ is a basis of $\mathcal{O}(D)$ such that P is $(D, \mathbf{x}', S)$-integral. In order to find a more intrinsic definition, we need to look at sets of points.

Lemma 3.1.7. *Let D be a very ample effective divisor on V. Let $\mathcal{R}$ be a subset of $V(k) \setminus \mathrm{Supp}(D)$. Then the following are equivalent.*

(a) *There exists a basis $\mathbf{x} = (x_0 = 1, x_1, \ldots, x_n)$ of $O(D)$ such that $\mathcal{R}$ is a set of $(D, \mathbf{x}, S)$-integral points.*

(b) *There exists a presentation $\mathcal{D}$ of D and an M_k-constant γ such that for all $P \in \mathcal{R}$ and all $v \in M_k \setminus S$,*

$$\lambda_{\mathcal{D},v}(P) \leq \gamma_v.$$

Proof. See [16, Lemma 1.4.1]. □

Going back to Roth's theorem, if the points P_i are not distinct we can still say the following.

Theorem 3.1.8 (Roth's Theorem with Multiplicities)**.** *Let S be a finite set of places of a number field k. Let $P_1, \ldots, P_n \in \mathbb{P}^1_k$ be distinct points and let $c_1, c_2, \ldots c_n$ be positive integers with $c_1 \geq c_2 \geq \cdots \geq c_n$. Let $D = \sum_{i=1}^n c_i P_i$ and let $\varepsilon > 0$. Then for $P \in \mathbb{P}^1_k$*

$$m_{D,S}(P) < (c_1 + c_2 + \varepsilon)h(P) + O(1).$$

Proof. See [10, Theorem 2.1]. □

3.2 Sharpness of the Main Result

Let C be a nonsingular projective curve defined over a number field k. Fix a point $R \in C(k)$. For $P \in C(\overline{k})$, let $k(P)$ be the field of definition of P (the field extension of k generated by its local coordinates).

Theorem 3.2.1. *Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $\varepsilon > 0$. Denote the set of archimedean places of k by $S_{k,\infty}$. Then there exists a finite extension k' of k and*

an infinite collection of points $P \in C(\overline{k})$ with $[k'(P) : k'] \leq d$ satisfying

$$m_{D,S_{k',\infty}}(P) \geq (N - \varepsilon)h_R(P) + O(1)$$

where $N_d(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ *taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree d.*

Proof. By finitely extending k to k', we may assume $O^*_{k'}$ is an infinite set.

Since D is effective, we know $m_{D,S_{k',\infty}} \geq O(1)$, so we may assume $N \geq 1$. For each k-morphism $\sigma : C \to \mathbb{P}^1$ of degree d, let $\sigma(\mathrm{Supp}(D)) = \{T_1, T_2, \ldots, T_r\}$ and define $n_i = n_i(\sigma) := |\sigma^{-1}(T_i) \cap \mathrm{Supp}(D)|$ for $i = 1, 2, \ldots, r$. Reorder indices so that $n_1 \geq n_2 \geq \ldots \geq n_r$. Then choose a morphism σ with $T_1 = 0$ and $T_2 = \infty$ such that $n_1(\sigma) + n_2(\sigma) = N$.

We consider the infinite set of points $P \in C(\overline{k})$ satisfying $\sigma(P) = (\alpha, 1)$ for some $\alpha \in O^*_{k'}$. For each $v \in M_{k'}$ define the local height $\lambda_{0+\infty,v}$ on $\mathbb{P}^1$ by

$$\lambda_{0+\infty,v}((a,b)) := \log \max_{0\leq i\leq 1}\left\{\left|\frac{x_i^2}{x_0x_1}\right|_v\right\}\Bigg|_{(a,b)} = \log\max\left\{\left|\frac{a}{b}\right|_v, \left|\frac{b}{a}\right|_v\right\}.$$

Since $\lambda_{0+\infty,v}(\sigma(P)) = \log\max\left\{|\alpha|_v, \left|\frac{1}{\alpha}\right|_v\right\}$ for all $v \in M_{k'}$, we see that $\lambda_{0+\infty,v}(\sigma(P)) = 0$ for $v \in M_{k'} \setminus S_{k',\infty}$ by definition of $O^*_{k'}$. Thus

$$\begin{aligned}
m_{\sigma^*(0+\infty),S_{k',\infty}}(P) &= \sum_{v\in S_{k',\infty}} \lambda_{\sigma^*(0+\infty),v}(P) + O(1)\\
&= \sum_{v\in S_{k',\infty}} \lambda_{0+\infty,v}(\sigma(P)) + O(1)\\
&= \sum_{v\in M_{k'}} \lambda_{0+\infty,v}(\sigma(P)) + O(1)\\
&= h_{0+\infty}(\sigma(P)) + O(1)\\
&= h_{\sigma^*(0+\infty)}(P) + O(1)
\end{aligned}$$

For any effective divisor E on C and $v \in M_{k'}$, we have $\lambda_{E,v}(P) \geq 0$. Thus we have $m_{E,S_{k',\infty}}(P) = \sum_{v\in S_{k',\infty}} \lambda_{E,v}(P) \leq \sum_{v\in M'_k} \lambda_{E,v}(P) = h_E(P)$. So if $\sigma^*(0+\infty) = \sum_{i=1}^m Q_i$ then $m_{Q_i,S_{k',\infty}}(P) \leq$

$h_{Q_i}(P)$ and

$$\begin{aligned}\sum_{i=1}^{m} m_{Q_i,S_{k'},\infty}(P) &= m_{\sigma^*(0+\infty),S_{k'},\infty}(P) + O(1)\\ &= h_{\sigma^*(0+\infty)}(P) + O(1)\\ &= \sum_{i=1}^{m} h_{Q_i}(P) + O(1).\end{aligned}$$

Therefore in fact $m_{Q,S_{k'},\infty}(P) = h_Q(P)$ for all $Q \in \mathrm{Supp}(\sigma^*(0+\infty))$. So

$$\begin{aligned}m_{D,S_{k'},\infty}(P) &= \sum_{Q\in\mathrm{Supp}(D)} m_{Q,S_{k'},\infty}(P) + O(1)\\ &\geq \sum_{Q\in\mathrm{Supp}(D)\cap\mathrm{Supp}(\sigma^*(0+\infty))} m_{Q,S_{k'},\infty}(P) + O(1)\\ &= \sum_{Q\in\mathrm{Supp}(D)\cap\mathrm{Supp}(\sigma^*(0+\infty))} h_Q(P) + O(1)\\ &\geq (n_1(\sigma) + n_2(\sigma) - \varepsilon)h_R(P) + O(1) \text{ by Theorem 2.2.12}\\ &= (N - \varepsilon)h_R(P) + O(1).\end{aligned}$$

□

3.3 Facts on Trigonal Maps

From this point forward the symbol $\sim$ will refer to linear equivalence of divisors on a variety.

We will make frequent use of the following theorem about divisors on curves. For a divisor D on a nonsingular projective curve C, let $l(D) := \dim_k H^0(C, \mathcal{O}(D))$.

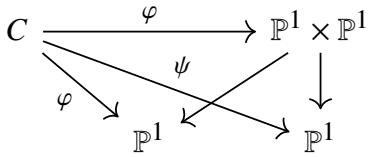
Theorem 3.3.1 (Riemann-Roch Theorem)**.** *Let D be a divisor on a curve C of genus g. Let K be a canonical divisor on C. Then*

$$l(D) - l(K - D) = \deg D + 1 - g.$$

Proof. See [7, Theorem IV.1.3]. □

Lemma 3.3.2. *Let C be a curve of genus $g \geq 3$ defined over k. Then C cannot be both hyperelliptic and trigonal.*

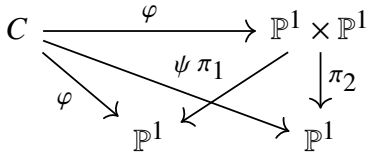
Proof. Suppose C is both hyperelliptic and trigonal. Then there exist finite morphisms $\varphi : C \to \mathbb{P}^1$ and $\psi : C \to \mathbb{P}^1$ of degrees 2 and 3 respectively. By the universal property of fibered products there exists a unique morphism $\varphi : C \to \mathbb{P}^1 \times \mathbb{P}^1$ such that the following diagram commutes.



By the commutative diagram we see the degree of φ divides the degrees of φ and ψ, that is 2 and 3, so the degree of φ is 1, meaning φ is a birational morphism. Thus $\varphi(C)$ is an irreducible curve on $\mathbb{P}^1 \times \mathbb{P}^1$ of type $(2, 3)$. It follows that the genus of C is bounded above by the formula $(d_1 - 1)(d_2 - 2)$ for the genus of a nonsingular curve of type (d_1, d_2) on $\mathbb{P}^1 \times \mathbb{P}^1$. That is to say $g \leq (2 - 1)(3 - 1) = 2$. □

Lemma 3.3.3. *Let C be a curve of genus $g \geq 5$ defined over k. Then C can be trigonal in at most one way (up to k-automorphism).*

Proof. Suppose C is trigonal in more than one way. Then there exist two finite morphisms $\varphi : C \to \mathbb{P}^1$ and $\psi : C \to \mathbb{P}^1$ of degree 3, distinct even up to an automorphism of $\mathbb{P}^1$. By the universal property of fibered products there exists a unique morphism $\varphi : C \to \mathbb{P}^1 \times \mathbb{P}^1$ such that the following diagram commutes.



By the commutative diagram we see the degree of φ divides the degrees of φ and ψ, so the degree of φ is either 1 or 3. However if the degree of φ is 3 then the projections π_1 and π_2 each have degree 1, so $\pi_1|_{\varphi(C)}$ and $\pi_2|_{\varphi(C)}$ are birational maps. Thus $\pi_1|_{\varphi(C)} \circ \pi_2|^{-1}_{\varphi(C)}$ is a birational map

from $\mathbb{P}^1$ to $\mathbb{P}^1$, which necessarily extends to a k-automorphism. But then $\varphi = \pi_1|_{\varphi(C)} \circ \pi_2|^{-1}_{\varphi(C)} \circ \psi$, a contradiction since φ and ψ were distinct trigonal maps up to k-automorphism of $\mathbb{P}^1$.

Thus we conclude the degree of φ is 1, meaning φ is a birational morphism. Then $\varphi(C)$ is an irreducible curve on $\mathbb{P}^1 \times \mathbb{P}^1$ of type $(3, 3)$. It follows that the genus of C is bounded above by the formula $(d_1 - 1)(d_2 - 2)$ for the genus of a nonsingular curve of type (d_1, d_2) on $\mathbb{P}^1 \times \mathbb{P}^1$. That is to say $g \leq (3 - 1)(3 - 1) = 4$. □

Lemma 3.3.4. *Let C be a curve of genus $g = 3$ defined over k. Then C has only finitely many distinct trigonal k-morphisms up to k-automorphism of $\mathbb{P}^1$.*

Proof. Let $\varphi : C \to \mathbb{P}^1$ be a finite k-morphism of degree 3. Let D be an effective divisor defined over k in the corresponding base-point free linear system. Then $\deg(D) = 3$, $l(D) = 2$. By Riemann-Roch, $l(K - D) = 1$, which is to say there exists a unique point $P \in C(\overline{k})$ such that $K - D \sim P$. Since $K - D$ is defined over k it follows that P is k-rational.

If $\psi : C \to \mathbb{P}^1$ is another trigonal morphism and E a corresponding divisor such that $K - E \sim P$ then $D \sim E$, implying φ and ψ correspond to the same linear system. Thus φ and ψ are equivalent up to automorphism of $\mathbb{P}^1$.

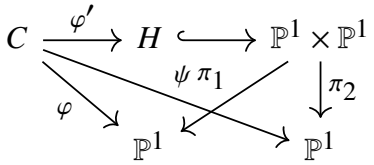
By Falting's Theorem, there exists at most finitely many k-rational points on C. Since each trigonal k-morphism has a corresponding k-rational point and no two distinct trigonal k-morphisms correspond to the same point, it follows that there are finitely many trigonal k-morphisms up to automorphism of $\mathbb{P}^1$. □

Lemma 3.3.5. *Let C be a curve of genus $g = 4$ defined over k. Then C can be trigonal in at most two distinct ways up to a k-automorphism of $\mathbb{P}^1$.*

Proof. Suppose C is trigonal in more than one way. Then there exist two finite morphisms $\varphi : C \to \mathbb{P}^1$ and $\psi : C \to \mathbb{P}^1$ of degree 3, distinct even up to a k-automorphism of $\mathbb{P}^1$. Let D and E be corresponding effective divisors of the respective base-point free linear systems. Let $(1, f)$ and $(1, g)$ be local equations for φ and ψ. Because $D + E + (1)$, $D + E + (f)$, $D + E + (g)$, and

$D + E + (f \cdot g)$ are all effective divisors, we can think of the functions 1, f, g, and $f \cdot g$ as elements of $L(D + E)$.

Assume 1, f, g, and $f \cdot g$ are k-linearly dependent. Consider the map $\varphi : C \to \mathbb{P}^1 \times \mathbb{P}^1$ given by $(\varphi, \psi) = (1, f) \times (1, g)$. Composing with the Segre embedding gives a map $C \to \mathbb{P}^3$ with coordinates $(1, f, g, f \cdot g)$. Since these are k-linearly dependent, the image lies in a hyperplane in $\mathbb{P}^3$. A hyperplane in $\mathbb{P}^3$ cuts out a curve of type $(1, 1)$ in $\mathbb{P}^1 \times \mathbb{P}^1$. Thus the image of φ lies in a curve H of type $(1, 1)$. Since neither φ nor ψ is constant, H must be a copy of $\mathbb{P}^1$ embedded in $\mathbb{P}^1 \times \mathbb{P}^1$. Thus we get an induced morphism $\varphi' : C \to H$ satisfying the following commutative diagram.



Since H has type $(1, 1)$ it follows that the projections $\pi_1|_H$ and $\pi_2|_H$ restricted to H are morphisms of degree 1 from $\mathbb{P}^1$ to itself, that is automorphisms of $\mathbb{P}^1$. Thus $\varphi = \pi_1|_H \circ \pi_2|_H^{-1} \circ \psi$, a contradiction since φ and ψ were distinct trigonal maps up to k-automorphism of $\mathbb{P}^1$. Thus we see the four functions 1, f, g, and $f \cdot g$ must in fact be k-linearly independent. Therefore $l(D + E) = \dim_k L(D + E) \geq 4$.

By Riemann-Roch we have $l(K - D - E) = l(D + E) - 3 \geq 1$. Since $\deg(K - D - E) = 0$ we conclude $K - D - E \sim 0$, that is $D + E$ is a canonical divisor.

Let $\xi : C \to \mathbb{P}^1$ be a finite morphism of degree 3 with corresponding effective divisor F. If ξ is not equivalent to φ (up to a k-automorphism of $\mathbb{P}^1$) then the same argument shows that $D + F$ is a canonical divisor. Thus $E \sim F$, implying ψ and ξ have the same corresponding linear system, which is to say ξ is equivalent to ψ. □

CHAPTER 4

PROOF OF THE MAIN THEOREM

4.1 Algebraic Points on Curves

A divisor B on a projective variety X of dimension n is called **big** if there exists an $a > 0$ and $j_0 > 0$ such that $H^0(V, \mathcal{O}_V(jB)) \geq aj^n$ for all $j > j_0$.

Lemma 4.1.1 (Kodaira's Lemma)**.** *Let B be a big divisor and D an arbitrary divisor on a nonsingular projective variety V. Then for $m \gg 0$,*

$$H^0(V, \mathcal{O}_V(mB - D)) \neq 0.$$

Corollary 4.1.2. *Let A be an ample divisor and D an arbitrary divisor on a nonsingular projective variety V. Then for $m \gg 0$, $h_D(P) \leq mh_A(P) + O(1)$ for all $P \in V(k)$.*

Proof. Since ample divisors are big, by Kodaira's Lemma we have

$$H^0(V, \mathcal{O}_V(mA - D)) \neq 0$$

for $m \gg 0$. So there exists an effective divisor E such that $mA \sim D + E$. Choose an $n \in \mathbb{Z}$ so that $E + nA$ is very ample.

$$\begin{aligned}(m+n)h_A(P) &= h_{(m+n)A}(P) + O(1) \\ &= h_{D+E+nA}(P) + O(1) \\ &= h_D(P) + h_{E+nA}(P) + O(1) \\ &\geq h_D(P) + O(1).\end{aligned}$$

□

Let C be a nonsingular projective curve of genus $g \geq 1$ defined over a number field k. Fix a point $R \in C(k)$. For $Q \in \{P \in C : [k(P) : k] = d\}$ let $\tilde{Q}_1, \ldots, \tilde{Q}_d$ be the Galois conjugates of Q, in some order, and define $\bar{Q} = (\tilde{Q}_1, \ldots, \tilde{Q}_d) \in C^d$ and $\varphi : C^d \to \mathrm{Sym}^d(C)$ by

$(P_1, \ldots, P_d) \mapsto P_1 + \ldots + P_d$. We identify $\mathrm{Sym}^d(C)$ with the set of effective divisors of degree d on C. Let $\pi_1 : C^d \to C$ be the first projection and let $\mu : \mathrm{Sym}^d(C) \to \mathrm{Jac}(C)$ be the map given by $P_1 + \ldots + P_d \mapsto O_C(P_1 + \ldots + P_d - dR)$.

We'll need the following Lemma, as shown in [9].

Lemma 4.1.3. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$*

$$m_{D,S}(Q) = \frac{1}{d} m_{\varphi_* \pi_1^* D,S}(\varphi(\bar{Q})) + O(1) \text{ and } h_R(Q) = \frac{1}{d} h_{\varphi_* \pi_1^* R}(\varphi(\bar{Q})) + O(1).$$

Proof. Since local heights are invariant under Galois maps,

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{d} \sum_{i=1}^{d} m_{D,S}(\tilde{Q}_i) + O(1) \\ &= \frac{1}{d} \sum_{i=1}^{d} m_{D,S}(\pi_i(\bar{Q})) + O(1) \\ &= \frac{1}{d} \sum_{i=1}^{d} m_{\pi_i^* D,S}(\bar{Q}) + O(1) \\ &= \frac{1}{d} m_{\sum_{i=1}^{d} \pi_i^* D,S}(\bar{Q}) + O(1) \\ &= \frac{1}{d} m_{\varphi^* \varphi_* \pi_1^* D,S}(\bar{Q}) + O(1) \\ &= \frac{1}{d} m_{\varphi_* \pi_1^* D,S}(\varphi(\bar{Q})) + O(1). \end{aligned}$$

The proof for global heights is identical. □

Theorem 4.1.4. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ and $\mu(\varphi(\bar{Q})) \notin \mu(\varphi_* \pi_1^*(D))$,*

$$m_{D,S}(Q) \leq \varepsilon h_R(Q) + O(1).$$

Proof. note that $\varphi_* \pi_1^*(D)$ is an effective divisor on $\mathrm{Sym}^d(C)$ and so a closed subscheme of dimension $d - 1$. By Lemma 2.3.2(a), $\varphi_* \pi_1^*(D) \subset \mu^*(\mu(\varphi_* \pi_1^*(D)))$. Let A be an ample divisor on $\mathrm{Jac}(C)$.

note that $\varphi_*\pi_1^*R$ is also ample. By Corollary 4.1.2 there exists an integer $m > 0$ such that

$$h_{\mu^*A}(E) \leq m h_{\varphi_*\pi_1^*R}(E) + O(1)$$

for all $E \in \mathrm{Sym}^d(C)$. Furthermore, for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ and $\mu(\varphi(\bar{Q})) \notin \mu(\varphi_*\pi_1^*(D))$,

$$\begin{aligned}
m_{\varphi_*\pi_1^*D,S}(\varphi(\bar{Q})) &\leq m_{\mu^*(\mu(\varphi_*\pi_1^*D)),S}(\varphi(\bar{Q})) + O(1) \text{ by Theorem 2.3.4(d)} \\
&= m_{\mu(\varphi_*\pi_1^*D),S}(\mu \circ \varphi(\bar{Q})) + O(1) \\
&\leq \frac{\varepsilon}{m} h_A(\mu \circ \varphi(\bar{Q})) + O(1) \text{ by Theorem 3.1.1} \\
&= \frac{\varepsilon}{m} h_{\mu^*A}(\varphi(\bar{Q})) + O(1) \\
&\leq \varepsilon h_{\varphi_*\pi_1^*R}(\varphi(\bar{Q})) + O(1) \text{ by Corollary 4.1.2.}
\end{aligned}$$

By Lemma 4.1.3, the desired result holds on C. □

Conversely, we see the following lemma.

Lemma 4.1.5. *Let C be a nonsingular projective curve of genus g defined over a number field k. Let $P \in C(k)$ and let $Q \in C(\overline{k})$ with $[k(Q) : k] = d$. Suppose that $\mu(\varphi(\bar{Q})) \in \mu(\varphi_*\pi_1^*(D))$, that is*

$$\tilde{Q}_1 + \cdots + \tilde{Q}_d \sim P + R_1 + \cdots + R_{d-1}$$

for some points $R_j \in C(\overline{k})$. If

$$g \geq \begin{cases} 1 & \text{when } d = 2 \\ 2 & \text{when } d = 3 \end{cases}$$

then $R_j \neq \tilde{Q}_k$ for any j and k. In particular, there exists a k-morphism $\sigma : C \to \mathbb{P}^1$ of degree d such that $\sigma^*(\sigma(Q)) = \tilde{Q}_1 + \cdots + \tilde{Q}_d$.

Furthermore if $d = 4$ and $g \geq 5$, then we also get such a k-morphism, provided $\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4$ is not a sum of two hyperelliptic divisors on C.

Proof. note that because $[k(P) : k] = 1$ and $[k(\tilde{Q}_j) : k] = d > 1$, we know $\tilde{Q}_j \neq P$ for all $1 \leq j \leq d$.

Without loss of generality, assume $R_{d-1} = \tilde{Q}_d$, so that cancelling like terms would leave us with

$$\tilde{Q}_1 + \cdots + \tilde{Q}_{d-1} \sim P + R_1 + \cdots + R_{d-2}.$$

If $d = 2$, then this says $\tilde{Q}_1 \sim P$, implying either $\tilde{Q}_1 = P$ or $g = 0$. But $\tilde{Q}_1 \neq P$ and by hypothesis $g \geq 1$. Thus we reach a contradiction.

If $d = 3$, then this says $\tilde{Q}_1 + \tilde{Q}_2 \sim P + R_1$. If one of $\tilde{Q}_1$ and $\tilde{Q}_2$ is equal to one of P and R_1, then since P is not equal to $\tilde{Q}_1$ or $\tilde{Q}_2$, this would imply R_1 is equal to either $\tilde{Q}_1$ or $\tilde{Q}_2$, so P is linearly equivalent to one of $\tilde{Q}_1$ and $\tilde{Q}_2$ further implying $g = 0$, a contradiction. On the other hand, if the points on the left side of the linear equivalence are distinct from the points on the right side then there exists a morphism $\sigma : C \to \mathbb{P}^1$ of degree two such that $\sigma(P) = \sigma(R_1)$. Since $g \geq 2$, this says C is hyperelliptic. Since P is a k-rational point and the unique hyperelliptic map σ is a k-morphism, R_1 must be k-rational as well. Let $\xi \in \mathrm{Gal}\left(\overline{k}/k\right)$. Then $\xi(R_2) \sim \xi(\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3) - P - R_1 = \tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 - P - R_1 \sim R_2$. Since $g > 0$, $\xi(R_2) = R_2$. Since ξ was arbitrary, R_2 is k-rational, contradicting the assumption $R_2 = \tilde{Q}_3$ since $\tilde{Q}_3$ is a cubic point over k.

If $d = 4$, then this says $\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 \sim P + R_1 + R_2$. Since $g \geq 5$, there exists at most one trigonal map (up to automorphism of $\mathbb{P}^1$), at most one hyperelliptic map (up to automorphism of $\mathbb{P}^1$), and not both. If C has a unique trigonal map σ with $\sigma(P) = \sigma(R_1) = \sigma(R_2)$, by uniqueness, σ is k-rational, else we could use Galois conjugation to get a new hyperelliptic morphism. Since P is a k-rational point, we see that R_1 and R_2 are at worst quadratic conjugates. Thus for any $\xi \in \mathrm{Gal}\left(\overline{k}/k\right)$, we have $\xi(R_3) \sim \xi(\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4) - P - \xi(R_1 + R_2) = \tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4 - P - R_1 - R_2 \sim R_3$. Since $g > 0$, $\xi(R_3) = R_3$. Since ξ was arbitrary, R_3 is a k-rational point, contradicting the assumption $R_3 = \tilde{Q}_4$, since $\tilde{Q}_4$ is a quartic point over k.

If this does not give a trigonal map, say $R_2 = \tilde{Q}_3$ as well, then C has a unique hyperelliptic map σ with $\sigma(\tilde{Q}_1) = \sigma(\tilde{Q}_2)$ and $\sigma(P) = \sigma(R_1)$ and by the same argument in the $d = 3$ case, R_1 is

k-rational. Thus for any $\xi \in \mathrm{Gal}\left(\overline{k}/k\right)$, we have $\xi(R_2 + R_3) \sim \xi(\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4) - P - R_1 = \tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4 - P - R_1 \sim R_2 + R_3$. So $\sigma(R_2) = \sigma(R_3)$. But $R_2 = \tilde{Q}_3$ and $R_3 = \tilde{Q}_4$, so $\sigma(\tilde{Q}_3) = \sigma(\tilde{Q}_4)$, meaning $\tilde{Q}_1 + \tilde{Q}_2 + \tilde{Q}_3 + \tilde{Q}_4$ is a sum of two hyperelliptic divisors on C, contradicting the hypothesis. □

Theorem 4.1.6. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\sigma : C \to \mathbb{P}^1$ be a k-morphism of degree d. Let $\sigma(\mathrm{Supp}(D)) = \{T_1, T_2, \ldots, T_r\}$ and define $n_i = n_i(\sigma) := |\sigma^{-1}(T_i) \cap \mathrm{Supp}(D)|$ for $i = 1, 2, \ldots, r$. Reorder indices so that $n_1 \geq n_2 \geq \ldots \geq n_r$. Let $\varepsilon > 0$. Then for all $Q \in C \setminus \mathrm{Supp}(D)$ with $[k(Q) : k] = d$ and $\sigma(Q) \in \mathbb{P}^1(k)$*

$$m_{D,S}(Q) \leq (n_1 + n_2 + \varepsilon)h_R(Q) + O(1)$$

Proof. Let $\iota : \mathbb{P}^1 \to \mathrm{Sym}^d(C) \subset \mathrm{Div}^+(C)$ be given by $\iota(T) = \sigma^*(T)$. Then ι is an embedding with $\iota^*\varphi_*\pi_1^* = \sigma_*$. Since $\sigma(Q) \in \mathbb{P}^1(k)$, any Galois map over k will only permute the set $\sigma^{-1}(\sigma(Q))$ implying $\iota \circ \sigma(Q) = \sigma^*(\sigma(Q)) = \tilde{Q}_1 + \cdots + \tilde{Q}_d$. Thus up to $O(1)$

$$\begin{aligned}
m_{D,S}(Q) &= \frac{1}{d} m_{\varphi_*\pi_1^*(D),S}(\varphi(\bar{Q})) \text{ by Lemma 4.1.3} \\
&= \frac{1}{d} m_{\varphi_*\pi_1^*(D),S}(i \circ \sigma(Q)) \\
&= \frac{1}{d} m_{i^*\varphi_*\pi_1^*(D),S}(\sigma(Q)) \\
&= \frac{1}{d} m_{\sigma_*(D),S}(\sigma(Q)) \\
&\leq \frac{1}{d}(n_1 + n_2 + \varepsilon) h_{\sigma(Q)}(\sigma(Q)) \text{ by Theorem 3.1.8} \\
&= \frac{1}{d}(n_1 + n_2 + \varepsilon) h_{\sigma^*\sigma(Q)}(Q) \\
&= \frac{1}{d}(n_1 + n_2 + \varepsilon) \left[h_{\tilde{Q}_1}(Q) + \cdots + h_{\tilde{Q}_d}(Q) \right] \\
&\leq (n_1 + n_2 + \varepsilon)(1 + \varepsilon) h_R(Q) \\
&= (n_1 + n_2 + \varepsilon(n_1 + n_2 + 2)) h_R(Q).
\end{aligned}$$

And replacing ε with $\varepsilon/(2d + 2)$ gives the desired result. □

Lemma 4.1.7. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$. Suppose there exist only a finite number of k-morphisms $C \to \mathbb{P}^1$ of degree d (modulo automorphisms of $\mathbb{P}^1$). Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ such that $\sigma(Q) \in \mathbb{P}^1(k)$ for some k-morphism $\sigma : C \to \mathbb{P}^1$ of degree d, we have*

$$m_{D,S}(Q) \leq (N_d(D) + \varepsilon)h_R(Q) + O(1)$$

where $N_d(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree d.

Proof. Let $\{\sigma_j\}$ be the unique set of representatives of the equivalence classes of k-morphisms $C \to \mathbb{P}^1$ of degree d (modulo automorphisms of $\mathbb{P}^1$) such that

$$n_1(\sigma_j) = \left|\sigma_j^{-1}(0) \cap \mathrm{Supp}(D)\right| \text{ and } n_2(\sigma_j) = \left|\sigma_j^{-1}(\infty) \cap \mathrm{Supp}(D)\right|$$

for all j, where n_i is as defined in Theorem 4.1.6. By definition it is clear that $N = n_1(\sigma_j) + n_2(\sigma_j)$ for some j. Let $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ such that $\sigma(Q) \in \mathbb{P}^1(k)$ for some k-morphism $\sigma : C \to \mathbb{P}^1$ of degree d. After composing with an automorphism of $\mathbb{P}^1$ we may assume $\sigma = \sigma_j$ for some j. Thus by Theorem 4.1.6, for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ such that $\sigma(Q) \in \mathbb{P}^1(k)$ for some k-morphism $\sigma : C \to \mathbb{P}^1$ of degree d, we have

$$\begin{aligned} m_{D,S}(Q) &\leq \max_j \{(n_1(\sigma_j) + n_2(\sigma_j) + \varepsilon)h_R(Q) + O_j(1)\} \\ &\leq (N_d(D) + \varepsilon)h_R(Q) + O(1). \end{aligned}$$

□

Corollary 4.1.8. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$. If $g \geq 2$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$,*

$$m_{D,S}(Q) \leq (N_d(D) + \varepsilon)h_R(Q) + O(1)$$

where $N_d(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree 2.

Proof. For those $Q \in C(\overline{k})$ with $\mu(\varphi(\bar{Q})) \notin \mu(\varphi_*\pi_1^*(D))$ the result follows from Theorem 4.1.4, regardless of the value of $N_d(D)$. For those $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ and $\mu(\varphi(\bar{Q})) \in \mu(\varphi_*\pi_1^*(D))$, Lemma 4.1.5 implies there exists a morphism $\sigma : C \to \mathbb{P}^1$ of degree 2 such that $\sigma^*(\sigma(Q)) = \varphi(\bar{Q})$, that is $\sigma(Q) \in \mathbb{P}^1(k)$. Since $g \geq 2$, such a hyperelliptic map is unique up to an automorphism of $\mathbb{P}^1$, so the result follows from Lemma 4.1.7. □

Corollary 4.1.9. *Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $\varepsilon > 0$. If $g \geq 3$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$,*

$$m_{D,S}(Q) \leq (N_d(D) + \varepsilon)h_R(Q) + O(1)$$

where $N_d(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree 3.

Proof. For those $Q \in C(\overline{k})$ with $\mu(\varphi(\bar{Q})) \notin \mu(\varphi_*\pi_1^*(D))$ the result follows from Theorem 4.1.4, regardless of the value of $N_d(D)$. For those $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ and $\mu(\varphi(\bar{Q})) \in \mu(\varphi_*\pi_1^*(D))$, Lemma 4.1.5 implies there exists a morphism $\sigma : C \to \mathbb{P}^1$ of degree 3 such that $\sigma^*(\sigma(Q)) = \varphi(\bar{Q})$, that is $\sigma(Q) \in \mathbb{P}^1(k)$. If $g \geq 5$, by Theorem 3.3.2 such a trigonal morphism is unique up to an automorphism of $\mathbb{P}^1$. If $g = 4$, then by Theorem 3.3.5 there exist at most two such trigonal morphisms. If $g = 3$, then by Theorem 3.3.4 there are only finitely many trigonal k-morphisms. So the result follows from Lemma 4.1.7. □

4.2 Quadratic Points on Elliptic Curves

First, a general lemma.

Lemma 4.2.1. *Let C be a projective nonsingular curve of genus g defined over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $R \in C(k)$ and let $\varepsilon > 0$. Let d be a positive integer and let Z be a finite union of irreducible curves in* $\mathrm{Sym}^d(C)$.

(a) *If $g = 1$ and $d = 2$ and there does not exist a subset $\{i_1, \ldots, i_4\} \subset \{1, \ldots, n\}$ such that*

$$P_{i_1} + P_{i_2} \sim P_{i_3} + P_{i_4}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ and $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (3 + \varepsilon)h_R(Q) + O(1).$$

(b) *If $g = 1$ and $d = 3$ and there does not exist a subset $\{i_1, \ldots, i_6\} \subset \{1, \ldots, n\}$ such that*

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ such that $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (5 + \varepsilon)h_R(Q) + O(1).$$

(c) *If $g = 2$ and $d = 3$ and there does not exist a subset $\{i_1, \ldots, i_6\} \subset \{1, \ldots, n\}$ such that*

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ such that $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (5 + \varepsilon)h_R(Q) + O(1).$$

Furthermore if there does not exist a subset $\{i_1, \ldots, i_5\} \subset \{1, \ldots, n\}$ and a point $T \in C(k)$ distinct from $P_{i_1}, P_{i_2}, P_{i_3}$ such that

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ such that $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (4 + \varepsilon)h_R(Q) + O(1).$$

Proof. Let $Z = \sum_{j=1}^{r} Z_j$ be the decomposition of Z into irreducible curves. Since $\varphi(\bar{Q}) \notin \mathrm{Supp}(\varphi_* \pi_1^* D)$, we may assume $Z_j \setminus \mathrm{Supp}(\varphi_* \pi_1^* D)$ is nonempty, that is Z_j is not a subset of

$\mathrm{Supp}(\varphi_*\pi_1^*P_i)$ for $i = 1, \ldots, n$. We think of Z_j with the reduced induced closed subscheme structure and let $\rho_j : Z_j \to X$ be the closed immersion. If there are only finitely many points $Q \in C(\overline{k})$ such that $[k(Q) : k] = d$ and $\varphi(\bar{Q}) \in Z_j$, then we are done. Else Z_j has infinitely many k-rational points, thus by Falting's Theorem Z_j has genus 0 or 1. If Z_j has genus 1 then for those $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ and $\varphi(\bar{Q}) \in \rho_j(Z_j)$,

$$\begin{aligned}
m_{D,S}(Q) &= \frac{1}{d} m_{\varphi_*\pi_1^*D,S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\
&= \frac{1}{d} m_{\rho_j^*\varphi_*\pi_1^*D,S}(\rho_j^{-1}(\varphi(\bar{Q}))) + O(1) \\
&\leq \frac{\varepsilon}{d} h_{\rho_j^*\varphi_*\pi_1^*R}(\rho_j^{-1}(\varphi(\bar{Q}))) + O(1) \text{ by Lemma 3.1.1} \\
&= \frac{\varepsilon}{d} h_{\varphi_*\pi_1^*R}(\varphi(\bar{Q})) + O(1) \\
&= \varepsilon h_R(Q) + O(1) \text{ by Lemma 4.1.3.}
\end{aligned}$$

Alternatively if Z_j has genus 0 then, since abelian varieties admit no rational subvarieties, the image $\mu(Z_j) \in \mathrm{Jac}(C) = C$ is a point. Thus Z_j is contained in a fiber Y of μ. Let $E \in Y$. Then the subvariety $Y \subset \mathrm{Sym}^d(C)$ may be thought of as the complete linear system $|E|$ of the degree d divisor E on C. Furthermore the divisor $\varphi_*\pi_1^*P_i|_Y$ may be thought of as the linear system $|E - P_i| + P_i$, and thus as a linear subspace of the projective space Y.

If $d = g + 1$, where $g = 1$ or 2, then by Riemann-Roch the complete linear systems of divisors of degree d all have dimension 1, so $Y = \mathbb{P}^1$. Since $\varphi_*\pi_1^*P_i|_Y$ is a linear subspace, it is either a single point, or all of Y. Furthermore, because Z_j has dimension 1, it follows that $Z_j = Y$. So either $Z_j \subset \mathrm{Supp}(\varphi_*\pi_1^*P_i)$, a contradiction, or $\rho_j^*\varphi_*\pi_1^*P_i = \varphi_*\pi_1^*P_i|_Y$ is a degree 1 divisor.

If $g = 1$ and $d = 3$, then by Riemann-Roch, the complete linear systems of divisors of degree d all have dimension 2. Riemann-Roch also tells us that $|E - P_i|$ has dimension 1 and so $\varphi_*\pi_1^*P_i|_Y$ is a line in the projective plane Y. note the divisors $\varphi_*\pi_1^*P_i$ are in 3-subgeneral position, thus so are the lines $\varphi_*\pi_1^*P_i|_Y$. By Theorem 3.1.3, there exists a finite set $\mathcal{H}$ of lines in Y such that for all

$P \in Y \setminus \bigcup_{H \in \mathcal{H}} H$

$$\begin{aligned} m_{\varphi_*\pi_1^* D|_Y,S}(P) &= \sum_{i=1}^{n} m_{\varphi_*\pi_1^* P_i|_Y,S}(P) + O(1) \\ &\leq (5+\varepsilon)h(P) + O(1) \text{ by Theorem 3.1.3,} \end{aligned}$$

where h is the canonical height on $Y \cong \mathbb{P}^2$. Thus if $Z_j \notin \mathcal{H}$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ and $\varphi(\bar{Q}) \in \rho_j(Z_j)$

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{3} m_{\varphi_*\pi_1^* D,S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\ &= \frac{1}{3} m_{\rho_j^*\varphi_*\pi_1^* D,S}(\rho_j^{-1}(\varphi(\bar{Q}))) + O(1) \\ &\leq \frac{1}{3}(5+\varepsilon) h_{\rho_j^*\varphi_*\pi_1^* R}(\rho_j^{-1}(\varphi(\bar{Q}))) + O(1) \\ &= \frac{1}{3}(5+\varepsilon) h_{\varphi_*\pi_1^* R}(\varphi(\bar{Q})) + O(1) \\ &= (5+\varepsilon) h_R(Q) + O(1) \text{ by Lemma 4.1.3.} \end{aligned}$$

Since this would satisfy every inequality in part (b), we need not consider this case any further. If $Z_j \in \mathcal{H}$, then either $Z_j \subset \mathrm{Supp}(\varphi_*\pi_1^* P_i)$, a contradiction, or $\rho_j^*\varphi_*\pi_1^* P_i$ has degree 1.

At most d of the divisors $\rho_j^*\varphi_*\pi_1^*(P_i)$ can coincide, and if c divisors

$$\rho_j^*\varphi_*\pi_1^*(P_{i_1}), \ldots, \rho_j^*\varphi_*\pi_1^*(P_{i_c})$$

coincide, then

$$P_{i_1} + \ldots + P_{i_c} + R_{c+1} + \ldots + R_d \sim E$$

for some $R_{c+1}, \ldots, R_d \in C(\overline{k})$. Let $\rho_j^*\varphi_*\pi_1^*(D) = \sum_{m=1}^{p} c_m E_m$ for some positive integers $c_1, c_2, \cdots, c_p$ with $c_1 \geq c_2 \geq \cdots \geq c_p$. Then for $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ and $\varphi(\bar{Q}) \in Z_j$

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{d} m_{\varphi_*\pi_1^*(D),S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\ &= \frac{1}{d} m_{\varphi_*\pi_1^*(D)|_{Y_{jk}},S}(\varphi(\bar{Q})) + O(1) \\ &\leq \frac{1}{d}(c_1 + c_2 + \varepsilon) h_{\varphi_*\pi_{1*}(R)|_{Y_{jk}}}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 3.1.8} \\ &= \frac{1}{d}(c_1 + c_2 + \varepsilon) h_{\varphi_*\pi_{1*}(R)}(\varphi(\bar{Q})) + O(1) \\ &= (c_1 + c_2 + \varepsilon) h_R(Q) + O(1) \text{ by Lemma 4.1.3.} \end{aligned}$$

If there does not exist a subset $\{i_1, \ldots, i_{2d}\} \subset \{1, \ldots, n\}$ such that

$$P_{i_1} + \ldots + P_{i_d} \sim P_{i_{d+1}} + \ldots + P_{i_{2d}}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ such that $\varphi(\bar{Q}) \in Z_j$ we have

$$m_{D,S}(Q) \leq (2d - 1 + \varepsilon)h_R(Q) + O(1).$$

Finally, in the special case where $g = 2$ and $d = 3$, if there does not exist a subset $\{i_1, \ldots, i_5\} \subset \{1, \ldots, n\}$ and a point $T \in C(k)$ distinct from $P_{i_1}, P_{i_2}, P_{i_3}$ such that

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T$$

then either such a linear equivalence does not exist for any $T \in C(\overline{k})$, in which case, for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ such that $\varphi(\bar{Q}) \in Z$, we have

$$m_{D,S}(Q) \leq (4 + \varepsilon)h_R(Q) + O(1).$$

Else, there does exist a subset $\{i_1, \ldots, i_5\} \subset \{1, \ldots, n\}$ and a point $T \in C(\overline{k})$ such that

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T$$

with either $T \notin C(k)$ or $T \in \{P_{i_1}, P_{i_2}, P_{i_3}\}$. However since every other point in the linear equivalence is k-rational and thus fixed under Galois maps over k, it follows that T is also fixed, and so $T \in C(k)$ automatically. Thus $T \in \{P_{i_1}, P_{i_2}, P_{i_3}\}$, say $T = P_{i_3}$. But that would imply $\varphi_* \pi_1^* P_{i_3}$ intersects the projective line $Y = Z_j$ in more than one point, contradicting the fact that $\rho_j^* \varphi_* \pi_1^* P_i = \varphi_* \pi_1^* P_i|_Y$ has degree 1 as shown above.

Since there are only finitely many irreducible components Z_j in Z, we may take the maximum of the constants $O(1)$ in each of the above inequalities to prove the same inequalities holds for all $Q \in C(\overline{k})$ with $[k(Q) : k] = d$ such that $\varphi(\bar{Q}) \in Z$. □

Proposition 4.2.2. *Suppose $g = 1$. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$*

$$m_{D,S}(Q) \leq (4 + \varepsilon)h_R(Q) + O(1)$$

and if there does not exist a subset $\{i_1, \ldots, i_4\} \subset \{1, \ldots, n\}$ *such that*

$$P_{i_1} + P_{i_2} \sim P_{i_3} + P_{i_4}$$

then for all $Q \in C(\overline{k})$ *with* $[k(Q) : k] = 2$ *we have*

$$m_{D,S}(Q) \leq (3 + \varepsilon)h_R(Q) + O(1).$$

Proof. We may assume $n > 2$. Since $\pi_1^*(R) + \pi_2^*(R)$ is an ample divisor on C^2, we see that $\varphi_*(\pi_1^*(R) + \pi_2^*(R)) = 2\varphi_*\pi_1^*(R)$ is an ample divisor on $\mathrm{Sym}^2(C)$ and therefore so is $\varphi_*\pi_1^*(R)$. Since any two points on a curve are numerically equivalent, we also have $\varphi_*\pi_1^*(P_i)$ is numerically equivalent to $\varphi_*\pi_1^*(R)$ for all i. The divisors $\varphi_*\pi_1^*(P_i)$ are in general position since the intersection of $\varphi_*\pi_1^*(P_{i_1})$ and $\varphi_*\pi_1^*(P_{i_2})$ in $\mathrm{Sym}^2(C)$ is the point $P_{i_1} + P_{i_2}$.

For each $v \in S$, choose two of the divisors $\varphi_*\pi_1^*(P_i)$ to be $D_{1,v}$ and $D_{2,v}$. Then applying Theorem 3.1.6 with $X = \mathrm{Sym}^2(C)$, $A = \varphi_*\pi_1^*(R)$ and $d_i = 1$, for $1 \leq i \leq 2$, we see there exists a proper Zariski-closed subscheme $Z \subset \mathrm{Sym}^2(C)$ such that for all points $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ and $\varphi(\bar{Q}) \in \mathrm{Sym}^2(C)(k) \setminus Z$,

$$\sum_{v \in S} \sum_{i=1}^{2} \lambda_{D_{i,v},v}(\varphi(\bar{Q})) < (3 + \varepsilon)h_{\varphi_*\pi_1^*(P_1)}(\varphi(\bar{Q})).$$

Since at most two of the divisors $\varphi_*\pi_1^*(P_i)$ intersect at a point, we see that a point in $\mathrm{Sym}^2(C)(k) \setminus Z$ can be v-adically close to at most two of these divisors for each $v \in S$. Points v-adically closest to $D_{1,v}$ and $D_{2,v}$ cannot be (arbitrarily) v-adically close to any other of the divisors $\varphi_*\pi_1^*(P_i)$, that is those local heights $\lambda_{\varphi_*\pi_1^*(P_i)}$ are bounded for such points. Thus for all points $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ and $\varphi(\bar{Q}) \in \mathrm{Sym}^2(C)(k) \setminus Z$ with $\varphi(\bar{Q})$ v-adically closest to $D_{1,v}$ and $D_{2,v}$ for each

$v \in S$,

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{2} m_{\varphi_* \pi_1^*(D),S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\ &= \frac{1}{2} \sum_{v \in S} \sum_{i=1}^{n} \lambda_{\varphi_* \pi_1^*(P_i),v}(\varphi(\bar{Q})) + O(1) \\ &= \frac{1}{2} \sum_{v \in S} \sum_{i=1}^{2} \lambda_{D_{i,v},v}(\varphi(\bar{Q})) + O(1) \\ &< \frac{1}{2}(3+\varepsilon) h_{\varphi_* \pi_1^*(R)}(\varphi(\bar{Q})) + O(1) \\ &= (3+\varepsilon) h_R(Q) + O(1) \text{ by Lemma 4.1.3.} \end{aligned}$$

Since this inequality does not depend upon the choices of $D_{1,v}$ and $D_{2,v}$ for each place $v \in S$, the result follows for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ and $\varphi(\bar{Q}) \in \mathrm{Sym}^2(C)(k) \setminus Z$.

Since $\varphi(\bar{Q}) \in \mathrm{Sym}^2(C)(k)$ it only remains to consider the case where $\varphi(\bar{Q}) \in Z$. By Lemma 4.2.1, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ such that $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (4+\varepsilon) h_R(Q) + O(1)$$

and if there does not exist a subset $\{i_1, i_2, i_3, i_4\} \subset \{1, \ldots, n\}$ such that

$$P_{i_1} + P_{i_2} \sim P_{i_3} + P_{i_4}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$ such that $\varphi(\bar{Q}) \in Z$ we have

$$m_{D,S}(Q) \leq (3+\varepsilon) h_R(Q) + O(1).$$

Combining the above inequalities, we get that the proposition holds for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$. □

Corollary 4.2.3. *Let C be a nonsingular projective curve of genus-1 defined over a number field k and let $R \in C(k)$. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$,*

$$m_{D,S}(Q) \leq (N_2(D) + \varepsilon) h_R(Q) + O(1)$$

where $N_2(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ *taken over all* k*-morphisms* $\sigma : C \to \mathbb{P}^1$ *of degree* 2*. If no such* k*-morphism exists, we say* $N_2(D) = 0$*.*

Proof. First note that since degree 2 morphisms are at most 2-to-1, we have $N_2(D) \leq 4$. By Riemann-Roch, the dimension of the complete linear system $|E|$ of any divisor E on C of positive degree is given by $\dim|E| = \deg(E) - 1$. If there are only finitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$, then $m_{D,S}(Q) \leq O(1)$, so we assume there are infinitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 2$. In particular, there exists a pair of conjugate k-quadratic points $Q_1, Q_2 \in C(\overline{k})$. Since $|Q_1 + Q_2|$=1 and $|Q_1 + Q_2 - T| = 0$ for all $T \in C(\overline{k})$, it follows that $Q_1 + Q_2$ is a degree 2 divisor defined over k, whose complete linear system, $|Q_1 + Q_2|$, is base-point-free of dimension 1. Thus it induces a degree 2 morphism $\omega : C \to \mathbb{P}^1$ defined over k.

If $\deg(D) = 1$, then after composing with a k-automorphism of $\mathbb{P}^1$, we may assume $\omega(P_1) = 0$, so $N_2(D) = 1$. If $\deg(D) = 2$, then after composing with a k-automorphism of $\mathbb{P}^1$, we may assume $\omega(P_1) = 0$ and either $\omega(P_2) = 0$ or $\omega(P_2) = \infty$, so $N_2(D) = 2$. In both these cases $N = \deg(D)$, so we have

$$\begin{aligned} m_{D,S}(Q) &\leq h_D(Q) \text{ by Definition 2.2.8} \\ &\leq (\deg(D) + \varepsilon)h_R(Q) + O(1) \text{ by Theorem 2.2.12} \\ &= (N_d(D) + \varepsilon)h_R(Q) + O(1). \end{aligned}$$

Suppose $\deg(D) \geq 3$. Then since $|P_1 + P_2|$=1 and $|P_1 + P_2 - T| = 0$ for all $T \in C(\overline{k})$, it follows that $P_1 + P_2$ is a degree 2 divisor defined over k, whose complete linear system, $|P_1 + P_2|$, is base-point-free of dimension 1. Thus it induces a degree 2 morphism $\sigma : C \to \mathbb{P}^1$ defined over k, such that $\sigma(P_1) = \sigma(P_2)$. By composing with an automorphism of $\mathbb{P}^1$, we may assume $\sigma(P_1) = \sigma(P_2) = 0$ and $\sigma(P_3) = \infty$. Thus we see $N_2(D) \geq 3$.

If $N_2(D) = 4$, then the inequality follows from Proposition 4.2.2.

Conversely, if there exists a subset $\{i_1, i_2, i_3, i_4\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} \sim P_{i_3} + P_{i_4}$, then there exists a k-morphism $\sigma : C \to \mathbb{P}^1$ of degree 2 such that $\sigma(P_{i_1}) = \sigma(P_{i_2}) = 0$ and $\sigma(P_{i_3}) = \sigma(P_{i_4}) = \infty$, so that $N_2(D) = 4$.

Thus if $N_2(D) = 3$, then such a subset of $\{1, \ldots, n\}$ does not exist and the inequality again follows from Proposition 4.2.2. □

4.3 Cubic Points on Curves of Low Genus

It remains to show the main theorem holds for points of degree 3 on curves of genus 1 and 2.

Theorem 4.3.1. *Let X be an irreducible projective surface defined over a number field k. Let S be a finite set of places of k and let $n \in \mathbb{N}$. For each $v \in S$, let $D_{1,v}, \ldots, D_{n,v}$ be effective divisors on X, defined over k having no irreducible components in common in their supports. Suppose there exists an ample divisor A and positive integers $d_{i,v}$ such that $D_{i,v}$ is numerically equivalent to $d_{i,v}A$ for all i and for all $v \in S$. Suppose there exists a nonconstant k-morphism $\sigma : X \to E$ for some elliptic curve E defined over k. Let $\varepsilon > 0$. Then there exists a proper closed subscheme $Z \subset X$ such that for all points $P \in X(k) \setminus Z$,*

$$\sum_{v \in S} \sum_{i=1}^{n} \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq (3 + \varepsilon) h_A(P) + O(1).$$

Proof. Let $R \in E(k)$. By Theorem 3.1.1, for any $Q \in E(k)$ we have

$$m_{Q,S}(P) \leq \varepsilon h_R(P) + O(1)$$

for all $P \in E(k) \setminus \{Q\}$. Thus for any $Q \in E(k)$

$$\begin{aligned} m_{\sigma^* Q,S}(P) &= m_{Q,S}(\sigma(P)) + O(1) \\ &\leq \varepsilon h_R(\sigma(P)) + O(1) \\ &= \varepsilon h_{\sigma^* R}(P) + O(1) \end{aligned}$$

for all $P \in X(k) \setminus \sigma^*(Q)$. By Corollary 4.1.2, there exists an $M \in \mathbb{N}$, depending only on R and A, such that for all $P \in X(k)$

$$\varepsilon h_{\sigma^* R}(P) \leq \varepsilon M \cdot h_A(P) + O(1).$$

By replacing ε with ε / M we can say that for any $Q \in E(k)$

$$m_{\sigma^* Q,S}(P) \leq \varepsilon h_A(P) + O(1)$$

for all $P \in X(k) \setminus \sigma^*(Q)$. Therefore, by Lemma 2.3.2(a) and Theorem 2.3.4(d), for any $Q \in X(k)$ we have

$$\begin{aligned} m_{Q,S}(P) &\leq m_{\sigma^*(\sigma(Q)),S}(P) + O(1) \\ &\leq \varepsilon h_A(P) + O(1) \end{aligned}$$

for all $P \in X(k) \setminus \sigma^*(\sigma(Q))$.

For each $v \in S$, let

$$Y_v = \bigcup_{1 \leq i < j \leq n} \mathrm{Supp}(D_{i,v}) \cap \mathrm{Supp}(D_{j,v}).$$

Since no two of the divisors share irreducible components in common, it follows that Y_v is a finite set of points. Partition the set X by which of the points of Y_v each point is v-adically closest to. note that if a point is v-adically closest to two points of Y_v, then it cannot be v-adically close to any of the divisors $D_{i,v}$, that is all of the local heights $\lambda_{D_{i,v},v}$ will be bounded. Consider those points P that are v-adically closest to $Q \in Y_v$.

For each pair of indices i and j we have, by definition,

$$\lambda_{D_{i,v} \cap D_{j,v},v}(P) = \min\{\lambda_{D_{i,v},v}(P), \lambda_{D_{j,v},v}(P)\}$$

for all $P \in X(k) \setminus \mathrm{Supp}(D_{i,v}) \cap \mathrm{Supp}(D_{j,v})$. But if $Q \in \mathrm{Supp}(D_{i,v}) \cap \mathrm{Supp}(D_{j,v})$, we have

$$\lambda_{Q,v}(P) = \min\{\lambda_{D_{i,v},v}(P), \lambda_{D_{j,v},v}(P)\} + O(1)$$

for those points $P \in X(k) \setminus \{Q\}$ such that Q is the v-adically closest point to P out of all of the points in Y_v. Thus we have

$$\min\{\lambda_{D_{i,v},v}(P), \lambda_{D_{j,v},v}(P)\} \leq \varepsilon h_A(P) + O(1)$$

for all such $P \in X(k) \setminus \sigma^*(\sigma(Q))$. Since we can repeat this for each pair of indices i and j, it follows that at most one of the local heights $\lambda_{D_{i,v},v}(P)$, say $\lambda_{D_{i_Q,v},v}(P)$, can be greater than $\varepsilon \cdot h_A(P)$ for infinitely many of the points $P \in X(k) \setminus \sigma^*(\sigma(Q))$ that are v-adically closest to Q. As such

$$\sum_i \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq \frac{\lambda_{D_{i_Q,v},v}(P)}{d_{i,v}} + \varepsilon(n-1)h_A(P) + O(1)$$

for all $P \in X(k) \setminus \left(\bigcup_{i=1}^{n} \mathrm{Supp}(D_{i,v}) \cup \sigma^*(\sigma(Q))\right)$ that are v-adically closest to Q.

Repeating this process for each $v \in S$ gives a collection of partitions, which together make a finer partition of X into those $Q_v \in Y_v$ that the points are closest to for each $v \in S$ together with a proper (since σ is nonconstant) closed subscheme of X,

$$Z_1 = \bigcup_{v \in S} \bigcup_{Q \in Y_v} \sigma^*(\sigma(Q)).$$

Then we have

$$\sum_{i=0}^{n} \sum_{v \in S} \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq \sum_{v \in S} \frac{\lambda_{D_{i_{Q_v},v},v}(P)}{d_{i,v}} + \varepsilon(n-1)|S|h_A(P) + O(1)$$

for all $P \in X(k) \setminus \bigcup_{v \in S} \left(\bigcup_{i=1}^{n} \mathrm{Supp}(D_{i,v}) \cup \sigma^*(\sigma(Q_v))\right)$ that are v-adically closest to Q_v for each $v \in S$. But by Theorem 3.1.6, there exists a proper closed subscheme $Z_2 \subset X$ such that

$$\sum_{v \in S} \frac{\lambda_{D_{i_{Q_v},v},v}(P)}{d_{i,v}} \leq (3+\varepsilon)h_A(P)$$

for all $P \in X(k) \setminus Z_2$. Let $Z = \bigcup_{v \in S} \bigcup_{i=1}^{n} \mathrm{Supp}(D_{i,v}) \cup Z_1 \cup Z_2$. Then for all $P \in X(K) \setminus Z$

$$\sum_{i=0}^{n} \sum_{v \in S} \frac{\lambda_{D_{i,v},v}(P)}{d_{i,v}} \leq 3h_A(P) + \varepsilon\left(1 + (n-1)|S|\right) h_A(P) + O(1).$$

Thus by replacing ε with $\varepsilon/(1+(n-1)|S|)$, we obtain the desired result. □

Proposition 4.3.2. *Let C be an elliptic curve defined over k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $R \in C(k)$ and let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$*

$$m_{D,S}(Q) \leq (6+\varepsilon)h_R(Q) + O(1)$$

and if there does not exist a subset $\{i_1, \ldots, i_6\} \subset \{1, \ldots, n\}$ such that

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ we have

$$m_{D,S}(Q) \leq (5+\varepsilon)h_R(Q) + O(1).$$

Proof. By Theorem 3.1.6, there exists a proper closed subscheme $Z \subset \mathrm{Sym}^3(C)$ such that for all $Q \in C(k)$ such that $[k(Q) : k] = 3$ and $\varphi(\bar{Q}) \notin Z$ we have

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{3} m_{\varphi_* \pi_1^* D, S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\ &\leq \frac{1}{3}(4+\varepsilon) h_{\varphi_* \pi_1^* R}(Q) + O(1) \text{ by Theorem 3.1.6} \\ &= (4+\varepsilon) h_R(Q) + O(1) \text{ by Lemma 4.1.3.} \end{aligned}$$

Let Z_j be an irreducible component of Z. Then $\mu|_{Z_j}$ is a k-morphism from the irreducible surface Z_j to an elliptic curve $\mathrm{Jac}(C) = C$.

If $\mu|_{Z_j}$ is a constant map then Z_j is contained in a fiber of μ. But the fibers of μ are 2-dimensional by Riemann-Roch, so it follows that Z_j is a fiber of μ, so there exists an $E \in \mathrm{Div}(C)$ such that $Z_j = |E| \cong \mathbb{P}^2$. Since $\varphi_* \pi_1^* P_i$ is the set of effective divisors on C with P_i in their support, we see that it cuts out the 1-dimensional linear system $|E - P_i| + P_i$ in $|E|$. Furthermore the divisors $(\varphi_* \pi_1^* P_i)|_{Z_j}$ on Z_j are in 3-subgeneral position. Thus we may apply Theorem 3.1.3 with $r = 2$ and $L_i = (\varphi_* \pi_1^* P_i)|_{Z_j}$ to get

$$\begin{aligned} m_{D,S}(Q) &= \frac{1}{3} m_{\varphi_* \pi_1^* D, S}(\varphi(\bar{Q})) + O(1) \text{ by Lemma 4.1.3} \\ &= \frac{1}{3} \sum_{i=1}^{n} m_{L_i, S}(\varphi(\bar{Q})) + O(1) \\ &\leq \frac{1}{3}(5+\varepsilon) h_{\varphi_* \pi_1^* R}(Q) + O(1) \text{ by Theorem 3.1.3} \\ &= (5+\varepsilon) h_R(Q) + O(1) \text{ by Lemma 4.1.3.} \end{aligned}$$

for all $Q \in C(k)$ such that $[k(Q) : k] = 3$ and $\varphi(\bar{Q}) \in Z_j \setminus Y_j$, where Y_j is a union of hyperplanes $Y_{jk} \subset Z_j \cong \mathbb{P}^2$. By Lemma 4.2.1, if there does not exist a subset $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ and $\varphi(\bar{Q}) \in Y_j$

$$m_{D,S}(Q) \leq (5+\varepsilon) h_R(Q) + O(1)$$

otherwise

$$m_{D,S}(Q) \leq (6+\varepsilon) h_R(Q) + O(1).$$

Combining the above inequalities we get the result on all of Z_j. Since there are only finitely many irreducible components Z_j in Z, we may take the maximum of all of the above constants in $O(1)$ to get the result for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$. □

Lemma 4.3.3. *Let C be a nonsingular projective curve of genus 1 over an algebraic number field k. Let $d \geq 3$ be an integer and let $P_1, \ldots, P_{2d-1} \in C(k)$ be distinct. Let P_{2d-1} be the identity element of the elliptic curve C. Suppose that for every morphism $\sigma : C \to \mathbb{P}^1$ over k of degree d we have*

$$\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \{P_1, \ldots, P_{2d-1}\}\right| \leq 2d - 2.$$

Then for every $i \in \{1, \ldots, 2d-2\}$, the inverse of P_i in the elliptic curve C is P_j for some $j \in \{1, \ldots, 2d-2\} \setminus \{i\}$.

Proof. We proceed by induction on the number of pairs of inverse points identified. Trivially, we have already identified zero such pairs. Suppose we have identified m pairs already and that $m < d - 1$. Let $M \subset \{1, \ldots, 2d-2\}$ be a set of representative indices, each pair of inverse points being represented by exactly one index, so that $|M| = m$. For each $i \in M$, define i^* to be the index of the inverse of P_i, that is to say $P_i + P_{i^*} \sim 2P_{2d-1}$. Let $I \subset \{1, \ldots, 2d-2\}$ be a subset disjoint from M with $|I| = d - 2 - m$ and let $J = \{1, \ldots, 2d-2\} \setminus (M \cup I)$. By Riemann-Roch, there exists a unique $R \in C(\overline{k})$ such that

$$R + P_{2d-1} + \sum_{i \in M \cup I} P_i \sim \sum_{j \in J} P_j.$$

Furthermore $R \in C(k)$ by uniqueness. If $R \notin \{P_j \mid j \in J\}$, then this linear equivalence defines a base-point-free 1-dimensional linear system over k of degree d. Thus there exists a corresponding morphism $\sigma : C \to \mathbb{P}^1$ over k with $\sigma^{-1}(0) = \{R, P_{2d-1}\} \cup \{P_i \mid i \in M \cup I\}$ and $\sigma^{-1}(\infty) = \{P_j \mid j \in J\}$, so that

$$\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \{P_1, \ldots, P_{2d-1}\}\right| = 2d - 1.$$

As this would contradict the hypothesis, we conclude there exists an $r \in J$ such that $R = P_r$. That is to say

$$P_{2d-1} + \sum_{i \in M \cup I} P_i \sim \sum_{j \in J \setminus \{r\}} P_j. \tag{4.1}$$

Once again by Riemann-Roch, there exists a $T \in C(\overline{k})$ such that

$$P_{2d-1} + \sum_{j \in J \setminus \{r\}} P_j \sim T + P_r + \sum_{i \in M \cup I} P_i.$$

By the same reasoning as above, either $T = P_{2d-1}$ or $T \in \{P_j \mid j \in J \setminus \{r\}\}$. But if $T = P_{2d-1}$, then

$$\sum_{j \in J \setminus \{r\}} P_j \sim P_r + \sum_{i \in M \cup I} P_i.$$

Comparing this to equivalence (4.1) reveals that $P_r \sim P_{2d-1}$. But according to Riemann-Roch, if two points on C are linearly equivalent, then they are equal, that is $P_r = P_{2d-1}$, a contradiction since $r \neq 2d - 1$ and the P_i are distinct. Therefore there exists a $t \in J \setminus \{r\}$ such that $T = P_t$. That is to say

$$P_{2d-1} + \sum_{j \in J \setminus \{r,t\}} P_j \sim P_r + \sum_{i \in M \cup I} P_i. \tag{4.2}$$

Adding equivalences (4.1) and (4.2) together we get

$$2P_{2d-1} + \sum_{i \in \{1,\ldots,2d-2\} \setminus \{r,t\}} P_i \sim \sum_{i \in \{1,\ldots,2d-2\}} P_i.$$

And after cancelling, we get $P_r + P_t \sim 2P_{2d-1}$, which is exactly the condition that P_r and P_t are inverse points in the elliptic curve C with identity P_{2d-1}. Thus we have determined $m + 1$ distinct pairs of inverse points on C. Therefore, by induction we conclude that we can find $d - 1$ distinct pairs of inverse points, which must consist of $P_1, \ldots, P_{2d-2}$ as desired.

□

Proposition 4.3.4. *Let C be a nonsingular projective curve of genus 1 over an algebraic number field k. Let $P_1, \ldots, P_5 \in C(k)$ be distinct. Suppose that for every morphism $\sigma : C \to \mathbb{P}^1$ over k of degree* 3 *we have*

$$\left| \left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty) \right) \cap \{P_1, \ldots, P_5\} \right| \leq 4.$$

Then if one of the five given points is chosen to be the identity element of the elliptic curve C, the five given points then form a subgroup of $C(k)$ of order 5.

Proof. Without loss of generality, let P_5 be the identity element of the elliptic curve C. By Lemma 4.3.3, for every $k \in \{1, \ldots, 4\}$ there exists a $k^* \in \{1, \ldots, 4\} \setminus \{k\}$ such that $P_k + P_{k^*} \sim 2P_5$. Let these four non-identity points be called $P_i, P_{i^*}, P_j, P_{j^*}$.

By Riemann-Roch, there exists an $R \in C(\overline{k})$ such that

$$R + P_5 + P_{i^*} \sim P_i + P_j + P_{j^*}. \tag{4.3}$$

Since we assume the above morphism σ does not exist, it must be the case that either $R = P_i$, $R = P_j$, or $R = P_{j^*}$. But if $R = P_i$, then equivalence (4.3) simplifies to

$$P_{1^*} + P_5 + P_{i^*} \sim P_i + 2P_5.$$

So $P_{i^*} \sim P_5$. By Riemann-Roch, this implies $P_{i^*} = P_5$, a contradiction.

Therefore $R = P_r$ with $r \in \{j, j^*\}$. In this case, equivalence (4.3) simplifies to

$$P_r + P_5 + P_{i^*} \sim P_i + 2P_5.$$

Adding P_i to both sides and cancelling like terms gives $P_r + P_5 \sim 2P_i$. As elements of the elliptic curve C, this says $2P_i = P_r$. Taking inverses, we also get $2P_{i^*} = P_{r^*}$. Repeating this process for the linear equivalence

$$T + P_5 + P_{j^*} \sim P_j + P_i + P_{i^*}$$

gives $T = P_t$ for some $t \in \{i, i^*\}$ and so $P_t + P_5 \sim 2P_j$. As elements of the elliptic curve C, this says $2P_j = P_t$ and $2P_{j^*} = P_{t^*}$. Since $2P_5 = P_5$, we see that these five points are closed under doubling.

Once again by Riemann-Roch, there exists a point $A \in C(\overline{k})$ such that

$$A + P_i + P_j \sim P_{i^*} + P_{j^*} + P_5.$$

Since we assume the above morphism σ does not exist, it must be the case that either $A = P_{i^*}$, $A = P_{j^*}$, or $A = P_5$. If $A = P_5$ however, then $P_i + P_j = P_{i^*} + P_{j^*}$ and adding $P_i + P_j$ to both sides

gives $P_r + P_t = 0$, which is not possible, given $r \in \{j, j^*\}$ and $t \in \{i, i^*\}$. Thus $A \in \{P_{i^*}, P_{j^*}\}$ and $P_i + P_j = P_u$ for some $u \in \{i^*, j^*\}$. Taking inverses gives $P_{i^*} + P_{j^*} = P_{u^*}$. Similarly, $P_i + P_{j^*} = P_v$ for some $v \in \{i^*, j\}$ and so $P_{i^*} + P_j = P_{v^*}$. Thus the set $\{P_1, \ldots, P_5\}$ is closed under addition, and therefore forms a subgroup of order 5 in the elliptic curve C. □

It is worth noting that this obstruction does not appear in higher degree examples, as demonstrated in the following.

Proposition 4.3.5. *Let C be a nonsingular projective curve of genus 1 over an algebraic number field k. Let $d \geq 4$ be an integer and let $P_1, \ldots, P_{2d-1} \in C(k)$ be distinct. Then there exists a morphism $\sigma : C \to \mathbb{P}^1$ over k of degree d such that*

$$\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \{P_1, \ldots, P_{2d-1}\}\right| = 2d - 1.$$

Proof. By way of contradiction, assume such a morphism does not exist. Let P_{2d-1} be the identity element of the elliptic curve C. Then by Lemma 4.3.3, for every $i \in \{1, \ldots, 2d-2\}$ there exists an $i^* \in \{1, \ldots, 2d-2\} \setminus \{i\}$ such that $P_i + P_{i^*} \sim 2P_{2d-1}$. Let M be a set of representative indices of these pairs, that is for each $i \in \{1, \ldots, 2d-2\}$, either $i \in M$ or $i^* \in M$ and not both, so that $|M| = d - 1$. Let $M_1 = M \setminus \{1, 1^*\}$ and note $|M_1| = d - 2$.

The proof is broken into two cases, but those cases are treated very similarly. First suppose d is even. Let $K \subset M_1$ with $|K| = \frac{d-2}{2}$. By Riemann-Roch, there exists an $R \in C(\overline{k})$ such that

$$R + P_1 + \sum_{i \in M_1 \setminus K} (P_i + P_{i^*}) \sim P_{2d-1} + P_{1^*} + \sum_{i \in K} (P_i + P_{i^*}). \tag{4.4}$$

Since we assume the desired morphism does not exist, it must be the case that either $R = P_{2d-1}$, $R = P_{1^*}$, or $R \in \{P_i \mid i \in K \text{ or } i^* \in K\}$. But if $R = P_{2d-1}$, then equivalence (4.4) simplifies to

$$P_{2d-1} + P_1 + (d-2)P_{2d-1} \sim P_{2d-1} + P_{1^*} + (d-2)P_{2d-1}.$$

So $P_1 \sim P_{1^*}$. By Riemann-Roch, this implies $P_1 = P_{1^*}$, a contradiction to Lemma 4.3.3. And if $R = P_{1^*}$, then equivalence (4.4) simplifies to

$$P_{1^*} + P_1 + (d-2)P_{2d-1} \sim P_{2d-1} + P_{1^*} + (d-2)P_{2d-1}.$$

So $P_1 \sim P_{2d-1}$. By Riemann-Roch, this implies $P_1 = P_{2d-1}$, a contradiction to the hypothesis.

Therefore $R = P_r$ for some $r \in \{1, \ldots, 2d-2\}$ with either $r \in K$ or $r^* \in K$. In this case equivalence (4.4) simplifies to

$$P_r + P_1 + (d-2)P_{2d-1} \sim P_{2d-1} + P_{1^*} + (d-2)P_{2d-1}.$$

Adding P_{1^*} to both sides and cancelling like terms gives

$$P_r + P_{2d-1} \sim 2P_{1^*}. \tag{4.5}$$

Now choose $K' \subset M_1 \setminus \{r, r^*\}$ with $|K'| = \frac{d-2}{2}$. note this subset exists because $|M_1 \setminus \{r, r^*\}| = d-3$ and $\frac{d-2}{2} \leq d-3 \iff d \geq 4$. By Riemann-Roch, there exists an $T \in C(\overline{k})$ such that

$$T + P_1 + \sum_{i \in M_1 \setminus K'} (P_i + P_{i^*}) \sim P_{2d-1} + P_{1^*} + \sum_{i \in K'} (P_i + P_{i^*}). \tag{4.6}$$

Once again this implies that $T = P_t$ for some $t \in \{1, \ldots, 2d-2\}$ with either $t \in K'$ or $t^* \in K'$. Therefore equivalence (4.6) simplifies to

$$P_t + P_1 + (d-2)P_{2d-1} \sim P_{2d-1} + P_{1^*} + (d-2)P_{2d-1}.$$

Adding P_{1^*} to both sides and cancelling like terms gives

$$P_t + P_{2d-1} \sim 2P_{1^*}. \tag{4.7}$$

Comparing equivalences (4.5) and (4.7) reveals that $P_r \sim P_t$, which implies that $P_r = P_t$, but that implies $r = t$, a contradiction to the construction of K'. Therefore our initial assumption must have been false and there exists a morphism $\sigma : C \to \mathbb{P}^1$ over k of degree d such that

$$\left| \left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty) \right) \cap \{P_1, \ldots, P_{2d-1}\} \right| = 2d-1.$$

Now suppose d is odd. Let $K \subset M_1$ with $|K| = \frac{d-1}{2}$. By Riemann-Roch, there exists an $R \in C(\overline{k})$ such that

$$R + P_{2d-1} + P_1 + \sum_{i \in M_1 \setminus K} (P_i + P_{i^*}) \sim P_{1^*} + \sum_{i \in K} (P_i + P_{i^*}). \tag{4.8}$$

Since we assume the desired morphism does not exist, it must be the case that either $R = P_{1^*}$ or $R \in \{P_i \mid i \in K \text{ or } i^* \in K\}$. But if $R = P_{1^*}$, then equivalence (4.8) simplifies to

$$P_{1^*} + P_{2d-1} + P_1 + (d-3)P_{2d-1} \sim P_{1^*} + (d-1)P_{2d-1}.$$

So $P_1 \sim P_{2d-1}$. By Riemann-Roch, this implies $P_1 = P_{2d-1}$, a contradiction.

Therefore $R = P_r$ for some $r \in \{1, \ldots, 2d-2\}$ with either $r \in K$ or $r^* \in K$. In this case equivalence (4.8) simplifies to

$$P_r + P_{2d-1} + P_1 + (d-3)P_{2d-1} \sim P_{1^*} + (d-1)P_{2d-1}.$$

Adding P_{1^*} to both sides and cancelling like terms gives

$$P_r + P_{2d-1} \sim 2P_{1^*}. \tag{4.9}$$

Now choose $K' \subset M_1 \setminus \{r, r^*\}$ with $|K'| = \frac{d-1}{2}$. note this subset exists because $|M_1 \setminus \{r, r^*\}| = d-3$ and $\frac{d-1}{2} \leq d-3 \iff d \geq 5$. By Riemann-Roch, there exists an $T \in C(\overline{k})$ such that

$$T + P_{2d-1} + P_1 + \sum_{i \in M_1 \setminus K'} (P_i + P_{i^*}) \sim P_{1^*} + \sum_{i \in K'} (P_i + P_{i^*}). \tag{4.10}$$

Once again this implies that $T = P_t$ for some $t \in \{1, \ldots, 2d-2\}$ with either $t \in K'$ or $t^* \in K'$. Therefore equivalence (4.10) simplifies to

$$P_t + P_{2d-1} + P_1 + (d-3)P_{2d-1} \sim P_{1^*} + (d-1)P_{2d-1}.$$

Adding P_{1^*} to both sides and cancelling like terms gives

$$P_t + P_{2d-1} \sim 2P_{1^*}. \tag{4.11}$$

Comparing equivalences (4.9) and (4.11) reveals that $P_r \sim P_t$, which implies that $P_r = P_t$, but that implies $r = t$, a contradiction to the construction of K'. Therefore our initial assumption must have been false and there exists a morphism $\sigma : C \to \mathbb{P}^1$ over k of degree d such that

$$\left| \left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty) \right) \cap \{P_1, \ldots, P_{2d-1}\} \right| = 2d-1.$$

□

Now we prove the desired inequality holds for cubic points on elliptic curves, excluding the special case when the support of the divisor consists of exactly five points forming a subgroup of the elliptic curve.

Corollary 4.3.6. *Let C be a nonsingular projective curve of genus 1 defined over a number field k and let $R \in C(k)$. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct, such that the set $\{P_1, \ldots, P_n\}$ is not a subgroup of order five of the elliptic curve $(C(k), P_n)$ (which is automatically true if $n \neq 5$). Define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$,*

$$m_{D,S}(Q) \leq (N_3(D) + \varepsilon)h_R(Q) + O(1)$$

where $N_3(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree 3. If no such k-morphism exists, we say $N_3(D) = 0$.

Proof. First note that since degree 3 morphisms are at most 3-to-1, we have $N_3(D) \leq 6$. We also clearly have $N_3(D) \leq \deg(D)$. By Riemann-Roch, the dimension of the complete linear system $|E|$ of any divisor E on C of positive degree is given by $\dim|E| = \deg(E) - 1$. If there are only finitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$, then $m_{D,S}(Q) \leq O(1)$, so we assume there are infinitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$. In particular, there exists a triple of conjugate k-cubic points $Q_1, Q_2, Q_3 \in C(\overline{k})$. Since $|Q_1 + Q_2 + Q_3| = 2$ and $|Q_1 + Q_2 + Q_3 - T - U| = 0$ for all $T, U \in C(\overline{k})$, it follows that $Q_1 + Q_2 + Q_3$ is a degree 3, very ample divisor defined over k, whose complete linear system $|Q_1 + Q_2 + Q_3|$ has dimension 2. Thus it induces an embedding $F : C \to \mathbb{P}^2$ defined over k, whose image is a curve over k of degree 3 such that the points $F(Q_1), F(Q_2), F(Q_3)$ lie on a line H over k. Projecting from any k-rational point A not on the curve $F(C)$ in $\mathbb{P}^2$ produces a degree 3 morphism $f_A : C \to \mathbb{P}^1$ over k.

If $\deg(D) = 1$, then choose any line L over k in $\mathbb{P}^2$ containing $F(P_1)$. As the intersection of two lines over k, the point $A := L \cap H$ is k-rational, thus different from $F(Q_1), F(Q_2), F(Q_3)$, thus not a point on $F(C)$. So f_A is a degree 3 morphism over k and after composing with a k-automorphism of $\mathbb{P}^1$, we may assume $f_A(P_1) = 0$, so that $N_3(D) = 1$.

If $\deg(D) = 2$, then let L be the line in $\mathbb{P}^2$ containing $F(P_1)$ and $F(P_2)$, thus a line over k. As the intersection of two lines over k, the point $B := L \cap H$ is k-rational, thus different from $F(Q_1), F(Q_2), F(Q_3)$, thus not a point on $F(C)$. So f_B is a morphism of degree 3 over k and after composing with a k-automorphism of $\mathbb{P}^1$, we may assume $f_B(P_1) = f_B(P_2) = 0$, so that $N_3(D) = 2$.

If $\deg(D) = 3$, then after composing with a k-automorphism of $\mathbb{P}^1$, we may assume $f_B(P_1) = f_B(P_2) = 0$ and $f_B(P_3) = \infty$, so that $N_3(D) = 3$.

If $\deg(D) = 4$, then let H_2 be the line in $\mathbb{P}^2$ containing $F(P_1), F(P_2), F(P_3)$, and let $g_A : C \to \mathbb{P}^1$ be the morphism of degree 3 over k induced by the projection from a point $A \in H_2(k)$. Then $g_A(P_1) = g_A(P_2) = g_A(P_3)$, so composing with a k-automorphism of $\mathbb{P}^1$, we may assume $g_A(P_1) = g_A(P_2) = g_A(P_3) = 0$ and $g_A(P_4) = \infty$, so that $N_3(D) = 4$.

If $\deg(D) = 5$, then by the hypothesis and by Proposition 4.3.4, we have $N_3(D) = 5$.

In these cases $N_3(D) = \deg(D)$, so we have

$$\begin{aligned} m_{D,S}(Q) &\leq h_D(Q) \text{ by Definition 2.2.8} \\ &\leq (\deg(D) + \varepsilon)h_R(Q) + O(1) \text{ by Theorem 2.2.12} \\ &= (N_3(D) + \varepsilon)h_R(Q) + O(1). \end{aligned}$$

Now suppose $\deg(D) \geq 6$. If we assume that $N_3(D) \leq 4$, then by Proposition 4.3.4, we know that the points $\{P_1, \ldots, P_5\}$ form a subgroup of order 5 of the elliptic curve C with identity element P_5. In particular there exist $i, j \in \{2, 3, 4\}$ such that $P_i + P_j = P_1$. Replacing P_1 with P_6 and applying Proposition 4.3.4 again to show that the points $\{P_2, \ldots, P_6\}$ form a subgroup of order 5 in the elliptic curve C with identity element P_5. But these points obey the same group law as before, and $P_i + P_j = P_1$, meaning the set is not closed under addition, a contradiction. Therefore we conclude that $N_3(D) \geq 5$.

If $N_3(D) = 6$, then the inequality follows from Proposition 4.3.2.

Conversely, if there exists a subset $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$, then there exists a k-morphism $\sigma : C \to \mathbb{P}^1$ of degree 3 such that $\sigma(P_{i_1}) = \sigma(P_{i_2}) = \sigma(P_{i_3})$ and $\sigma(P_{i_4}) = \sigma(P_{i_5}) = \sigma(P_{i_6})$. After composing with a k-automorphism of

$\mathbb{P}^1$, we may assume $\sigma(P_{i_1}) = \sigma(P_{i_2}) = \sigma(P_{i_3}) = 0$ and $\sigma(P_{i_4}) = \sigma(P_{i_5}) = \sigma(P_{i_6}) = \infty$, so that $N_3(D) = 6$.

Thus if $N_3(D) = 5$, then such a subset of $\{1, \ldots, n\}$ does not exist and the inequality again follows from Proposition 4.3.2. □

Proposition 4.3.7. *Let C be a nonsingular projective curve of genus 2 defined over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^n P_i$. Let $R \in C(k)$ and let $\varepsilon > 0$.*

If there exists a subset $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$

$$m_{D,S}(Q) \leq (6 + \varepsilon)h_R(Q) + O(1).$$

If such a linear equivalence does not exist, but there exists a subset $\{i_1, i_2, i_3, i_4, i_5\} \subset \{1, \ldots, n\}$ and a point $T \in C(k)$ distinct from the points $P_{i_1}, P_{i_2}, P_{i_3}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$

$$m_{D,S}(Q) \leq (5 + \varepsilon)h_R(Q) + O(1).$$

And if neither of these hold, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$

$$m_{D,S}(Q) \leq (4 + \varepsilon)h_R(Q) + O(1)$$

Proof. By Theorem 3.1.6, there exists a proper closed subscheme $Z \subset \mathrm{Sym}^3(C)$ such that for all $P \in \mathrm{Sym}^3(C)(k) \setminus Z$,

$$m_{D,S}(P) \leq (4 + \varepsilon)h_{\varphi_* \pi_1^* R}(P).$$

Let Z_j be an irreducible component of Z. Then $\mu|_{Z_j}$ is a k-morphism from the irreducible surface Z_j to the abelian variety $\mathrm{Jac}(C)$.

If $\mu|_{Z_j}$ were a constant map then Z_j would be contained in a fiber of μ. But the fibers of μ are 1-dimensional by Riemann-Roch, a contradiction, so $\mu|_{Z_j}$ is nonconstant.

If the image of $\mu|_{Z_j}$ is a curve, then Theorem 4.3.1 says there exists a proper closed subscheme Y_j of Z_j such that for all $P \in Z_j(k) \setminus Y_j$

$$m_{D|_{Z_i},S}(P) \leq (3+\varepsilon)h_{(\varphi_*\pi_1^*R)|_{Z_i}}(P) + O(1).$$

Since Y_j is a proper closed subscheme we may assume it is 1-dimensional, and is thus a union of curves. By Lemma 4.2.1, if there does not exist a subset $\{i_1, i_2, i_3, i_4, i_5\} \subset \{1, \ldots, n\}$ and a point $T \in C(k)$ distinct from the points $P_{i_1}, P_{i_2}, P_{i_3}$ such that

$$P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T,$$

then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ and $\varphi(\bar{Q}) \in Y_j$

$$m_{D,S}(Q) \leq (4+\varepsilon)h_R(Q) + O(1).$$

And if there does not exist a subset $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$, then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$ and $\varphi(\bar{Q}) \in Y_j$

$$m_{D,S}(Q) \leq (5+\varepsilon)h_R(Q) + O(1),$$

else

$$m_{D,S}(Q) \leq (6+\varepsilon)h_R(Q) + O(1).$$

Finally, if the image of $\mu|_{Z_j}$ is all of $\mathrm{Jac}(C)$, then $Y_j = \mathrm{Supp}\left(\mu^*\mu_*\varphi_*\pi_1^*D|_{Z_j}\right)$ is a finite union of irreducible curves Y_{jk} on Z_j. By Theorem 4.1.4, it is enough to show the inequality holds on these curves, which of course follows once again from Lemma 4.2.1.

Combining the above inequalities we get the result on all of Z_j. Since there are only finitely many irreducible components Z_j in Z, we make take the maximum of all of the above constants $O(1)$ to get the result for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$.

□

Lemma 4.3.8. *Let C be a nonsingular projective curve of genus 2. Let D be an effective divisor on C of degree 3. Then the complete linear system $|D|$ has a base point if and only if $K \leq D$ for a canonical divisor K on C.*

Proof. By Riemann-Roch, $\dim|D| = 1$. Suppose D has a base point $P \in C(\overline{k})$. Then there exists an effective divisor E of degree 2 such that $D = E + P$. Furthermore $\dim|E| = \dim|D - P| = \dim|D| = 1$. By Riemann-Roch, $\dim|K - E| = 0$, and since $\deg(K - E) = 0$, this implies $E \sim K$. That is to say, E is a canonical divisor with $E \leq D$, as was to be shown.

Conversely, suppose $K \leq D$ for a canonical divisor K. Then $D = K + P$ for some $P \in C(\overline{k})$. Thus $\dim|D - P| = \dim|K| = 1 = \dim|D|$, so P is a base point of D. □

Corollary 4.3.9. *Let C be a nonsingular projective curve of genus 2 defined over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Suppose that either $n \leq 2$ or else that there exist $i_1, i_2, i_3 \in \{1, \ldots, n\}$ such that the set $\{P_{i_1}, P_{i_2}, P_{i_3}\}$ does not contain a pair of hyperelliptic conjugates (which is automatically true when $n \geq 5$). Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$,*

$$m_{D,S}(Q) \leq (N_3(D) + \varepsilon)h_R(Q) + O(1)$$

where $N_3(D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all finite k-morphisms $\sigma : C \to \mathbb{P}^1$ of degree 3. If no such k-morphism exists, we say $N_3(D) = 0$.

Proof. First note that since degree 3 morphisms are at most 3-to-1, we have $N_3(D) \leq 6$. We also clearly have $N_3(D) \leq \deg(D)$. If there are only finitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$, then $m_{D,S}(Q) \leq O(1)$, so we assume there are infinitely many points $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$. In particular, there exists a triple of conjugate k-cubic points $Q_1, Q_2, Q_3 \in C(\overline{k})$. By Riemann-Roch, $\dim|Q_1 + Q_2 + Q_3| = 1$.

If the linear system $|Q_1 + Q_2 + Q_3|$ has a base point, then by Lemma 4.3.8, $K \leq Q_1 + Q_2 + Q_3$ for a canonical divisor K on C. Without loss of generality, say $K = Q_1 + Q_2$. By uniqueness, $|K|$ is fixed under Galois action. Thus if ξ is any Galois action that takes Q_2 to Q_3, then $\xi(Q_1) = Q_i$ for some $i \in \{1, 2\}$, so $Q_1 + Q_2 \sim \xi(Q_1 + Q_2) = Q_i + Q_3$ and subtracting Q_i from both sides leaves $Q_j \sim Q_3$ for some $j \in \{1, 2\}$, implying $Q_j = Q_3$, a contradiction. Therefore $|Q_1 + Q_2 + Q_3|$ is a 1-dimensional base point free linear system of degree 3 defined over k. It follows that the

corresponding k-morphism $\omega : C \to \mathbb{P}^1$ has degree 3 with $\omega(Q_1) = \omega(Q_2) = \omega(Q_3)$. Therefore if $\deg(D) = 1$ or 2, then $N_3(D) = \deg(D)$.

Alternatively, if there exist $i_1, i_2, i_3 \in \{1, \ldots, n\}$ such that $\{P_{i_1}, P_{i_2}, P_{i_3}\}$ does not contain a pair of hyperelliptic conjugates, then the complete linear system $|P_{i_1} + P_{i_2} + P_{i_3}|$ is base point free by Lemma 4.3.8. So there exists a k-morphism $\gamma : C \to \mathbb{P}^1$ of degree 3 with $\gamma(P_{i_1}) = \gamma(P_{i_2}) = \gamma(P_{i_3}) = 0$. If $deg(D) = 3$, then this shows $N_3(D) = 3$.

In these cases, where $N_3(D) = \deg(D)$, we have

$$\begin{aligned} m_{D,S}(Q) &\leq h_D(Q) \text{ by Definition 2.2.8} \\ &\leq (\deg(D) + \varepsilon)h_R(Q) + O(1) \text{ by Theorem 2.2.12} \\ &= (N_3(D) + \varepsilon)h_R(Q) + O(1). \end{aligned}$$

From here on, suppose $deg(D) \geq 4$. Then there exists a fourth point in the support of D and the morphism γ must map it somewhere. After a k-automorphism of $\mathbb{P}^1$, we may assume it is sent to infinity, and so $N_3(D) \geq 4$.

If $N_3(D) = 6$, then the inequality follows from Proposition 4.3.7.

Conversely, if there exists a subset $\{i_1, i_2, i_3, i_4, i_5, i_6\} \subset \{1, \ldots, n\}$ such that $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + P_{i_6}$, then there exists a k-morphism $\sigma : C \to \mathbb{P}^1$ of degree 3 such that $\sigma(P_{i_1}) = \sigma(P_{i_2}) = \sigma(P_{i_3}) = 0$ and $\sigma(P_{i_4}) = \sigma(P_{i_5}) = \sigma(P_{i_6}) = \infty$, so that $N_3(D) = 6$.

Thus if $N_3(D) = 5$, then such a subset of $\{1, \ldots, n\}$ does not exist and the inequality again follows from Proposition 4.3.7.

If $N_3(D) \geq 5$ then there exists a subset $\{i_1, i_2, i_3, i_4, i_5\} \subset \{1, \ldots, n\}$ and a k-morphism $\delta : C \to \mathbb{P}^1$ of degree 3 such that $\delta(P_{i_1}) = \delta(P_{i_2}) = \delta(P_{i_3}) = 0$ and $\delta(P_{i_4}) = \delta(P_{i_5}) = \infty$. Since $0 \sim \infty$ in $\mathbb{P}^1$, it follows that $\delta^*0 \sim \delta^*\infty$. That is $P_{i_1} + P_{i_2} + P_{i_3} \sim P_{i_4} + P_{i_5} + T$ for some $T \in C(\overline{k})$. Since $\delta(T) = \infty$, it is clear that T is distinct from the points $P_{i_1}, P_{i_2}, P_{i_3}$. Since δ is defined over k, for any Galois action $\xi \in G(\overline{k}/k)$ we have $\xi(\delta^*(\infty)) = \delta^*(\xi(\infty)) = \delta^*(\infty)$ so $P_{i_4} + P_{i_5} + \xi(T) = \xi(P_{i_4} + P_{i_5} + T) = P_{i_4} + P_{i_5} + T$, implying $\xi(T) = T$. Since ξ was arbitrary, we have $T \in C(k)$. Ergo if such a subset and point do not exist, then $N_3(D) < 5$, so $N_3(D) = 4$ and

the result follows from Proposition 4.3.7. □

Corollary 4.3.10. *Let C be a nonsingular projective curve of genus 2 defined over a number field k. Let S be a finite set of places of k. Let $P_1, \ldots, P_n \in C(k)$ be distinct and define the divisor $D := \sum_{i=1}^{n} P_i$. Let $\varepsilon > 0$. Then for all $Q \in C(\overline{k})$ with $[k(Q) : k] = 3$,*

$$m_{D,S}(Q) \leq (\tilde{N}_3(D) + \varepsilon) h_R(Q) + O(1)$$

where $\tilde{N}_3(D) = N_3(C, \overline{k}, D) := \max\left\{\left|\left(\sigma^{-1}(0) \cup \sigma^{-1}(\infty)\right) \cap \mathrm{Supp}(D)\right|\right\}$ taken over all finite morphisms $\sigma : C \to \mathbb{P}^1$ of degree 3. If no such morphism exists, we say $\tilde{N}_3(D) = 0$.

Proof. note that $N_3(D) \leq \tilde{N}_3(D)$, so the inequality is implied by Corollary 4.3.9 except in cases where $\deg(D) = 3$ or 4.

Consider the morphism $[\cdot, \cdot] : C^2 \to \mathrm{Jac}(C)$ defined by $[T, U] = \mathcal{O}(U - T)$. If $[T, U] = [T', U']$, then $T + U' \sim T' + U$, and since the hyperelliptic morphism is unique, it follows that $[\cdot, \cdot]$ is 2-to-1, and comparing dimensions, we see it is surjective.

Thus if $\deg(D) = 4$, there exist $T, U \in C(\overline{k})$ such that

$$P_{i_1} + P_{i_2} + T \sim P_{i_3} + P_{i_4} + U.$$

We can always arrange the points so that P_{i_1} and P_{i_2} are not hyperelliptic conjugates and P_{i_3} and P_{i_4} are not hyperelliptic conjugates, so this defines a base point free linear system of dimension 1 and degree 3. Thus there is a morphism $\sigma : C \to \mathbb{P}^1$ of degree 3 with $\sigma(P_{i_1}) = \sigma(P_{i_2}) = 0$ and $\sigma(P_{i_3}) = \sigma(P_{i_4}) = \infty$, that is $\tilde{N}_3(D) = 4$.

Similarly if $\deg(D) = 3$, then for any $V \in C(\overline{k})$ there exist $T, U \in C(\overline{k})$ such that

$$P_{i_1} + P_{i_2} + T \sim P_{i_3} + V + U.$$

We can always arrange the points so that P_{i_1} and P_{i_2} are not hyperelliptic conjugates and choose V so that V is not the hyperelliptic conjugate of P_{i_3} and V is not equal to P_{i_1} or P_{i_2}, so that this defines a base point free linear system of dimension 1 and degree 3. Thus there is a morphism $\sigma : C \to \mathbb{P}^1$ of degree 3 with $\sigma(P_{i_1}) = \sigma(P_{i_2}) = 0$ and $\sigma(P_{i_3}) = \infty$, that is $\tilde{N}_3(D) = 3$.

In these cases, where $\tilde{N}_3(D) = \deg(D)$, we have

$$\begin{aligned} m_{D,S}(Q) &\leq h_D(Q) \text{ by Definition 2.2.8} \\ &\leq (\deg(D) + \varepsilon)h_R(Q) + O(1) \text{ by Theorem 2.2.12} \\ &= (\tilde{N}_3(D) + \varepsilon)h_R(Q) + O(1). \end{aligned}$$

□

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[2] P. Corvaja and U. Zannier. On integral points on surfaces. *Ann. of Math. (2)*, 160(2):705–726, 2004.

[3] Pietro Corvaja and Umberto Zannier. On a general Thue's equation. *Amer. J. Math.*, 126(5):1033–1055, 2004.

[4] Jan-Hendrik Evertse and Roberto G. Ferretti. A generalization of the Subspace Theorem with polynomials of higher degree. In *Diophantine approximation*, volume 16 of *Dev. Math.*, pages 175–198. SpringerWienNewYork, Vienna, 2008.

[5] Gerd Faltings. Diophantine approximation on abelian varieties. *Ann. of Math. (2)*, 133(3):549–576, 1991.

[6] Joe Harris and Joe Silverman. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.*, 112(2):347–356, 1991.

[7] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[8] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[9] Aaron Levin. On the Schmidt subspace theorem for algebraic points. *Duke Math. J.*, 163(15):2841–2885, 2014.

[10] Aaron Levin. Wirsing-type inequalities. *Bull. Inst. Math. Acad. Sin. (N.S.)*, 9(4):685–710, 2014.

[11] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[12] Min Ru and Pit-Mann Wong. Integral points of $P^n - \{2n + 1 \text{ hyperplanes in general position}\}$. *Invent. Math.*, 106(1):195–216, 1991.

[13] Joseph H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. *Math. Ann.*, 279(2):193–216, 1987.

[14] Xiangjun Song and Thomas J. Tucker. Dirichlet's theorem, Vojta's inequality, and Vojta's conjecture. *Compositio Math.*, 116(2):219–238, 1999.

[15] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2018.

[16] Paul Vojta. *Diophantine approximations and value distribution theory*, volume 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987.

[17] Paul Vojta. A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing. *J. Amer. Math. Soc.*, 5(4):763–804, 1992.