Distribution Agreement

In presenting this dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this dissertation. I retain all ownership rights to the copyright of the dissertation. I also retain the right to use in future works (such as articles or books) all or part of this dissertation.

_____ _____

Roberto Hernandez Date

Rational Points on a Family of Genus 3 Hyperelliptic Curves

By

Roberto Hernandez
Doctor of Philosophy

Mathematics

David Zureick-Brown, Ph.D.
Advisor

Raman Parimala, Ph.D.
Committee Member

Suresh Venapally, Ph.D
Committee Member

Accepted:

Kimberly Jacob Arriola, Ph.D.
Dean of the James T. Laney School of Graduate Studies

June 25, 2025

Date

Rational Points on a Family of Genus 3 Hyperelliptic Curves

By

Roberto Hernandez
B.A., California State University, Fullerton, CA, 2020
M.S., Emory University, GA, 2024

Advisor: David Zureick-Brown, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2025

Abstract

Rational Points on a Family of Genus 3 Hyperelliptic Curves
By Roberto Hernandez

Let $C/\mathbb{Q}$ be a curve defined over the rational numbers of genus $g \geq 2$. In 1922, Mordell conjectured that such a curve had only finitely many rational points. This question puzzled mathematicians for over 60 years until Faltings' proved it in 1983. In fact, Faltings' proved the more general version which said that the curve was allowed to be defined over any number field. This was a groundbreaking result and signified a huge advancement in arithmetic geometry. Unfortunately, Faltings' theorem isn't effective, meaning that the proof doesn't actually tell us how to find the points, only that there's finitely many. Despite new, simpler proofs of Faltings' theorem by Voljta and Bombieri, we still do not have a grasp of an effective version of Faltings' theorem. In practice, Chabauty–Coleman is a powerful tool for finding rational points on curves, but there are examples for which this method fails. We give a detailed exposition of the method developed by Dem'yanenko and Manin to explicitly find rational points on curves. To this end, we construct a family of genus 3 hyperelliptic curves for which we can compute the rational points on via the method of Dem'yanenko–Manin while avoiding the method of Chabauty–Coleman.

Rational Points on a Family of Genus 3 Hyperelliptic Curves

By

Roberto Hernandez
B.A., California State University, Fullerton, CA, 2020
M.S., Emory University, GA, 2024

Advisor: David Zureick-Brown, Ph.D.

A dissertation submitted to the Faculty of the
Emory College of Arts and Sciences of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2025

Acknowledgments

I would like to thank the Math Department at Emory University for the support and resources provided to me during my time in graduate school. It has been a rewarding experience and I have had the pleasure of working with many incredible faculty who have helped me become a better researcher and educator. I would also like to thank the staff who were always there to help, and in particular to Terry, who always provided a friendly face and an occasional fun Atlanta United outing.

I would also like to thank my advisor David Zureick-Brown, for always being available for questions and for all the advice he provided relating to research and navigating the job market. His mentorship was an invaluable part of my graduate journey.

One of the things I am most proud of in my journey through math has been the community of amazing people who I have met and have helped me reach this point. There are far too many to name, but to those of you who have been there to support me and give me advice, know that I am so grateful for you.

I also have to give a shout out to my community from back home for always reminding me where I came from and for letting me bring a piece of home to Atlanta. My family has been the greatest support system and I would not be who I am today without their love and care.

Last but definitely not least, I have to thank Jazzy, who I embarked on this journey with and have learned so much from. Thank you for all the love and support you give, and for being my home away from home.

Contents

Chapter 1

Introduction

In 1900, Hilbert challenged the mathematical community with his list of problems that were to be tackled for the next century. In particular, the 10th problem asks whether there exists a general algorithm which takes as input a Diophantine equation and decides whether there exists a solution in the integers. This question was answered negatively in 1970 with Matiyasevich [13] concluding the work that had been started 20 years earlier by Davis, Robinson, and Putnam. In 1983, Faltings [6] proved Mordell's Conjecture stating that any non-singular curve C defined over $\mathbb{Q}$ of genus greater than one has finitely many rational points. In fact, he proved a more general version which allowed the curve to be defined over any number field rather than simply over $\mathbb{Q}$. His ground breaking result symbolized an advancement in arithmetic geometry that had been out of reach since 1922, the year Mordell first made the conjecture. Now, the study of rational points on non-singular curves defined over $\mathbb{Q}$ can be fully classified into the following trichotomy:

(a) $\text{Gen}(C) = 0$: In this case, we know that C either has no rational points, or infinitely many, in which case it can be realized as a conic in projective space.

(b) $\text{Gen}(C) = 1$: Assuming C has a rational point, these are known as elliptic curves and the theory is rich in regards to the study of their rational points. It is a

result of Mordell-Weil that the rational points form a finitely generated abelian group and moreover, Mazur's torsion theorem restricts the structure of the torsion subgroup.

(c) $\mathrm{Gen}(C) > 1$: This is precisely the case when Faltings's theorem applies. Here we know that C has finitely many rational points.

This exemplifies that geometry governs arithmetic, as the genus is the most important geometric invariant of a curve. While Faltings's theorem is revolutionary, its only flaw is that it doesn't give an instructive way to obtain all the rational points on C. Effectively finding rational points on curves of genus greater than one is an active area of research, with many working to better understand or improve current methods. The method which has proved to be most powerful in computing rational points on curves has been the method Chabauty–Coleman. In this thesis, we focus on the method developed by Dem'yanenko [5] in 1968, extended by Manin [12] in 1969. We present an explicit family of curves for which we can use the method of Dem'yanenko–Manin and will aim to restrict the cases so that we avoid satisfying the hypothesis of Chabauty–Coleman.

1.1 Outline

This thesis is organized in the following way:

Chapter 2: We give the necessary background involving the theory of heights, elliptic curves, hyperelliptic curves, elliptic surfaces and Jacobians. We follow the treatment of the subject given in [9], [18], and [17].

Chapter 3: We describe the method of Dem'yanenko–Manin and give an outline of how it provides an effective tool for computing rational points on specific curves. We also give an overview of curves with certain geometric aspects that are well suited for this method and why in practice it is difficult to find such curves.

Chapter 4: We demonstrate the construction of the family of genus 3 hyperelliptic curves for which we can use Dem'yanenko–Manin and discuss the morphisms we obtain to an elliptic curve. We also state one of our main results which deals with the decomposition of the Jacobian for our family of curves. We also discuss how we, conjecturally, have infinitely many curves in our family for which the method of Dem'yanenko-Manin applies, while Chabauty-Coleman does not.

Chapter 5: Here we mainly state and prove our lemmas bounding the canonical height of the image of a point on C_a, which in turn allows us to effectively find the rational points. We end by demonstrating an example of the method in question.

Chapter 2

Background

Let k be a number field and let V/k be a smooth projective variety defined over k, with a fixed embedding into some projective space $\mathbb{P}^n$. In this situation, the study of rational and integral points on varieties requires a way of measuring the "size" or "arithmetic complexity" of a point. In order to do this, we use a fundamental tool called a height function. A height function is a positive-valued function

$$h : V(k) \to [0, \infty)$$

which assigns to each point on the variety a positive real number. The idea here is that we want a way to translate geometric information about the variety to arithmetic information about its k-rational points. A good height function should therefore have two properties:

1. There should be only a finite number of points with bounded height. In other words, the set

   $$\{P \in V(k) : h(P) \leq B\}$$

   is finite. This is called the Northcott property.

2. The "size" of a point should reflect both the arithmetic nature of the point and

the geometric characteristics of the variety.

Our survey of the subject closely follows [9] so we begin by describing height function on projective space and then use the theory of divisors to extend the definition more generally for varieties.

2.1 Heights

Let $P \in \mathbb{P}^n(\mathbb{Q})$ and write $P = (x_0, x_1, \ldots, x_n)$ with $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$. We define the height of P to be

$$H(P) = \max\{|x_0|, |x_1|, \ldots, |x_n|\}.$$

We note that in defining the height on $\mathbb{P}^n(\mathbb{Q})$ in this way, we satisfy the first property that all "good" height functions should have. That is, the set

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) \leq B\}$$

is finite, since there are only finitely many integers x satisfying $|x| \leq B$.

Definition 1. Let k be a number field and let $P \in \mathbb{P}^n(k)$. The multiplicative height of P is the quantity

$$H_k(P) = \prod_{v \in M_k} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\}$$

and the logarithmic height is defined as

$$h_k(P) = \log H_k(P).$$

The definition of the height of P in this way is well-defined, due to the product formula,

and is independent of the choice of homogeneous coordinates for P. We can also define an absolute height on $\mathbb{P}^n$ which is independent of the field.

Definition 2. The absolute multiplicative height on $\mathbb{P}^n$ is the function

$$H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [1, \infty), \qquad H(P) = H_k(P)^{1/[k:Q]}$$

where k is any field with $P \in \mathbb{P}^n(k)$. The absolute logarithmic height on $\mathbb{P}^n$ is given by

$$h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty), \qquad h(P) = \log H(P) = \frac{1}{[k : \mathbb{Q}]} h_k(P).$$

Next we describe the first example of the interplay between geometry and arithmetic through the language of height functions.

Theorem 2.1.1. Let X be a closed subvariety of $\mathbb{P}^n$ and let $\varphi : X \to \mathbb{P}^n$ be a morphism of degree d. Then

$$h(\varphi(P)) = dh(P) + O(1) \qquad \text{for all } P \in X(\overline{\mathbb{Q}}).$$

It is important to note here that the $O(1)$ depends only on the map φ, but it independent of the point P. In practice, it is generally straightforward to provide an upper bound of the form $h(\varphi(P)) \leq dh(P) + c_1(\varphi)$. However, providing a lower bound of the form $h(\varphi(P)) \geq dh(P) + c_2(\varphi)$ is more challenging. We will see in a future section how we handle these bounds in our case.

Now assume that V is a projective variety defined over $\mathbb{Q}$ with an embedding $\varphi : V \to \mathbb{P}^n$ into projective space. In this way we can define a height function on the variety V.

Definition 3. Let $\varphi : V \to \mathbb{P}^n$ be a morphism. The height on V relative to φ is the function

$$h_\varphi : V(\mathbb{Q}) \to [0, \infty), \qquad h_\varphi(P) = h(\varphi(P)),$$

where $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty)$ is the height function on projective space that we defined in the previous section.

In this way, we see that defining heights on varieties is very natural once you have an embedding of your variety into projective space. In the following theorem, we present Weil's construction that associates a height function to every divisor. This gives us a way to define a height function on every variety. This theorem can be viewed as a machine that converts geometric statements in terms of divisor class relations into arithmetic statements described by relations among height functions.

Theorem 2.1.2 (Weil's Height Machine)**.** Let k be a number field. For every smooth projective variety V/k there exists a map

$$h_V : \mathrm{Div}(V) \to \{\text{functions } V(\overline{k}) \to \mathbb{R}\}$$

with the following properties:

1. (Normalization) Let $H \subset \mathbb{P}^n$ be a hyperplane, and let $h(P)$ be the absolute logarithmic height on $\mathbb{P}^n$ defined before. Then

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1) \qquad \text{for all } P \in \mathbb{P}^n(\overline{k}).$$

2. (Functoriality) Let $\varphi : V \to W$ be a morphism and let $D \in \mathrm{Div}(W)$. Then

$$h_{V,\varphi^* D}(P) = h_{W,D}(\varphi(P)) + O(1) \qquad \text{for all } P \in V(\overline{k}).$$

3. (Additivity) Let $D, E \in \mathrm{Div}(V)$. Then

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1) \qquad \text{for all } P \in V(\overline{k}).$$

4. (Linear Equivalence) Let $D, E \in \mathrm{Div}(V)$ with D linearly equivalent to E. Then

$$h_{V,D}(P) = h_{V,E}(P) + O(1) \qquad \text{for all } P \in V(\overline{k}).$$

5. (Positivity) Let $D \in \mathrm{Div}(V)$ be an effective divisor, and let B be the base locus of the linear system $|D|$. Then

$$h_{V,D}(P) \geq O(1) \qquad \text{for all } P \in (V - B)(\overline{k}).$$

6. (Algebraic Equivalence) Let $D, E \in \mathrm{Div}(V)$ with D ample and E algebraically equivalent to 0. Then

$$\lim_{\substack{P \in V(\overline{k}) \\ h_{V,D}(P) \to \infty}} \frac{h_{V,E}(P)}{h_{V,D}(P)} = 0.$$

7. (Finiteness) Let $D \in \mathrm{Div}(V)$ be ample. Then for every finite extension k'/k and every constant B, the set

$$\{P \in V(k') : h_{V,D}(P) \leq B\}$$

is finite.

8. (Uniqueness) The height functions $h_{V,D}$ are determined, up to $O(1)$, by normalization, functoriality for embeddings, and additivity.

It is important to note that Weil's height machine requires smoothness of your variety, but the construction still works when dealing with singular varieties. One does have to pass to use Cartier divisors rather than Weil divisors instead. Again, we state that the $O(1)$'s appearing in the heights presented in Weil's height machine are all explicitly computable, and depend only on φ, V, and D.

Remark 1. Note that Property 4 in Weil's height machine tells us that the heights

given by linearly equivalent divisors are equal up to some constant, so in particular, we can rephrase the previous theorem in terms of the Picard group of V, rather than its group of divisors.

As we saw in the previous section, the height machine assigns to each divisor on V a height function. These height functions are all well-defined and satisfy various properties. In some cases, it is possible to define a height function with particularly nice properties.

Theorem 2.1.3 (Néron, Tate)**.** Let V/k be a smooth variety defined over a number field. Let $D \in \mathrm{Div}(V)$ and let $\varphi : V \to V$ be a morphism. Suppose that $\varphi^* D \sim \alpha D$ for some number $\alpha > 1$. Then there is a unique function called the canonical height on V relative to φ and D,

$$\hat{h}_{V,\varphi,D} : V(\overline{k}) \to \mathbb{R},$$

with the following properties:

1. $\hat{h}_{V,\varphi,D}(P) = h_{V,D}(P) + O(1)$ for all $P \in V(\overline{k})$.
2. $\hat{h}_{V,\varphi,D}(\varphi(P)) = \alpha \hat{h}_{V,\varphi,D}(P)$ for all $P \in V(\overline{k})$.

It is important to note here that the canonical height depends only on the linear equivalence class of D and that it can be computed as the following limit:

$$\hat{h}_{V,\varphi,D}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\varphi^n(P)),$$

where $\varphi^n = \varphi \circ \varphi \cdots \circ \varphi$. In particular, the canonical height has many useful properties when the theory is applied to abelian varieties with a symmetric divisor class, as we see in the following result, again due to Néron and Tate.

Theorem 2.1.4 (Néron, Tate)**.** Let A/k be an abelian variety defined over a number field, and let $D \in \mathrm{Div}(A)$ be a divisor whose divisor class is symmetric. There is a

height function

$$\hat{h}_{A,D} : A(\overline{k}) \to \mathbb{R},$$

called the canonical height on A relative to D, with the following properties:

1. $$\hat{h}_{A,D}(P) = h_{A,D}(P) + O(1) \text{ for all } P \in A(\overline{k}).$$

2. For all integers m,

$$\hat{h}_{A,D}([m]P) = m^2 \hat{h}_{A,D}(P) \text{ for all } P \in A(\overline{k}).$$

3. (Parallelogram Law)

$$\hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q) \text{ for all } P, Q \in A(\overline{k}).$$

4. The canonical height map $\hat{h}_{A,D} : A(\overline{k}) \to \mathbb{R}$ is a quadratic form. The associated pairing $\langle \cdot, \cdot \rangle_D : A(\overline{k}) \times A(\overline{k}) \to \mathbb{R}$ defined by

$$\langle P, Q \rangle_D = \frac{\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q)}{2}$$

   is bilinear and satisfies $\langle P, P \rangle = \hat{h}_{A,D}(P)$.

5. (Uniqueness) The canonical height $\hat{h}_{A,D}$ depends only on the divisor class of the divisor D. It is uniquely determined by (1) and (2) for any one integer $m \geq 2$.

Moreover, if the divisor D from the previous theorem is ample, then we actually obtain a stronger result, which says that the canonical height of a point $P \in V(\overline{k})$ is 0 if and only if P is a torsion point. Thus, $\hat{h}_{A,D}$ is a positive definite quadratic form on $A(\overline{k})/(\text{torsion})$. In fact, we know more is true.

Proposition 1. Let A/k be an abelian variety defined over a number field, and let $D \in \mathrm{Div}(A)$ be an ample divisor with symmetric divisor class.

1. For all $P \in A(\overline{k})$, we have $\hat{h}_{A,D}(P) \geq 0$, with equality if and only if P is a point of finite order.

2. The associated canonical height function extends $\mathbb{R}$-linearly to a positive definite quadratic form

$$\hat{h}_{A,D} : A(\overline{k}) \otimes \mathbb{R} \to \mathbb{R}.$$

In particular, if $P_1, \ldots, P_r \in A(\overline{k}) \otimes \mathbb{R}$ are linearly independent, then the height regulator

$$\det(\langle P_i, P_j \rangle_D)_{1 \leq i,j \leq r}$$

is strictly greater than 0.

The two previous results are for divisor classes which are symmetric, but it turns out that there are analogous results for anti-symmetric divisor classes. In that case, it turns out that the associated canonical heights turn out to be linear rather than quadratic. Now, since any divisor can almost be written as the sum of a symmetric divisor and an antisymmetric divisor, then we can find a canonical height function associated to every divisor on V. Of interest to us for this thesis will be when we define the corresponding notions of heights on the simplest of abelian varieties, an elliptic curve. In the next section we recall some of the theory surrounding elliptic curves.

2.2 Elliptic Curves over $\mathbb{Q}$

Our main focus in this section will be elliptic curves over $\mathbb{Q}$, but it is important to note that the theory has been well-developed more generally over number fields, and even over local fields. All the facts we mention here can be found with more detail in

[18]. First, we recall that an elliptic curve is defined as a smooth, projective, genus one curve with a specified base point (usually ∞). It turns out that there is an equivalent definition in terms of abelian varieties. Indeed, an elliptic curve can also be defined as an abelian variety of dimension 1. For our purposes, we will focus mainly on the former definition, and in fact, we will be more explicit in that we present explicit equations for all the elliptic curves we will deal with. Concretely, an elliptic curve can be described by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbb{Q}$, remembering that this is an affine representation of E and it includes the extra point at infinity $[0, 1, 0]$. Even better, in our case we can write E in its short Weierstrass form given by

$$E : y^2 = Ax + B,$$

with $A, B \in \mathbb{Q}$. This could be done anytime the characteristic of your field is not 2 or 3, via substitutions. Associated with each elliptic curve are two important invariants: the discriminant Δ, and its j-invariant given by:

$$\Delta = -16(4A^3 + 27B^2) \qquad \text{and} \qquad j = -1728\frac{(4A)^3}{\Delta}.$$

Note that there are equations for the j-invariant and discriminant of the longer Weierstrass equation above, but we present the ones for this form for convenience. The j-invariant controls the isomorphism class of an elliptic curve over $\overline{\mathbb{Q}}$ while the discriminant can help us detect primes of bad reduction. In particular, we have the following result:

Proposition 2. Two elliptic curves are isomorphic over $\overline{\mathbb{Q}}$ if and only if they have the same j-invariant.

One of the most important features of elliptic curves is that their points satisfy a group law, that is, the rational points of E, $E(\mathbb{Q})$, forms a group with the identity being the point at infinity, O. Now, once we know that we can properly define addition on the rational points of an elliptic curve, a natural question one can ask is: are there points $P \in E(\mathbb{Q})$ such that $[m]P = O$ where $[m]P = P + P + \cdots + P$ (m terms)?

Definition 4. Let E be an elliptic curve and let $m \geq 1$ be an integer. The m-torsion points on E form a subgroup of $E(\mathbb{Q})$ and we denote them by

$$E[m] = \{P \in E : m[P] = O\}.$$

The torsion subgroup of E, denoted E_{tor} is the set of points of finite order, denoted

$$E_{\text{tor}} = \bigcup_{m=1}^{\infty} E[m].$$

Now that we have defined the rational points on an elliptic curve as well as its torsion subgroup, we are ready to state arguably the two most important results about the arithmetic of elliptic curve.

Theorem 2.2.1 (Mordell-Weil)**.** Let E be an elliptic curve over $\mathbb{Q}$. The group $E(\mathbb{Q})$ is finitely generated, and moreover, it has the form $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \times \mathbb{Z}^r$ where r is called the rank of $E(\mathbb{Q})$.

Theorem 2.2.2 (Mazur's Torsion Theorem)**.** Let E be an elliptic curve over $\mathbb{Q}$. The torsion subgroup E_{tor} is isomorphic to one of the following fifteen groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \quad &\text{with} \quad 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad &\text{with} \quad 1 \leq N \leq 4. \end{aligned}$$

Further, each of these groups occurs as the torsion subgroup of some elliptic curve over $\mathbb{Q}$.

In particular, the Mordell-Weil theorem implies that the rank of E really controls the finiteness of rational points on E. Concretely, if $\text{Rank}(E) = 0$, then $\#E(\mathbb{Q})$ is finite; otherwise there are infinitely many rational points on E. This is something that is special about elliptic curves, as we will see in a future discussion, the infinitude of rational points on curves is heavily dependent on the genus of the curve.

2.3 Elliptic Curves over Local Fields

Let E be an elliptic curve over some local field K, complete with respect to a discrete valuation v. The main purpose of this section is to discuss the reduction of elliptic curves modulo some prime number p. First, we recall that an elliptic curve is given by some Weierstrass equation say,

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the $a_i \in K$. There is some notion of a minimal Weierstrass equation which is determined by the decomposition of the discriminant. Concretely, if all the prime factors appearing in the discriminant of E have valuation strictly less than 12, we can conclude the given model of E is minimal. The important thing to keep in mind here is that over any local field, every elliptic curve has a minimal model, which is unique up to a change of coordinates.

Now that we can work under the assumption that we have a minimal model of E, we turn our focus to the reduction modulo p of E, which we will denote $\widetilde{E}$. It is important to note that in our case, starting out with an integral model defined over $\mathbb{Q}$, and reducing modulo p means that $\widetilde{E}$ will now be defined over $\mathbb{F}_p$. To obtain $\widetilde{E}$, we reduce the coefficients of E modulo p and we write

$$\widetilde{E} : y^2 = \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$$

where $\widetilde{a_i} \in k$. Now, in doing the reduction of E we may inadvertently introduce singularities in the form of cusps or nodes.

Definition 5. Let E be an elliptic curve over $\mathbb{Q}$ and let $\widetilde{E}$ be its reduction modulo some prime p. Then

1. E has good reduction at p if $\widetilde{E}$ is nonsingular.
2. E has multiplicative reduction at p if $\widetilde{E}$ has a node.
3. E has additive reduction at p if $\widetilde{E}$ has a cusp.

In the cases of (1) and (2) we say that E has bad reduction at p. Moreover, if E has multiplicative reduction at p, then the reduction is said to be split if the slopes of the tangent lines at the node lie in $\mathbb{F}_p$, and is otherwise called nonsplit.

The next result allows us to determine the reduction type of an elliptic curve from its minimal Weierstrass equation.

Proposition 3. Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass equation

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation, and let c_4 be the usual expression involving the a_i. Then

1. E has good reduction at p if and only if $v_p(\Delta) = 0$. In this case $\widetilde{E}$ is an ellptic curve.
2. E has multiplicative reduction at p if and only if $v_p(\Delta) > 0$ and $v_p(c_4) = 0$.
3. E has additive reduction at p if and only if $v_p(\Delta) > 0$ and $v_p(c_4) > 0$.

2.4 Heights on Elliptic Curves

Having defined heights on projective space and varieties, we focus in more on our main object of study which are elliptic curves and discuss the canonical height on an elliptic curve. First, recall that any nonconstant function f in the function field $K(E)$ determines a surjective morphism from E to $\mathbb{P}^1$. Concretely, f gives the map

$$f : E \to \mathbb{P}^1, \qquad P \mapsto \begin{cases} [1,0] \text{ if } P \text{ is a pole of } f \\ [f(P),1] \text{ otherwise.} \end{cases}$$

With this in mind, we can now define the height on an elliptic curve.

Definition 6. Let $E/\mathbb{Q}$ be an elliptic curve and let f be a function in the function field of E. The height on E relative to f is the function

$$h_f : E(\overline{\mathbb{Q}}) \to \mathbb{R}, \qquad h_f(P) = h(f(P)).$$

Then next result verifies that the height defined in this way satisfies the Northcott property that we want height functions to have.

Proposition 4. Let $E/\mathbb{Q}$ be an elliptic curve and f be a nonconstant function. Then for any constant C, the set

$$\{P \in E(\overline{\mathbb{Q}} : h_f(P) \leq C\}$$

is a finite set of points.

We also present results which lie at the heart of the relationship between height functions and the additive law we have on an elliptic curve.

Proposition 5. Let $E/\mathbb{Q}$ be an elliptic curve and let f be an even function (i.e., a function satisfying $f \circ [-1] = f$). Then for all $P, Q \in E(\overline{\mathbb{Q}})$ we have

1. $h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$.

2. $h_f([m]P) = m^2 h_f(P) + O(1)$ for $m \in \mathbb{Z}$.

It's important to remark here that the $O(1)$'s appearing in the proposition depend on E, f, and m, but are independent of the points P and Q. Moreover, this result is true more generally for odd functions as well since if f is odd, f^2 is even.

2.5 Elliptic Surfaces

One way to define an elliptic surface is an a one-parameter algebraic family of elliptic curves. Concretely, since we are working over $\mathbb{Q}$, consider rational functions $A(T), B(T) \in \mathbb{Q}(T)$, then we can look at the elliptic surface

$$E_T : y^2 = x^3 + A(T)x + B(T).$$

We can replace T with some $t \in \mathbb{Q}$ and for most cases, we will get a well-defined elliptic curve over $\mathbb{Q}$. The only cases where we do not obtain an elliptic curve is for those values $t \in \mathbb{Q}$ for which $A(t) = \infty$, $B(t) = \infty$, or $\Delta(t) = -16(4A(t)^3 + 27B(t)^2) = 0$. We call E_t the specialization of E_T. It turns out that as long as the discriminant of E_T is non-zero, E_T will be an elliptic curve defined over $Q(T)$, so much of the theory that one develops over $\mathbb{Q}$ will still be true over the function field.

Definition 7. Let C be a non-singular projective curve. An elliptic surface over C consists of the following data:

1. a surface $\mathcal{E}$ (2-dimensional projective variety)

2. a morphism

$$\pi : \mathcal{E} \to C$$

such that for all but finitely many points $t \in C(\overline{k})$, the fiber

$$\mathcal{E}_t = \pi^{-1}(t)$$

is a non-singular curve of genus 1,

3. a section to π,

$$\sigma_0 : C \to \mathcal{E}.$$

It turns out that most of the fibers of an elliptic surface will be smooth, and so we call those good fibers. The cases where $\mathcal{E}_t$ is not smooth are called bad fibers. Of particular interest to us are rational elliptic surfaces and elliptic K3 surfaces. Following [15] we describe some of the background about these two specific families of elliptic surfaces.

Definition 8. The Néron-Severi group of $\mathcal{E}$, denoted by $\mathrm{NS}(\mathcal{E})$, is the group of divisors modulo algebraic equivalence.

It turns out that $\mathrm{NS}(\mathcal{E})$ is a finitely generated group and that the intersection pairing on the group of $\mathrm{Div}(\mathcal{E})$ gives a well-defined pairing on $\mathrm{NS}(\mathcal{E})$. Of importance to us will be the fundamental relation between the rank of the elliptic surface, and its associated elliptic curve.

Theorem 2.5.1 (Shioda-Tate)**.** Let $\mathcal{E}$ be an elliptic surface defined over $\mathbb{Q}$, and E be its associated elliptic curve. Then

$$\mathrm{Rank}(\mathrm{NS}(\mathcal{E})) = \mathrm{Rank}(E(\mathbb{Q})) + 2 + \sum_{t \in C}(r_t - 1),$$

where r_t is the number of irreducible components in the fiber $\mathcal{E}_t$.

We should note that $\mathrm{Rank}(\mathrm{NS}(\mathcal{E}))$ is called the Picard number of $\mathcal{E}$, denoted $\rho(\mathcal{E})$ and so we will commonly use the Shioda-Tate formula to calculate the rank of the elliptic

surface to help bound the rank of specializations from below. Concretely, we have the reformulation of the Shioda-Tate formula as follows:

$$\text{Rank}(E(\mathbb{Q})) = \rho(\mathcal{E}) - 2 - \sum_{t \in C}(r_t - 1).$$

Rational elliptic surfaces are elliptic surfaces which are fibred over the projective line. That is, in the definition we presented earlier, $C \cong \mathbb{P}^1$. As a consequence of Tate's algorithm, we can present every rational elliptic surface with a globally minimal Weierstrass model. In particular, a rational elliptic surface S with a section is given by the following equation:

$$S : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $\deg(a_i) \leq i$. It turns out that the Picard number of a rational elliptic surface defined over $\mathbb{Q}$ is exactly 10, which makes this class of elliptic surfaces nice for our purposes since Shioda-Tate implies that to find the rank, we only need to compute the number of components of the bad fibers. This will be incredibly useful when we work with our explicit equations in Chapter 4.

We now turn our focus briefly to elliptic K3 surfaces. A K3 elliptic surface X has base curve $\mathbb{P}^1$, and can be expressed by a globally minimal model as follows:

$$X : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in \mathbb{Q}[t]$ and $\deg(a_i) \leq 2i$. In general the Picard number of an elliptic surface S is bounded above by $b_2(S)$, the 2nd Betti number. For elliptic K3 surfaces, $b_2(S) = 22$ so that serves as an upper bound for X. In particular, when the field is of characteristic 0, the upper bound is 20. Thus, for our purposes, $\rho(X) \leq 20$ and this will help us place an upper bound on the elliptic K3 surface which appears as a factor in our

Jacobian.

One of the main uses of elliptic surfaces is that they provide a way exhibit explicit elliptic curves of high rank. Namely, we have the following result due to Néron and Silverman.

Theorem 2.5.2. Let $E/K(t)$ be a non-isotrivial (nonconstant j-invariant) elliptic surface. Then the specialization map

$$\sigma_t : E \to E_t$$

is well-defined and injective for all but finitely many points $t \in K$.

In practice, one constructs an elliptic surface of large rank, and then tries to find specializations in which the rank jumps. One of the most famous applications of this technique was done by Elkies, when finding the, at the time, record breaking elliptic curve of rank 28 over $\mathbb{Q}$.

2.6 Hyperelliptic Curves and Jacobians

We now begin our discussion on hyperelliptic curves, which are generalizations of elliptic curves. We note that our focus will remain over $\mathbb{Q}$, but the theory is vastly expansive over more general fields.

Definition 9. A hyperelliptic curve is of the form $C : y^2 = f(x)$, where $f(x)$ is a monic polynomial of degree $2g + 1$ or $2g + 2$, which admits a degree 2 map to $\mathbb{P}^1$.

It's important to note that hyperelliptic curves live in weighted projective space $\mathbb{P}(1, g + 1, 1)$ so the projective equation of a hyperelliptic curve ma contain one or two points at infinity, depending on the degree of f. In particular, if $\deg(f)$ is even, then C has two points at infinity, and if $\deg(f)$ is odd, then C only has one point at infinity.

Moreover, every genus 2 curve is hyperelliptic. This is because the anti-canonical map given by the anti-canonical divisor is a morphism of degree 2 from C to $\mathbb{P}^1$. In our work, we will explicitly show the family of genus 3 hyperelliptic curves which arise from our construction and since the genus is 3, Falting's theorem tells us that there are only finitely many rational points.

There is a natural abelian variety attached to each hyperelliptic curve called the Jacobian, denoted $J(C)$. It is an abelian variety of dimension g over $\mathbb{Q}$, and it is therefore projective and although it could in principle be presented through equations, it is typically not favorable to work with it in that way. Instead, we use that there is an $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism between the abelian group $J(\overline{\mathbb{Q}})$ and the group of linear equivalence classes of degree-0 divisors on $C_{\overline{\mathbb{Q}}}$. The Jacobian can be defined in fact for elliptic curves, but it turns out that for an elliptic curve E, we have $E \cong J(E)$. Also, as it pertains to rational points, there have been many advancements in the search for effective Falting's through the use of the Jacobian. In particular, the following result is one that is very commonly used to find rational points on curves.

Theorem 2.6.1 (Chabauty-Coleman)**.** Let X be a curve of $g \geq 2$ over $\mathbb{Q}$. Let J be it's Jacobian. Let p be a prime of good reduction and let $r = \mathrm{Rank}(J(\mathbb{Q}))$. If $r < g$, then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. Moreover, $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)$.

The Jacobian possesses many nice geometric properties, but of main concern for us is the fact that there is a nice way to embed a projective curve into its Jacobian. Indeed, given a fixed point $P_0 \in C$, then one defines the map $P \mapsto (P) - (P_0)$ for $P \in C$. In this way we've defined a map from the curve C to $J(C)$ and it turns out that as long as the genus of C is nonzero, this map is an embedding of C onto its Jacobian. For our purposes, we will discuss the Jacobian of our hyperelliptic curves, but this fact is true more generally for any smooth projective curve of genus at least 1.

Definition 10. A simple abelian variety is an abelian variety whose only subvarieties are itself and zero.

It turns out that, much like in the theory of finite abelian groups, there is a decomposition of abelian varieties into simpler abelian varieties.

Proposition 6. Let A be an abelian variety. Then there exist pairwise non-isogenous simple abelian varieties $A_1, \ldots, A_r$ and positive integers $n_1, \ldots, n_r$ such that $A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}$. This decomposition is unique up to isogeny.

In particular, this means that we can decompose the Jacobian of our curve into a product of simpler abelian varieties. In our context, we will actually enforce the Jacobian of our curves to decompose into a product of elliptic curves.

Chapter 3

Dem'yanenko–Manin

We now turn our attention to the method by which we will find the rational points on our hyperelliptic curves. It was first developed by Dem'yanenko [5] to show that rational points on a certain class of curves could be effectively computed and then extended by Manin [12] to give an upper bound on the p-power torsion on elliptic curves. More recently, it has been used by Silverman [16] to show that there are no rational points on a certain family of twists of Fermat curves and by Viada [19] to find rational points on curves of increasing genus embedded in products of elliptic curves. Other examples of this method in practice are given by Kulesz and Girard [11], [7].

3.1 Statement

Let C be a smooth projective curve of genus $g \geq 2$ over a number field K. Let A be an abelian variety over K, and let $f_1, \ldots, f_m$ be morphisms from C to A defined over K. Recall that a morphism is a rational map with no base points.

Definition 11. Let $f_1, \ldots, f_m$ be morphisms from C to A. We say the f_i are independent if $\sum n_i f_i$ is the constant map, then $n_i = 0$ for all i.

In practice, we don't typically use the definition to check whether a set of morphisms

are independent, instead we use a very nice lemma due to Cassels [4].

Lemma 3.1.1 (Cassels)**.** Let $f_1, \ldots, f_m$ be morphisms from C to A. Let D be the matrix whose coefficients are

$$\langle f_i, f_j \rangle = \frac{1}{2} \left(d(f_i + f_j) - d(f_i) - d(f_j) \right),$$

where $d(f_i)$ denotes the degree of the morphism. The m morphisms are independent if and only if $\det(D) \neq 0$.

For our purposes, we will work with explicit morphisms between our curves and thus these degrees are computable through the use of the computer programming system Magma [3].

Theorem 3.1.2 (Dem'yanenko-Manin)**.** Let C be a curve over a number field K and A be an abelian variety over K. Let $f_1, \ldots, f_m$ be morphisms from C to A that are defined over K and independent. Assume further that $\mathrm{Rank}(A) < m$. Then $C(K)$ is finite and it is possible to effectively bound the height of the points in $C(K)$.

It is important to note here that the conclusion that $C(K)$ is finite is not of particular interest, indeed, this is already true in this setting due to Falting's. The important part here is the second conclusion, ensuring that we can effectively find the K-rational points on C via height considerations.

Sketch of proof. Let $P \in C(K)$. Combining the functoriality relationship in 2.1.2 and the relationship between the canonical and naive heights on A we obtain

$$\hat{h}_A(f_i(P)) = c d(f_i) h_C(P) + O(1),$$

where c is a constant depending on the normalization of the heights involved. Com-

bining this fact with the height pairing in 2.1.4 we obtain

$$\lim_{h_C(P)\to\infty} \frac{\langle f_i(x), f_j(x)\rangle}{h_C(x)} = \langle f_i, f_j\rangle.$$

Now, taking the determinant over m gives the following:

$$\lim_{h_C(P)\to\infty} \frac{\det\left[\langle f_i(x), f_j(x)\rangle\right]}{h_C^m(x)} = \det\left[\langle f_i, f_j\rangle\right],$$

but the assumption that the m maps are linearly independent and the fact that the pairing $\langle\cdot,\cdot\rangle$ is positive definite, implies that $\det\left[\langle f_i, f_j\rangle\right] > 0$. Thus, it must be that $\det\left[\langle f_i(x), f_j(x)\rangle\right] > 0$, provided that $h_C(x)$ is sufficiently large. Hence, by 3.1.1, we have that $f_1(x), f_2(x), \ldots, f_m(x)$ must be linearly independent on A. We can rephrase this instead by saying that the set

$$\{x \in C(K) : f_1(x), f_2(x), \ldots, f_m(x) \text{ are linearly dependent in } A(K)\}$$

is a set of bounded height. Due to the Northcott property, we know that this must then be a finite set and, in particular, we can find a coefficient c such that $h_C(x) \leq c$. $\square$

In order to use this method of finding rational points on curves we need to obtain multiple maps from our curve to the same abelian variety. Now, as we have discussed before, the Jacobian is an abelian variety which can be decomposed into simpler abelian varieties. Moreover, our curve embeds into the Jacobian, and thus if we can impose conditions such that the Jacobian splits into a product of the same elliptic curve we will obtain multiple maps from our curve C to the same abelian variety.

As one can imagine, it is difficult in practice to know whether the curve you are dealing with has multiple maps to the same elliptic curve, which makes this method not commonly used in the literature. Indeed, the few successful attempts of using this method have been made through imposing conditions on the curve so that it

naturally has maps to elliptic curves or its Jacobian splits. Moreover, if one looks at a "random" curve with multiple independent maps to the same elliptic curve then the images of a point $P \in C$ by these maps are usually independent, invalidating the hypothesis. In the next section we show the construction of our family of hyperelliptic curves who have 2 maps to the same elliptic curve, then we only need to restrict the rank of the elliptic curve to be exactly equal to 1, so that we also avoid the method of Chabauty-Coleman. Our construction is most similar to the one exhibited in [11].

3.2 Simplification in Rank 1

We now describe how this method simplifies when $\text{Rank}(A) = 1$ since this is the situation we will be in. Suppose we have two morphisms, say $f_1, f_2 : C \to A$ where $\text{Rank}(A) = 1$. Let $P \in C(K)$, then

$$\begin{cases} f_1(P) = [n]R + T_1 \\ f_2(P) = [m]R + T_2 \end{cases}$$

where R is the generator of the free part of A and $T_i \in A(K)_{\text{tor}}$. Taking canonical heights we have

$$\begin{cases} \hat{h}(f_1(P)) = n^2\hat{h}(R) \\ \hat{h}(f_2(P)) = m^2\hat{h}(R). \end{cases}$$

Subtracting second equation from the first and taking absolute values gives us that following relation:

$$\left|\hat{h}(f_1(P)) - \hat{h}(f_2(P))\right| = \left|n^2\hat{h}(R) - m^2\hat{h}(R)\right| = \left|n^2 - m^2\right| \hat{h}(R).$$

If it happens to be the case that $n = \pm m$, then that would imply that $f_1(P) \pm f_2(P) \in A(K)_{\text{tor}}$, and so we could find those points directly through computation since the

torsion group is finite. Note also that we can bound this quantity from above using the triangle inequality. Indeed,

$$\left|\hat{h}(f_1(P)) - \hat{h}(f_2(P))\right| \leq \left|\hat{h}(f_1(P)) - h(f_1(P))\right| + \left|\hat{h}(f_2(P)) - h(f_2(P))\right| + \left|h(f_1(P)) - h(f_2(P))\right|.$$

Thus, if $n \neq \pm m$, then combining these two expressions we can obtain an upper bound, say B, such that $|n^2 - m^2| < B$. It is important to note here that the constant B would only depend on f_1, f_2, and A, but would be independent of P. In this way, we bound the possible values of n and m, and so all that would be left to do would be to find the possible points on $C(K)$ whose images on $A(K)$ are of the form $nR + T_i$ with $n < B$. Again, this is a finite computation that can be done fairly quickly on Magma. Thus, we have effectively found all the K-rational points on C.

Chapter 4

Family of Genus 3 Curves

In this chapter we will describe the construction of the curves in our family and see how some elliptic curves arise from that construction. In order to avoid the method of Chabauty-Coleman, we will then need to also consider some restrictions on these elliptic curves in order to control their ranks.

4.1 Construction of C_a

We now begin describing how we obtain the family of genus 3 hyperelliptic curves and the maps to the same abelian variety. Consider the quartic $g(x) = x^4 - a^2x^2 + 1$. Notice that we can pick two distinct non-zero points $z \neq w$ such that $g(z) = g(w)$. In this way we obtain

$$\begin{aligned} z^4 - a^2z^2 + 1 &= w^4 - a^2w^2 + 1 \\ z^4 - w^4 &= a^2(z^2 - w^2) \\ z^2 + w^2 &= a^2, \end{aligned}$$

but this last equation is a circle of radius a in z and w. As usual, we can parameterize rational points on this circle by considering the line $w = zx + a$, as long as $a \neq 0$. In

doing so we have

$$\begin{aligned} z^2 + (zx + a)^2 &= a^2 \\ z^2 + z^2x^2 + 2zxa + a^2 &= a^2 \\ z^2(1 + x^2) &= -2zxa \\ z &= -\frac{2xa}{x^2 + 1}. \end{aligned}$$

Thus, we obtain the parameterization of rational points on the circle given by $(z(x), w(x)) = \left(-\frac{2ax}{x^2+1}, -\frac{a(x+1)(x-1)}{x^2+1}\right)$ for any $x \in \mathbb{Q}$. Now, we take the function $z(x) = -\frac{2ax}{x^2+1}$ and plug it into our quartic $f(x)$. Indeed,

$$g(z(x)) = \left(-\frac{2ax}{x^2+1}\right)^4 - a^2\left(-\frac{2ax}{x^2+1}\right)^2 + 1,$$

which after multiplying the entire equation by $(x^2+1)^4$ to clear denominators simplifies to

$$g(z(x))(x^2+1)^4 = x^8 + (4 - 4a^4)x^6 + (8a^4 + 6)x^4 + (4 - 4a^4)x^2 + 1.$$

The right side of the above equation will define the $f(x)$ for our hyperelliptic curve. Concretely, our family of hyperelliptic curves will be defined as:

$$C_a : y^2 = x^8 + (4 - 4a^4)x^6 + (8a^4 + 6)x^4 + (4 - 4a^4)x^2 + 1,$$

which since $f(x)$ is degree 8, we can deduce that for every value of a, we obtain a genus 3 hyperelliptic curve. Also note that this construction arose from the first quartic $g(x) = x^4 - a^2x^2 + 1$, and if we define the curve $H_a : y^2 = x^4 - a^2x^2 + 1$, this is a genus 1 hyperelliptic curve. This implies that H_a is in fact an elliptic curve and Magma can give us the Weierstrass equation and the map between the curves. In fact, we have

that

$$\begin{aligned} H_a : y^2 = x^4 - a^2x^2 + 1 &\cong E_a : y^2 = x^3 + 2a^2x^2 + (a^4 - 4)x \\ (x, y) &\mapsto (2x^2 - 2y - 1, 4x^3 - 4xy - 2x). \end{aligned}$$

In this way we have successfully constructed a curve with multiple maps to the same elliptic curve, lending itself nicely to the method of Dem'yanenko-Manin. We can in fact be very concrete and display the maps we obtain. Firstly, we obtain the maps

$$\begin{aligned} \psi_1 : C_a &\to H_a \\ (x, y) &\mapsto \left(z(x), \frac{y}{(x^2+1)^2}\right) \\ \psi_2 : C_a &\to H_a \\ (x, y) &\mapsto \left(w(x), \frac{y}{(x^2+1)^2}\right) \end{aligned}$$

and composing ψ_1, ψ_2 with the isomorphism between H_a and E_a above, we have two maps from C_a to E_a. From here on out, we will denote by the composition of these maps φ_1 and φ_2.

Lemma 4.1.1. The maps $\varphi_1, \varphi_2 : C_a \to E_a$ are independent.

Proof. The maps φ_1 and φ_2 in projective coordinates are given explicitly by

$$\begin{aligned} \varphi_1 = [&-a^2x^6 + 5a^2x^4z^2 - 2x^2y + 5a^2x^2z^4 - 2yz^2 - a^2z^6, \\ &4a^3x^5z - 24a^3x^3z^3 + 8axyz + 4a^3xz^5, \\ &x^6 + 3x^4z^2 + 3x^2z^4 + z^6] \\ \varphi_2 = [&a^2x^6 - 5a^2x^4z^2 - 2x^2y - 5a^2x^2z^4 - 2yz^2 + a^2z^6, \\ &-2a^3x^6 + 14a^3x^4z^2 + 4ax^2y - 14a^3x^2z^4 - 4ayz^2 + 2a^3z^6, \\ &x^6 + 3x^4z^2 + 3x^2z^4 + z^6]. \end{aligned}$$

The codomain of these maps is an elliptic curve so when we consider $\varphi_1 + \varphi_2$ we need to remember that the addition is defined as on an elliptic curve. Luckily for us we do not have to do the calculation by hand as it is a quick calculation on Magma that $\deg(\varphi_1) = \deg(\varphi_2) = 2$, and that $\deg(\varphi_1 + \varphi_2) = 4$. Thus, we obtain the matrix

$$M = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

and we can clearly see that $\det(M) \neq 0$ and thus by 3.1.1 the maps are independent. □

Now, maps between curves induce maps on their Jacobians so in particular we have maps from $J(C_a) \to J(E_a) \cong E_a$. More importantly, these maps will be surjective and have finite kernel, so they will be isogenies. This means that $J(C_a)$ has two factors of E_a in its isogeny decomposition. We also know that C_a has genus 3, and $\dim J(C_a) = 3$, hence the isogeny decomposition of $J(C_a)$ is $E_a \times E_a \times E'$ where E' is some other elliptic curve. For our purposes, it will be useful to know an equation for E' since we will want to ensure it has nonzero rank so that we avoid Chabauty-Coleman. It turns out that we can find an equation for E' by quotienting C_a by one of its automorphisms and searching for an elliptic curve which is non-isogenous to E_a. This a finite search that can be done on Magma and we obtain

$$E' : y^2 = x^3 + (-4 - a^4)x^2 + 4a^4x.$$

We are now in the position where we have a family of genus 3 hyperelliptic curves whose Jacobian decomposes in a way favorable to the use of Dem'yanenko-Manin. We summarize the above discussion in the following result.

Theorem 4.1.2. Let C_a be the genus 3 hyperelliptic curve

$$C_a : y^2 = x^8 + (4 - 4a^4)x^6 + (8a^4 + 6)x^4 + (4 - 4a^4)x^2 + 1.$$

Then, $J(C_a)$ $E_a \times E_a \times E'$.

At this point we now need to find conditions on the parameter a so that $\text{Rank}(E_a) = 1$ (since we have two independent maps φ_1, φ_2) and $\text{Rank}(E') \neq 0$.

4.2 Controlling the Ranks of E_a and E'

The focus of this section will be to demonstrate sufficient conditions to restrict the ranks of E_a and E'. The main tool to do this will be the Parity conjecture. Before stating the conjecture we define global root numbers and discuss how we compute them in practice. All throughout this section we consider an elliptic curve E over a number field K.

Definition 12. The global root number $w(E/K)$ of an elliptic curve over K is defined as the product of the local root numbers $w(E/K_v) \in \{-1, 1\}$. In particular,

$$w(E/K) = \prod_v w(E/K_v),$$

where the product runs over all places of K, including the infinite ones.

Local root numbers of elliptic curves are defined using epsilon-factors of Weil-Deligne representations, however, for our purposes we will not need to introduce formal definitions and we instead direct the interested reader to [14] for formal definitions. They have been classified for all places of number fields, so we will not concern ourselves with proving any results, but instead use them for our computations. For instance, we make use of the following result from [10]. We remark that the result has more cases, and we have only included the ones relevant to our purposes.

Theorem 4.2.1. Let E be an elliptic curve over a local field $\mathcal{K}$ of characteristic zero. When $\mathcal{K}$ is non-Archimedean, let k be its residue field and let $v : \mathcal{K}^\times \to \mathbb{Z}$ denote

the normalized valuation with respect to $\mathcal{K}$. Let $\left(\frac{*}{k}\right)$ denote the quadratic residue symbol on $k^\times$ and $(a,b)_\mathcal{K}$ denote the Hilbert symbol in $\mathcal{K}$.

1. If $\mathcal{K}$ is Archimedean, then $w(E/\mathcal{K}) = -1$.

2. If $E/\mathcal{K}$ has good reduction, then $w(E/\mathcal{K}) = 1$.

3. If $E/\mathcal{K}$ has split multiplicative reduction, then $w(E/\mathcal{K}) = -1$.

4. If $E/\mathcal{K}$ has non-split multiplicative reduction, then $w(E/\mathcal{K}) = 1$.

5. If $E/\mathcal{K}$ has additive, potentially multiplicative reduction and $\mathrm{char}(k) = 2$, then $w(E/\mathcal{K}) = (-1, -c_6)_\mathcal{K}$. In particular, if $\mathcal{K} = \mathbb{Q}_2$, then

$$w(E/\mathbb{Q}_2) = \begin{cases} -1 & \text{if } c_6' \equiv 1(\bmod 4) \\ +1 & \text{if } c_6' \equiv 3(\bmod 4) \end{cases}$$

   where $c_6' = \dfrac{c_6}{2^{v(c_6)}}$.

In particular, this result tells us that to determine local root numbers, we only need to determine the reduction type of our elliptic curve at its various primes. Now, over $\mathbb{Q}$, the places are precisely the primes, and the usual infinite place. It is a known fact that the only places where our elliptic curve may have bad reduction is at the primes which divide the discriminant and so we only need to consider those primes, since the primes of good reduction have local root number 1, and as such will not change the parity of the global root number. We now state the Parity Conjecture, which is known to be true in certain cases and helps predict the existence of points of infinite order on elliptic curves.

Conjecture 1 (Parity Conjecture)**.** Let E/K be an elliptic curve over a number field. Then

$$(-1)^{\mathrm{Rank}(E)} = w(E/K)$$

where $w(E/K)$ is the global root number of E.

For our purposes, we will want to show that the global root number of E_a is 1, so that we can conclude (conjecturally), that its rank is odd. I should also note that we actually want its rank to be exactly 1, since we have two morphisms to E_a, but we are only able to prove that the rank is odd. However, results by Bhargava and Shankar [2] show that, when ordered by height, about 50% of elliptic curves over $\mathbb{Q}$ have rank 0 and the other 50% have rank 1. In particular, we note that we have not been able to find a value of a which satisfies the conditions we prescribe such that $\text{Rank}(E_a) \geq 3$. Additionally, as we have been reiterating, to avoid Chabuaty-Coleman, we will also impose conditions so that $w(E'/\mathbb{Q}) = 1$, implying that the rank is non-zero. We are now ready to state and prove our results about the ranks of E_a and E'.

Theorem 4.2.2. Let $a \in \mathbb{Z}$ such that $a^2 - 2$ and $a^2 + 2$ are both prime. Then, $\text{Rank}(E_a)$ is odd.

Proof. Per our previous discussion, we only need to determine the local root numbers at the primes of bad reduction, which are the primes dividing the discriminant. Note that $\Delta(E_a) = 2^8(a^2-2)^2(a^2+2)^2$. Thus, we will only consider the cases where $p \in \{2, a^2-2, a^2+2\}$.

First consider $p = 2$. Note that $c_4 = 16a^4 + 192$ and $c_6 = 64a^6 - 2304a^2$ and thus we have that $v_2(c_4) = 4$, $v_2(c_6) = 6$ and $v_2(\Delta) = 8$. Looking at Table 1 in [8] and noting that $2c_6' + c_4' \equiv 11 \bmod 16$ tells us that $w_2(E_a) = -1$. We remark that we've used here the fact that a must be odd. Indeed, if a were even then $a^2 - 2$ and $a^2 + 2$ are not prime.

Now consider $p = a^2 - 2$. Reducing the equation of E_a modulo p gives us

$$y^2 \equiv 2a^2x^2 + x^3 \bmod p.$$

This is a nodal curve, so we have multiplicative reduction. Also, the Legendre symbol

$\left(\frac{2a^2}{p}\right)$ determines whether it is of non-split or split type. We have

$$\begin{aligned}
\left(\frac{2a^2}{p}\right) &= \left(\frac{2}{p}\right)\left(\frac{a^2}{p}\right) \\
&= \left(\frac{2}{p}\right) \quad \text{since } p \nmid a^2 \\
&= \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases} \\
&= \begin{cases} 1 & \text{if } a^2 \equiv 1, 3 \bmod 8 \\ -1 & \text{if } a^2 \equiv 5, 7 \bmod 8 \end{cases}
\end{aligned}$$

and since a is odd, it always the case that $a^2 \equiv 1 \bmod 8$. Hence, in our situation $\left(\frac{2a^2}{p}\right) = 1$, and thus E_a has split multiplicative reduction at $p = a^2 - 2$. By 4.2.1 we have that $w_p(E_a) = -1$.

Finally, consider $p = a^2 + 2$. Reducing E_a modulo p gives

$$y^2 \equiv 2a^2x^2 + x^3 \bmod p.$$

We again have multiplicative reduction and $\left(\frac{2a^2}{p}\right)$ determines the type.

$$\begin{aligned}
\left(\frac{2a^2}{p}\right) &= \left(\frac{2}{p}\right)\left(\frac{a^2}{p}\right) \\
&= \left(\frac{2}{p}\right) \quad \text{since } p \nmid a^2 \\
&= \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases} \\
&= \begin{cases} 1 & \text{if } a^2 \equiv 5, 7 \bmod 8 \\ -1 & \text{if } a^2 \equiv 1, 3 \bmod 8. \end{cases}
\end{aligned}$$

Since a is odd, it is always the case that $a^2 \equiv 1 \bmod 8$, and so $\left(\frac{2a^2}{p}\right) = -1$. Thus, E_a has non-split multiplicative reduction at $p = a^2 + 2$. Hence, by 4.2.1 we have $w_p(E_a) = 1$.

Putting it all together we now have that the global root number of E_a over $\mathbb{Q}$ is $w(E_a/\mathbb{Q}) = (-1)(-1)(-1)(1) = -1$, which would imply that the rank of E_a is odd by the Parity Conjecture. □

Under these conditions we have an infinite family of elliptic curves E_a whose rank is odd. We should also note that we've checked all values of a which satisfy the hypothesis and are $\leq 2,000,000$ and have not been able to find such an a with $\text{Rank}(E_a) \neq 1$.

Conjecture 2. There are infinitely many $a \in \mathbb{Z}$ such that $a^2 - 2$ and $a^2 + 2$ are simultaneously prime.

Although we do not prove the above conjecture, we note that this is very similar to the Twin Prime Conjecture, which is widely accepted by the mathematical community. We now do a similar analysis for E', but note that its discriminant is $\Delta(E') = 2^8a^8(a^2 - 2)^2(a^2 + 2)^2$, which complicates things because $a, a^2 - 2$, and $a^2 + 2$ are simultaneously prime only once, exactly when $a = 3$. In general, one of a or $a^2 + 2$ will be divisible by 3 so we will make from now on the assumption that a is divisible by 3. Thus, we will need to do an analysis of E' at the primes $2, 3$, $q, a^2 - 2$, and $a^2 + 2$ for q a prime bigger than 3. We will see in our next result that we will need another condition on q, in particular, we will need $q \equiv 3 \bmod 4$.

Theorem 4.2.3. Let $a = 3q$, with q prime, $q \equiv 3 \bmod 4$ and $a^2 - 2$, $a^2 + 2$ are both prime. Then, $\text{Rank}(E')$ is odd.

Proof. We proceed as we did with E_a. We have $\Delta(E') = 2^8a^8(a^2 - 2)^2(a^2 + 2)^2$ and so we need to find the reduction type at the following primes $p \in \{2, 3, q, a^2 - 2, a^2 + 2\}$. First consider $p = 2$. Using Theorem 3.7 from [1] and noting that in their notation,

$E' = E_{C_2\times C_2}(-4,-a^4,1) = E_{C_2\times C_2}(a,b,d)$. We have $v_2(a) = 2$, and $bd \equiv 3 \bmod 4$ and thus the reduction type is I_0^*. Since we have additive, potentially multiplicative reduction and $c_6' \equiv 3 \bmod 4$, 4.2.1 tells us that $w_2(E') = 1$. We should note that by Theorem 3.7 in [1], we know that $p = 2$ is the only prime at which we have additive reduction, and thus for the rest of the primes we only need to check whether the reduction type is split or non-split.

Consider now $p = 3$. Reducing E' modulo p gives

$$y^2 \equiv x^3 + 2x^2 \bmod p,$$

and since $\left(\frac{2}{3}\right) = -1$, we have non-split multiplicative reduction. Hence, by 4.2.1 $w_3(E') = 1$.

Consider now $p = q$. Reducing E' modulo p gives

$$y^2 \equiv x^3 - 4x^2 \bmod p,$$

so $\left(\frac{-4}{q}\right)$ will determine the type. Note that

$$\begin{aligned}\left(\frac{-4}{q}\right) &= \left(\frac{-1}{q}\right)\left(\frac{4}{q}\right)\\ &= \left(\frac{-1}{q}\right) \text{ since } q \nmid 4\\ &= -1 \text{ if } q \equiv 3 \bmod 4.\end{aligned}$$

Thus, by 4.2.1, $w_q(E') = 1$.

At the primes $a^2 - 2$ and $a^2 + 2$ we can verify via Magma that the reduction types are split and so at the last two places needed we have $w_p(E') = -1$.

Putting this all together we have $w(E'/\mathbb{Q}) = (-1)(1)(1)(1)(-1)(-1) = -1$, which implies that the rank is odd by the Parity Conjecture. $\square$

Conjecture 3. There are infinitely many $3q$, with $q > 3$ and $q \equiv 3 \bmod 4$ such that $9q^2 - 2$ and $9q^2 + 2$ are simultaneously prime.

We again note that we do not know how to prove such a conjecture, but there is enough evidence to believe its validity. We have now managed to (conjecturally) provide an infinite set of curves such that we can find the rational points via Dem'yanenko-Manin while avoiding Chabauty-Coleman. In the next chapter, we describe the height restrictions on the rational points on C_a and explicitly find $C_a(\mathbb{Q})$.

Chapter 5

Height Bounds

In order to find the rational points on C_a via Dem'yanenko-Manin, we first needed to find conditions so that our family of curves satisfies the hypothesis. Having done that, we now work with φ_1 and φ_2, in order to obtain bounds on the canonical height of the possible rational points on C_a. Recall from our discussion in 3.2 that we have the following inequality in terms of the canonical heights:

$$\left|\hat{h}(f_1(P)) - \hat{h}(f_2(P))\right| \leq \left|\hat{h}(f_1(P)) - h(f_1(P))\right| + \left|\hat{h}(f_2(P)) - h(f_2(P))\right| + \left|h(f_1(P)) - h(f_2(P))\right|.$$

The aim of this chapter will be to bound the last term on the right-hand side of the inequality since the first two can be bounded via Magma by the command

```
SilvermanBound();
```

which takes as input an elliptic curve. Once we have accomplished that, we will be ready to effectively find rational points on a certain set of curves from our family C_a.

5.1 Bounding the Difference in Naive Heights

Recall that we have explicit maps φ_1 and φ_2 and if we are concerned with bounding the quantity

$$\Big|h(\varphi_1(P)) - h(\varphi_2(P))\Big|,$$

then we should attempt to get a better understanding of what equations define $\varphi_1(P)$ and $\varphi_2(P)$ and calculate bounds for their naive height. Recall also that the naive height of a point on an elliptic curve was simply defined as the height of the x-coordinate of the image of the point and so we are really only concerned with the x-coordinate of these images. In affine coordinates we have

$$\begin{aligned} x(\varphi_1(P)) &= \frac{-a^2x^4 + 6a^2x^2 - 2y - a^2}{x^4 + 2x^2 + 1} \\ x(\varphi_2(P)) &= \frac{a^2x^4 - 6a^2x^2 - 2y + a^2}{x^4 + 2x^2 + 1}. \end{aligned}$$

We run into an issue here that both numerators in these maps depend on the y-coordinate of the point P which means that we will need to use the defining equation of our curve to get the terms purely in terms of x. This step is essential for determining lower bounds of the heights of $\varphi_1(P)$ and $\varphi_2(P)$.

Recall that the defining equation for our family of hyperelliptic curves is:

$$\begin{aligned} y^2 &= x^8 + (4 - 4a^4)x^6 + (8a^4 + 6)x^4 + (4 - 4a^4)x^2 + 1 \\ y &= \sqrt{x^8 + (4 - 4a^4)x^6 + (8a^4 + 6)x^4 + (4 - 4a^4)x^2 + 1}. \end{aligned}$$

Note that $4 - 4a^4$ is negative for all values of $a > 1$ and so, in particular these terms will only decrease the value and so by ignoring them we "maximize" how large the

y-coordinate could be. Indeed, we have

$$y' = \sqrt{x^8 + (8a^4 + 6)x^4 + 1} \geq y.$$

Moreover, we can further maximize y' with the following inequality:

$$\begin{aligned} \sqrt{x^8 + (8a^4 + 6)x^4 + 1} &\leq \sqrt{x^8} + \sqrt{(8a^4 + 6)x^4} + 1 \\ &\leq x^4 + (3a^2 + 3)x^4 + 1 = y''. \end{aligned}$$

We arrive at the ladder of inequalities $y'' \geq y' \geq y$, and this is how we will minimize the numerator of both the images of φ_1 and φ_2. In particular, replacing y with y'' in $x(\varphi_1(P))$ and $x(\varphi_2(P))$ we have:

$$\begin{aligned} x(\varphi_1(P)) &= \frac{-a^2x^4 + 6a^2x^2 - 2y - a^2}{x^4 + 2x^2 + 1} \\ &\geq \frac{(-2 - a^2)x^4 - 6x^2 + (-2 - a^2)}{x^4 + 2x^2 + 1} \\ x(\varphi_2(P)) &= \frac{a^2x^4 - 6a^2x^2 - 2y + a^2}{x^4 + 2x^2 + 1} \\ &\geq \frac{(a^2 - 2)x^4 + (-12a^2 - 6)x^2 + (a^2 - 2)}{x^4 + 2x^2 + 1}. \end{aligned}$$

It will be convenient for us to define the following homogeneous polynomials

$$\begin{aligned} F_1(X, Z) &= (-2 - a^2)X^4 - 6X^2Z^2 + (-2 - a^2)Z^4 \\ G_1(X, Z) &= X^4 + 2X^2Z^2 + Z^4 \\ F_2(X, Z) &= (a^2 - 2)X^4 + (-12a^2 - 6)X^2Z^2 + (a^2 - 2)Z^4 \\ G_2(X, Z) &= X^4 + 2X^2Z^2 + Z^4. \end{aligned}$$

Note that $F_1(X,1)$ and $G_1(X,1)$ are simply the numerator and denominator for the lower bound of $x(\varphi_1(P))$ and that they are relatively prime in $\mathbb{Q}[X]$, so they generate the unit ideal in $\mathbb{Q}[X]$. This implies that we have the following result.

Lemma 5.1.1. Define the polynomials

$$\begin{aligned}
F_1(X,Z) &= (-2-a^2)X^4 - 6X^2Z^2 + (-2-a^2)Z^4 \\
G_1(X,Z) &= X^4 + 2X^2Z^2 + Z^4 \\
f_1(X,Z) &= -\frac{1}{2(a^2-1)}X^2Z^2 - \frac{1}{a^2-1}Z^4 \\
g_1(X,Z) &= -\frac{\frac{1}{2}a^2+1}{a^2-1}X^2Z^2 - \frac{3}{a^2-1}Z^4 \\
f_2(X,Z) &= -\frac{1}{2(a^2-1)}X^2Z^2 - \frac{1}{a^2-1}X^4 \\
g_2(X,Z) &= -\frac{\frac{1}{2}a^2+1}{a^2-1}X^2Z^2 - \frac{3}{a^2-1}X^4.
\end{aligned}$$

Then the following identities hold:

$$\begin{aligned}
F_1(X,Z)f_1(X,Z) + G_1(X,Z)g_1(X,Z) &= Z^8 \\
F_1(X,Z)f_2(X,Z) + G_1(X,Z)g_2(X,Z) &= X^8.
\end{aligned}$$

Proof. The existence of such identities is due to the fact that $F_1(X,Z)$ and $G_1(X,Z)$ are relatively prime homogeneous polynomials. The validity of the identities is a tedious calculation but can verified through computer algebra systems such as Magma [3], for instance. □

Remark 2. Our inequalities which"removed" the y-coordinate from the images of $\varphi_1(P)$ and $\varphi_2(P)$ made it so that we had relatively prime $F_1(X,1)$ and $G_1(X,1)$, which was a necessary step to find our identities.

We state our similar result for $F_2(X,Z)$ and $G_2(X,Z)$.

Lemma 5.1.2. Define the polynomials

$$\begin{aligned}
F_2(X,Z) &= (a^2-2)X^4 + (-12a^2-6)X^2Z^2 + (a^2-2)Z^4 \\
G_2(X,Z) &= X^4 + 2X^2Z^2 + Z^4 \\
h_1(X,Z) &= \frac{1}{14a^2+2}X^2Z^2 + \frac{1}{7a^2+1}Z^4 \\
i_1(X,Z) &= -\frac{\frac{1}{14}a^2-\frac{1}{7}}{a^2+\frac{1}{7}}X^2Z^2 + \frac{\frac{6}{7}a^2+\frac{3}{7}}{a^2+\frac{1}{7}}Z^4 \\
h_2(X,Z) &= \frac{1}{14a^2+2}X^2Z^2 + \frac{1}{7a^2+1}X^4 \\
i_2(X,Z) &= -\frac{\frac{1}{14}a^2-\frac{1}{7}}{a^2+\frac{1}{7}}X^2Z^2 + \frac{\frac{6}{7}a^2+\frac{3}{7}}{a^2+\frac{1}{7}}X^4.
\end{aligned}$$

Then the following identities hold:

$$\begin{aligned}
F_2(X,Z)h_1(X,Z) + G_2(X,Z)i_1(X,Z) &= Z^8 \\
F_2(X,Z)h_2(X,Z) + G_2(X,Z)i_2(X,Z) &= X^8.
\end{aligned}$$

Proof. This again relies on the fact that $F_2(X,1)$ and $G_2(X,1)$ are relatively prime and a tedious calculation. □

The polynomials $f_1, f_2, g_1, g_2, h_1, h_2, i_1$ and i_2 were all found through the help of Magma [3] using the Euclidean algorithm for polynomials.

If we write $x = x(P) = \frac{a}{b}$ in lowest terms then we can write $x(\varphi_1(P)) = \frac{F_1(a,b)}{G_1(a,b)}$ and $x(\varphi_2(P)) = \frac{F_2(a,b)}{G_2(a,b)}$ as quotients of integers. We can restate the identities for our our lemmas using this notation. For 5.1.1, we have

$$\begin{aligned}
F_1(a,b)f_1(a,b) + G_1(a,b)g_1(a,b) &= b^8 \\
F_1(a,b)f_2(a,b) + G_1(a,b)g_2(a,b) &= a^8.
\end{aligned}$$

This implies that we have

$$\begin{aligned} |b^8| &\leq 2\max\{|f_1(a,b)|, |g_1(a,b)|\}\max\{|F_1(a,b)|, |G_1(a,b)\} \\ |a^8| &\leq 2\max\{|f_2(a,b)|, |g_2(a,b)|\}\max\{|F_1(a,b)|, |G_1(a,b)\}. \end{aligned}$$

Now looking at the expressions of f_1, f_2, g_1, and g_2, we have the following inequality:

$$\max\{|f_1|, |f_2|, |g_1|, |g_2|\} \leq 2\max\{|a|^4, |b|^4\}.$$

Thus, we can combine the above inequalities to obtain the following lower bound on the height of $\varphi_1(P)$:

$$\begin{aligned} \max\{|a^8|, |b^8|\} &\leq 4\max\{|a|^4, |b|^4\}\max\{|F_1|, |G_1|\} \\ \frac{\max\{|a|^4, |b|^4\}}{4} &\leq \max\{|F_1|, |G_1|\} \\ \frac{1}{4}H(P)^4 &\leq H(\varphi_1(P)) \\ \log\left(\frac{1}{4}\right) + 4h(P) &\leq h(\varphi_1(P)). \end{aligned}$$

We can do the exact same argument for the identities in 5.1.2 and obtain

$$\log\left(\frac{1}{4}\right) + 4h(P) \leq h(\varphi_2(P)).$$

Now to obtain the upper bounds for the heights we use x-coordinate of the affine maps for φ_1 and φ_2 which we recall here:

$$\begin{aligned} x(\varphi_1(P)) &= \frac{-a^2x^4 + 6a^2x^2 - 2y - a^2}{x^4 + 2x^2 + 1} \\ x(\varphi_2(P)) &= \frac{a^2x^4 - 6a^2x^2 - 2y + a^2}{x^4 + 2x^2 + 1}. \end{aligned}$$

The first way to obtain an "easy" upper bound is to simply ignore all the terms which may decrease the numerator, that it all terms which are negative. We thus obtain,

$$\begin{aligned} x(\varphi_1(P)) &= \frac{-a^2x^4 + 6a^2x^2 - 2y - a^2}{x^4 + 2x^2 + 1} \\ &\leq \frac{6a^2x^2}{x^4 + 2x^2 + 1} \end{aligned}$$

$$\begin{aligned} x(\varphi_2(P)) &= \frac{a^2x^4 - 6a^2x^2 - 2y + a^2}{x^4 + 2x^2 + 1} \\ &\leq \frac{a^2x^4 + a^2}{x^4 + 2x^2 + 1}. \end{aligned}$$

If we let $x = x(P) = \frac{r}{s}$ as before, we can rewrite these as:

$$x(\varphi_1(P)) \leq \frac{6a^2r^2s^2}{r^4 + 2r^2s^2 + s^4}$$

$$x(\varphi_2(P)) \leq \frac{a^2r^4 + s^4a^2}{r^4 + 2r^2s^2 + s^4}.$$

Now, since the height is simply the max between the numerator and the denominator we only need to determine which of the two is largest. In other words, we have:

$$\begin{aligned} H(\varphi_1(P)) &\leq \max\{6a^2H(P)^4, 4H(P)^4\} \\ h(\varphi_1(P)) &\leq \log(6) + 2\log(a) + 4h(P) \end{aligned}$$

and

$$\begin{aligned} H(\varphi_2(P)) &\leq \max\{2a^2H(P)^4, 4H(P)^4\} \\ h(\varphi_2(P)) &\leq \log(2) + 2\log(a) + 4h(P). \end{aligned}$$

We summarize the bounds we have discussed above in the following lemma.

Lemma 5.1.3. For $P \in C_a(\mathbb{Q})$, we have:

$$\log\left(\frac{1}{4}\right) + 4h(P) \leq h(\varphi_1(P)) \leq \log(6) + 2\log(a) + 4h(P)$$
$$\log\left(\frac{1}{4}\right) + 4h(P) \leq h(\varphi_2(P)) \leq \log(2) + 2\log(a) + 4h(P).$$

Combining the inequalities from 5.1.3, we obtain the inequality following inequality:

$$|h(\varphi_1(P)) - h(\varphi_2(P))| \leq \log(6) + 2\log(a) - \log\left(\frac{1}{4}\right). \tag{5.1}$$

We also have the following lemma regarding the difference between the canonical height and naive height on our elliptic curve E_a.

Lemma 5.1.4. Let $P \in E_a(\mathbb{Q})$. Then we have:

$$\left|\hat{h}_{E_a}(P) - h_{E_a}(P)\right| \leq 24.$$

Proof. As mentioned earlier, this can be computed on Magma via the command

```
SilvermanBound(E_a);
```

We should also mention that this bound can be improved using the command

```
SiksekBound(E_a);
```

□

We have finally arrived at the point where we can state our main theorem of this section concerning the difference of canonical heights on E_a.

Theorem 5.1.5. Let $P \in C_a(\mathbb{Q})$. Then we have

$$\left|\hat{h}_{E_a}(\varphi_1(P)) - \hat{h}_{E_a}(\varphi_2(P))\right| \leq 51.18 + 2\log(a).$$

Proof. This is a combination of the inequalities (5.1) and 5.1.4 used in 5 we discussed at the beginning of this chapter. □

We are now in the position to demonstrate an example of how we find rational points on a curve in our family.

Example 1. Let $a = 3$. Note that this value does not satisfy the conditions stipulated in Conjecture 3 but we remark that those conditions are sufficient, not necessary in order to find examples where we can use Dem'yanenko-Manin, while avoiding Chabauty-Coleman. By Theorem 5.1.5, we have that

$$\left|\hat{h}_{E_3}(\varphi_1(P)) - \hat{h}_{E_3}(\varphi_2(P))\right| \leq 52.13.$$

Also, since $a = 3$, we have

$$E_3 : y^2 = x^3 + 18x^2 + 77x$$

and using Magma we can find a generator for its free part, say R. We find $\hat{h}(R) = 0.922$. This implies that

$$\left|n^2 - m^2\right| \leq 57.88 \Rightarrow \max\{|n|, |m|\} \leq \frac{1}{2}(57.88 + 1) < 29.$$

Now all that is left to do is perform a search for either:

- $P \in C_3(\mathbb{Q})$ such that $\varphi_1(P) \pm \varphi_2(P) \in E_3(\mathbb{Q})_{\text{tor}}$
- $P \in C_3(\mathbb{Q})$ such that $\varphi_1(P) = nR + T$ or $\varphi_2(P) = nR + T$ with $T \in E_3(\mathbb{Q})_{\text{tor}}$ and $|n| \leq 28$.

Both of these are finite computations which can be carried out easily on Magma so we find:

$$C_3(\mathbb{Q}) = \{(\pm 1 : \pm 4 : 1), (0 : \pm 1 : 1), (1 : \pm 1 : 0)\}.$$

Bibliography

[1] Alexander J. Barrios and Manami Roy. Local data of rational elliptic curves with nontrivial torsion. *Pacific Journal of Mathematics*, 318(1):1–42, August 2022. ISSN 0030-8730. doi: 10.2140/pjm.2022.318.1. URL `http://dx.doi.org/10.2140/pjm.2022.318.1`.

[2] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[4] JWS Cassels. On a theorem of dem'janenko. *Journal of the London Mathematical Society*, 1(1):61–66, 1968.

[5] Vadim Andreevich Dem'yanenko. Rational points of a class of algebraic curves. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 30(6):1373–1396, 1966.

[6] Gerd Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73:349–366, 1983.

[7] Martine Girard and Leopoldo Kulesz. Computation of sets of rational points of

genus-3 curves via the dem'janenko–manin method. *LMS Journal of Computation and Mathematics*, 8:267–300, 2005.

[8] Emmanuel Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 326(9):1047–1052, 1998. ISSN 0764-4442. doi: https://doi.org/10.1016/S0764-4442(98)80060-8. URL `https://www.sciencedirect.com/science/article/pii/S0764444298800608`.

[9] Marc Hindry and Joseph H Silverman. *Diophantine geometry: an introduction*, volume 201. Springer Science & Business Media, 2013.

[10] Lilybelle Cowland Kellock and Vladimir Dokchitser. Root numbers and parity phenomena, 2023. URL `https://arxiv.org/abs/2303.07883`.

[11] Leopoldo Kulesz. Application de la méthode de dem'janenko–manin à certaines familles de courbes de genre 2 et 3. *Journal of Number Theory*, 76(1):130–146, 1999.

[12] Ju I Manin. The p-torsion of elliptic curves is uniformly bounded. *Selected Papers Of Yu I Manin*, 3:185, 1969.

[13] Yuri Vladimirovich Matiyasevich. The diophantineness of enumerable sets. In *Doklady Akademii Nauk*, volume 191, pages 279–282. Russian Academy of Sciences, 1970.

[14] David E Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Mathematica*, 87(2):119–151, 1993.

[15] Matthias Schütt, Tetsuji Shioda, Matthias Schütt, and Tetsuji Shioda. Elliptic surfaces. *Mordell–Weil Lattices*, pages 79–114, 2019.

[16] Joseph H Silverman. Rational points on certain families of curves of genus at least 2. *Proceedings of the London Mathematical Society*, 3(3):465–481, 1987.

[17] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[18] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[19] Evelina Viada. An explicit manin-dem'janenko theorem in elliptic curves. *Canadian Journal of Mathematics*, 70(5):1173–1200, 2018.