

UC Irvine

UC Irvine Previously Published Works

Title

Rational points on a family of genus 3 hyperelliptic curves

Permalink

<https://escholarship.org/uc/item/9kr5b2m2>

Journal

Journal of Number Theory, 286

ISSN

0022-314X

Author

Hernandez, Roberto

Publication Date

2026-09-01

DOI

10.1016/j.jnt.2026.02.008

Copyright Information

This work is made available under the terms of a Creative Commons Attribution License, available at <https://creativecommons.org/licenses/by/4.0/>

Peer reviewed

Rational Points on a Family of Genus 3 Hyperelliptic Curves

Roberto Hernandez

Department of Mathematics, University of California, Irvine

Abstract

We compute the rational points on certain members of the following family of hyperelliptic curves

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

via the method first developed by Dem'yanenko [Dem68] and then further generalized by Manin [Man69]. In particular, we show that the method of Chabauty–Coleman, while applicable to certain members of this family, is not the most efficient way of computing $C_a(\mathbb{Q})$. We adapt the approach of [Kul99], incorporating root numbers to further restrict the possible ranks of the elliptic curves arising in the Jacobian decomposition.

Keywords: Elliptic curves, rational points, heights

1. Introduction

In 1983, Faltings' [Fal83] proved Mordell's Conjecture stating that any non-singular curve C defined over a number field of genus greater than one has finitely many rational points. Since then, there have been simplifications to his original argument, most notably done through the work of Bombieri [Bom90] and Vojta [Voj91]. While Faltings' theorem marked a milestone in arithmetic geometry, its limitation is that it does not 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. In practice, the most powerful tool for computing rational points on curves has been the Chabauty–Coleman method. In this work, we focus on the method developed by Dem'yanenko [Dem68] in 1968, extended by Manin [Man69] in 1969. We present an explicit family of curves

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

for which the method of Dem'yanenko–Manin proves particularly effective. In this setting, the method of Chabauty–Coleman does not generally apply in a useful way. In particular, the Jacobian of C_a is isogenous to a product of elliptic curves, written $\text{Jac}_{C_a} \sim E_a \times E_a \times E'$, and Chabauty–Coleman can only be applied in the special cases where $\text{Rank}(E_a) = 0$ or $\text{Rank}(E') = 0$. In those cases, however, the rational points on C_a can already be determined by pulling back the (finite) rational points on either E_a or E' . The more interesting case is where $\text{Rank}(E_a) = 1$ and $\text{Rank}(E') \neq 0$, because the conditions to apply Chabauty–Coleman are not met, and the Dem'yanenko–Manin method becomes essential. Concretely, we will show that

$$C_{237}(\mathbb{Q}) = \{(\pm 1 : \pm 4 : 1), (0 : \pm 1 : 1), (1 : \pm 1 : 0)\},$$

to showcase a particular instance of the method. We will also along the way prove certain facts about a family of elliptic curves which arise in our construction. In particular, we prove the following results about the Mordell–Weil group of the particular elliptic curve $E_a: y^2 = x^3 + 2a^2x^2 + (a^4 - 4)x$.

Proposition 1. *Suppose that $a \equiv 0 \pmod{3}$, then $E_a(\mathbb{Q})_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Theorem 4.1. *Suppose that $a^2 - 2$ and $a^2 + 2$ are simultaneously prime, then $\text{Rank}(E_a) = 1$.*

Email address: roberh5@uci.edu (Roberto Hernandez)

We recall that the method of Chabauty–Coleman uses p -adic techniques to produce p -adic locally analytic functions, and relies on the assumption that rank of the Jacobian of C over $\mathbb{Q}$, say r , is strictly smaller than the genus of C . In 1941, Chabauty [Cha41] proved that if the rank of the Jacobian is smaller than g , then the set $C(\mathbb{Q}_p) \cap \overline{\text{Jac}_C(\mathbb{Q})}$ is finite. Moreover, in 1985, Coleman [Col85] showed that if you also assume that you have a prime $p > 2g$ of good reduction, then you can place an upper bound on the number of rational points on C .

Theorem (Chabauty–Coleman). *Let C be a smooth, projective, geometrically integral curve over $\mathbb{Q}$ and let $r := \text{Rank Jac}_C(\mathbb{Q})$. If $r < g$ and $p > 2g$ is a prime of good reduction, then $C(\mathbb{Q}_p) \cap \overline{\text{Jac}_C(\mathbb{Q})}$ is finite and $\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2$.*

We highlight a family of curves for which we cannot apply this theorem because $\text{Rank}(\text{Jac}_{C_a}(\mathbb{Q})) \geq g$, but the method of Dem’yanenko–Manin gives a procedure to find $C_a(\mathbb{Q})$. For that, we will force the Jacobian of the curves to fully decompose, and then aim to restrict the ranks of the elliptic curves which appear in the decomposition.

Code

Throughout this project, we used the computer algebra system Magma [BCP97]. All calculations and claims can be found at the following GitHub repository:

<https://github.com/robertohernandez8/rational-points-genus-3-hyperelliptic-curves.git>

2. Background

First, we provide some relevant background material which can be found in more detail for instance in [HS13]. Everything we discuss in this article will be over $\mathbb{Q}$, unless stated otherwise.

An elliptic curve is an abelian variety of dimension one, equipped with a distinguished point denoted $\mathcal{O} = [0 : 1 : 0]$. It can be described concretely via its Weierstrass equation

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

Two important invariants of an elliptic curve are its discriminant, Δ , and the j -invariant. We recall some of the invariants associated to elliptic curves below.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j(E) &= \frac{c_4^3}{\Delta}. \end{aligned}$$

In particular, the j -invariant controls the isomorphism class of an elliptic curve over $\overline{\mathbb{Q}}$, while the discriminant helps detect primes of bad reduction. We also recall that a hyperelliptic curve over $\mathbb{Q}$ is a smooth, projective curve of genus $g \geq 2$ defined over $\mathbb{Q}$ which admits a degree 2 map to $\mathbb{P}^1$. Equivalently, over $\mathbb{Q}$, we can choose a model in affine coordinates of the form

$$C: y^2 = f(x),$$

where $f(x)$ is a monic polynomial of degree $2g + 1$ or $2g + 2$.

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

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

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 M_K be the set of absolute values on K . Let $P \in \mathbb{P}^n(K)$. The multiplicative height of P is the quantity

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}$$

and the logarithmic height is defined as

$$h_K(P) = \log H_K(P).$$

Theorem 2.1 ([HS13], Theorem B.2.5). Let X be a closed subvariety of $\mathbb{P}^n$ and let $\varphi: X \rightarrow \mathbb{P}^n$ be a morphism of degree d . Then

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

It is important to note here that the $O(1)$ depends only on the map φ , but it is independent of the point P .

Definition 2. Let $\varphi: V \rightarrow \mathbb{P}^n$ be a morphism. The height on V relative to φ is the function

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

where $h: \mathbb{P}^n(\overline{\mathbb{Q}}) \rightarrow [0, \infty)$ is the height function on projective space defined above.

In this way, we see that defining heights on varieties is very natural once you have an embedding of your variety into projective space. 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

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

Definition 3. 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

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

Definition 4. The canonical height on $E/\mathbb{Q}$, denoted by $\hat{h}$ or $\hat{h}_E$, is the function

$$\hat{h}: E(\overline{\mathbb{Q}}) \rightarrow \mathbb{R}$$

defined by

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{N \rightarrow \infty} 4^{-N} h_f([2^N]P)$$

where $f \in \mathbb{Q}(E)$ is any nonconstant even function.

Theorem 2.2 ([Sil09], Theorem VIII.9.3). Let $E/\mathbb{Q}$ be an elliptic curve, and $\hat{h}$ the canonical height on E .

(a) For all $P \in E(\overline{\mathbb{Q}})$ and all $m \in \mathbb{Z}$,

$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

(b) Let $P \in E(\overline{\mathbb{Q}})$. Then $\hat{h}(P) \geq 0$ and

$$\hat{h}(P) = 0 \quad \text{if and only if} \quad P \text{ is a torsion point.}$$

We are now ready to formally state the main result we use in our exploration, and explain how the method simplifies in the case of rank 1. 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 $f_1, \dots, f_m$ be morphisms from C to A defined over K . Recall that a morphism is a rational map with no base points.

Definition 5. Let $f_1, \dots, f_m$ 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 do not typically use the definition to check whether a set of morphisms are independent, instead we use the following lemma due to Cassels.

Lemma 2.3 ([Cas68], Lemma 3). Let $f_1, \dots, f_m$ be morphisms from C to A . Let D be the matrix whose coefficients are

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

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 hyperelliptic curve C_a and an elliptic curve, E_a , and thus these degrees are computable through the use of the computer algebra system Magma.

Theorem 2.4 (Dem'yanenko–Manin). Let C be a curve over a number field K and A be an abelian variety over K . Let $f_1, \dots, f_m$ be morphisms from C to A that are defined over K and independent. Assume further that $\text{Rank}(A) < m$. Then $C(K)$ is finite and it is possible to effectively bound the height of the points in $C(K)$.

For a proof of the statement and some examples carried out in practice see [GK05], [Kul99]. The method of Dem'yanenko–Manin simplifies when the $\text{Rank}(A) = 1$ since that would mean that we would only need two independent maps, say $f_1, f_2: C \rightarrow A$. Moreover, if we let $P \in C(\mathbb{Q})$ and R be a generator for the free part of $A(\mathbb{Q})$, then

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

where $T_i \in A(\mathbb{Q})_{\text{tor}}$. 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 the second equation from the first and taking absolute values gives us the following relation:

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

If it happens to be the case that $n = \pm m$, then that would imply that $f_1(P) \pm f_2(P) \in A(\mathbb{Q})_{\text{tor}}$, 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 , as we will see in Section 5. In this way, we bound the possible values of n and m , so all that would be left to do would be to find the points on $C(\mathbb{Q})$ whose images on $A(\mathbb{Q})$ are of the form $nR + T_i$ with $n < B$. Again, this is a finite computation that can be done using Magma.

3. Construction of C_a

The main goal of this section is to demonstrate how we obtain the family of genus 3 hyperelliptic curves, and the two independent maps to the same elliptic curve. In particular, we will arrive at the following result.

Theorem 3.2. *Let a be a nonzero integer and 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, $\text{Jac}_{C_a} \sim E_a \times E_a \times E'$.

Consider the quartic $g(x) = x^4 - a^2x^2 + 1$. Notice that we can pick two distinct non-zero points $z \neq \pm w$ 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 . 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 $g(x)$. 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 genus 3 hyperelliptic curves will be defined as:

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

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

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

In particular, we have 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

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

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 3.1. The maps $\varphi_1, \varphi_2: C_a \rightarrow E_a$ are independent.

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

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

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. A quick calculation on Magma shows 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 Lemma 2.3 the maps are independent. $\square$

Now, maps between curves induce maps on their Jacobians so in particular we have maps from $\text{Jac}_{C_a} \rightarrow \text{Jac}_{E_a} \cong E_a$. More importantly, these maps will be surjective and have finite kernel, so they will be isogenies. This means that Jac_{C_a} has two factors of E_a in its isogeny decomposition. We also know that C_a has genus 3, and $\dim \text{Jac}_{C_a} = 3$, hence the isogeny decomposition of Jac_{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. One way to find an equation for E' is by quotienting C_a by 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 the quotient curve

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

under the automorphism $\tau: C_a \rightarrow C_a$ defined via $[x, y, z] \mapsto [z, y, -x]$. This discussion completes the proof for Theorem 3.2. 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. Our goal now is 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. Controlling the ranks of E_a and E'

In this section we will show that under certain conditions on a , E_a has full 2-torsion, and that $\text{Rank}(E_a) = 1$. We will also make use of the parity conjecture to force the rank of E' to be odd, hence nonzero. A quick search for points on E_a yields the point $P_a = (-a^2, 2a) \in E_a(\mathbb{Q})$. Over the function field, one can see that

this point has infinite order by noting that if it were a torsion point, every specialization would have to be torsion as well. Using a computer algebra system, we compute

$$\hat{h}_{E_2}(P_2) = 0.6758,$$

which shows that P_2 is not a torsion point, and so P_a is not a torsion point. We do a brief search for values of $a \in \mathbb{Z}$ such that $P_a \in E_a(\mathbb{Q})_{\text{tor}}$ and find that P_a is torsion when $a \in \{0, \pm 1\}$. Silverman's Specialization theorem ([Sil09], Theorem C.20.3) tells us that there should be only finitely many a where this should occur, and we believe that these are the only integral values where this happens (we have searched for other instances in the interval $[-100000, 100000]$ and have not found any more), but have not found a proof. With this in mind, if $a \notin \{0, \pm 1\}$, then the rank is at least 1. Our aim is now to show that 1 is also an upper bound for the rank. First, note that

$$\begin{aligned} E_a: y^2 &= x^3 + 2a^2x^2 + (a^4 - 4)x \\ &= x(x + a^2 - 2)(x + a^2 + 2) \end{aligned}$$

so we know that we have three distinct 2-torsion points $(0, 0)$, $(-a^2 + 2, 0)$, and $(-a^2 - 2, 0)$. To ease notation, we will let $e_1 = 0$, $e_2 = -a^2 + 2$, and $e_3 = -a^2 - 2$.

Proposition 1. Suppose that $a \equiv 0 \pmod{3}$, then $E_a(\mathbb{Q})_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. First note that since $a \equiv 0 \pmod{3}$, then $a^2 \equiv 0 \pmod{3}$ and so $a^2 - 2 \equiv 1 \pmod{3}$ and $a^2 + 2 \equiv 2 \pmod{3}$. Thus, 3 never divides $a^2 - 2$ or $a^2 + 2$. Per our above discussion, we already know that E_a contains full 2-torsion. Further, since E_a has discriminant

$$\Delta(E_a) = 2^8(a^2 - 2)^2(a^2 + 2)^2,$$

it has good reduction at the prime 3. Reducing modulo 3 we see that

$$\tilde{E}_a: y^2 = x^3 + 2x$$

which one can easily verify has $\#\tilde{E}_a(\mathbb{F}_3) = 4$. Now, since $E_a[2] \subset E_a(\mathbb{Q})_{\text{tor}}$ and $E_a(\mathbb{Q})_{\text{tor}}$ injects into $\tilde{E}_a(\mathbb{F}_3)$ see [[Sil09], VII.3.1], it must be that $E_a[2] = E_a(\mathbb{Q})_{\text{tor}}$. $\square$

Theorem 4.1. Suppose that $a^2 - 2$ and $a^2 + 2$ are simultaneously prime, then $\text{Rank}(E_a) = 1$.

Proof. We proceed via a complete 2-descent as in [Sil09] (X.1.4). The elliptic curve E_a has discriminant $\Delta(E_a) = 2^8(a^2 - 2)^2(a^2 + 2)^2$ and so the set $S = \{2, a^2 - 2, a^2 + 2, \infty\}$. We now consider the set

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \text{ord}_p(b) \equiv 0 \pmod{2} \text{ for all } p \notin S\}.$$

Concretely, we can identify the set $\mathbb{Q}(S, 2)$ with

$$\{\pm 1, \pm 2, \pm(a^2 - 2), \pm(a^2 + 2), \pm 2(a^2 - 2), \pm 2(a^2 + 2), \pm(a^4 - 4), \pm 2(a^4 - 4)\}.$$

There is an injective homomorphism $E_a(\mathbb{Q})/2E_a(\mathbb{Q}) \hookrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ defined by

$$P = (x, y) \mapsto \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_1, e_2 \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2 \right) & \text{if } x = e_1 \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1} \right) & \text{if } x = e_2 \\ (1, 1) & \text{if } P = \mathcal{O}. \end{cases}$$

The pair $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ will be the image of a point $P = (x, y) \in E_a(\mathbb{Q})/2E_a(\mathbb{Q})$ if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = -a^2 + 2 \tag{1}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -a^2 - 2, \tag{2}$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. There are 256 pairs in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ and for each one we must check whether the defining system of equations has a solution in $\mathbb{Q}$. Luckily, the fact that the map $E_a(\mathbb{Q})/2E_a(\mathbb{Q}) \rightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ is a homomorphism greatly reduces the number of cases we need to check directly. Indeed, if (b_1, b_2) and (b'_1, b'_2) come from $E_a(\mathbb{Q})$, then so does $(b_1b'_1, b_2b'_2)$, while if (b_1, b_2) comes from $E_a(\mathbb{Q})$ but (b'_1, b'_2) does not, then $(b_1b'_1, b_2b'_2)$ will not. We now proceed by describing certain cases for pairs (b_1, b_2) where we can either find a solution to the system or explain their non-existence. Our results will be summarized in Table 1 at the end of the paper where each cell will either have the corresponding point on $E_a(\mathbb{Q})$ if the system has a solution, or the obstruction of a solution to the system.

1. If $b_1 > 0$ and $b_2 < 0$, then (2) has no solutions in $\mathbb{R}$ since the right-hand side of the equation will be negative while the left hand side will be positive.
2. The four 2-torsion points $\{\mathcal{O}, (0, 0), (-a^2 + 2, 0), (-a^2 - 2, 0)\}$ on $E_a(\mathbb{Q})$ map via the map described above to the pairs $\{(1, 1), ((a^2 - 2)(a^2 + 2), a^2 - 2), (-(a^2 - 2), -(a^2 - 2)), (-(a^2 + 2), -1)\}$, respectively.
3. Consider the pair $b_1 = -1$ and $b_2 = -2$. Then the system

$$\begin{aligned} -z_1^2 + 2z_2^2 &= -a^2 + 2 \\ -z_1^2 - 2z_3^2 &= -a^2 - 2, \end{aligned}$$

has the solution $(a, 1, 1)$ with the corresponding point $(-a^2, 2a) \in E_a(\mathbb{Q})$.

4. Taking the pair $(-1, -2)$ from above and multiplying it by the three pairs coming from the non-trivial 2-torsion points gives three new pairs: $\{(-(a^2 - 2)(a^2 + 2), -2(a^2 - 2)), (a^2 - 2, 2(a^2 - 2)), (a^2 + 2, 2)\}$ whose corresponding points on $E_a(\mathbb{Q})$ are: $\left\{ \left(\frac{-a^4 + 4}{a^2}, \frac{-2a^4 + 8}{a^3} \right), (a^2 - 2, 2a^3 - 4a), (a^2 + 2, -2a^3 - 4a) \right\}$.
5. If $b_1 \not\equiv 0 \pmod{a^2 + 2}$ and $b_2 \equiv 0 \pmod{a^2 + 2}$ then (1) implies that $z_1, z_2 \in \mathbb{Z}_{a^2+2}$. Then from (2) we see that $z_1 \equiv 0 \pmod{a^2 + 2}$, which would imply that

$$-a^2 + 2 \equiv 0 \pmod{a^2 + 2},$$

which is not true. Therefore there are no solutions in $\mathbb{Q}_{a^2+2}$.

6. If $b_1 \not\equiv 0 \pmod{a^2 - 2}$ and $b_2 \equiv 0 \pmod{a^2 - 2}$ then through a similar argument as before, reversing the roles of equations (1) and (2) we obtain that the system does not have any solutions in $\mathbb{Q}_{a^2-2}$.
7. Consider the pair $b_1 = -1$ and $b_2 = 1$. We obtain the system

$$\begin{aligned} -z_1^2 - z_2^2 &= -a^2 + 2 \\ -z_1^2 + z_3^2 &= -a^2 - 2. \end{aligned}$$

Subtracting the second equation from the first gives

$$-z_2^2 - z_3^2 = 4,$$

which has no solutions over $\mathbb{R}$. This same line of reasoning also shows that the pairs $(b_1, b_2) = (-1, 2)$ and $(b_1, b_2) = (-2, 1)$ have no solutions over $\mathbb{R}$.

8. Consider the pair $(b_1, b_2) = (1, 2)$. Then we have the system

$$\begin{aligned} z_1^2 - 2z_2^2 &= -a^2 + 2 \\ z_1^2 - 2z_3^2 &= -a^2 - 2. \end{aligned}$$

Note that since a must be odd, the first equation of the system tells us that $v_2(-a^2 + 2) = 0$, and so $v_2(z_1^2 - 2z_2^2) = 0$ as well. This implies that $v_2(z_1), v_2(z_2) \geq 0$. For similar reasons using the second equation, we can deduce that $v_2(z_3) \geq 0$. Now, subtracting the second equation from the first gives us

$$\begin{aligned} 2z_3^2 - 2z_2^2 &= 4 \\ \implies z_3^2 - z_2^2 &= 2. \end{aligned}$$

Assume now that $z_2 = \frac{Y}{d}$ and $z_3 = \frac{X}{d}$ for $X, Y, d \in \mathbb{Z}$ with $\gcd(X, d) = \gcd(Y, d) = 1$ and d odd. We can then rewrite the last equation as

$$\begin{aligned} \left(\frac{X}{d}\right)^2 - \left(\frac{Y}{d}\right)^2 &= 2 \\ \implies X^2 - Y^2 &= 2d^2 \\ \implies (X - Y)(X + Y) &= 2d^2 \end{aligned}$$

Note that $X - Y$ and $X + Y$ must have the same parity. However, they cannot both be odd, otherwise their product would be odd. Also, they cannot both be even, because then that would force $v_2(d) \geq 1$, contradicting that it was odd. Thus, this equation has no solutions in $\mathbb{Q}$.

9. Consider the pair $(b_1, b_2) = (2, 1)$. We obtain the system

$$\begin{aligned} 2z_1^2 - z_2^2 &= -a^2 + 2 \\ 2z_1^2 - 2z_3^2 &= -a^2 - 2. \end{aligned}$$

Note that for the same reasoning as in Case (8) above, we have that $v_2(z_1) \geq 0$, $v_2(z_2) \geq 0$, and $v_2(z_3) \geq 0$. Given this, the second equation in the system already implies that

$$a^2 \equiv 0 \pmod{2}$$

which implies that a is even, which contradicts our initial assumption that $a^2 - 2$ and $a^2 + 2$ are simultaneously prime. This same line of reasoning also shows that the pairs $(b_1, b_2) = (2, 2)$ and $(b_1, b_2) = (-2, -2)$ also contradict the primality of $a^2 - 2$ and $a^2 + 2$. We will denote this obstruction in Table 1 as $\star$.

10. Finally, we consider the pair $(b_1, b_2) = ((a^2 - 2)(a^2 + 2), 2)$. This gives the system

$$\begin{aligned} (a^2 - 2)(a^2 + 2)z_1^2 - 2z_2^2 &= -a^2 + 2 \\ (a^2 - 2)(a^2 + 2)z_1^2 - 2(a^2 - 2)(a^2 + 2)z_3^2 &= -a^2 - 2. \end{aligned}$$

We start by noting that the first equation in the system implies that $v_{a^2-2}(z_2) > 0$, which implies that $v_{a^2-2}(z_1) \geq 0$. Then using those two facts along with the second equation of the system we can deduce that $v_{a^2-2}(z_3) \geq 0$. Reducing the second equation modulo $a^2 - 2$ gives

$$-(a^2 + 2) \equiv 0 \pmod{a^2 - 2},$$

but this cannot happen since $a^2 - 2$ and $a^2 + 2$ are distinct primes. We will denote this obstruction in Table 1 as $\diamond$.

The remaining cells of Table 1 are now filled in using the multiplicative rule we discussed earlier. The size of $E_a(\mathbb{Q})/2E_a(\mathbb{Q})$ is 2^{2+r} where $r := \text{Rank}(E_a)$, and we have found that only 2^3 pairs in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ are the image of a point in $E_a(\mathbb{Q})/2E_a(\mathbb{Q})$. Therefore, $r = 1$. $\square$

Remark 1. We could try this same analysis for E' , however the factorization of its discriminant forces certain primality conditions that would make $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ a set of size 4096. Even then, this provides an upper bound for its rank, and we were not able to find an explicit point of infinite order as we did in the case of E_a to also place a lower bound.

Definition 6. 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. We instead direct the interested reader to [Roh93] for a more detailed exposition of local root numbers. 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 [KD23]. We remark that the result has more cases, and we have only included the ones relevant to our purposes.

Theorem 4.2 ([KD23], Theorem 2.3). 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 $v: \mathcal{K}^\times \rightarrow \mathbb{Z}$ 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 $\text{char}(k) = 2$, then $w(E/\mathcal{K}) = (-1, -c_6)_\mathcal{K}$. In particular, if $\mathcal{K} = \mathbb{Q}_2$, then

$$w(E/\mathbb{Q}_2) = \begin{cases} -1 & \text{if } c'_6 \equiv 1 \pmod{4} \\ +1 & \text{if } c'_6 \equiv 3 \pmod{4} \end{cases}$$

$$\text{where } c'_6 = \frac{c_6}{2^{v(c_6)}}.$$

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 various primes. Now, over $\mathbb{Q}$, the places are precisely the primes, and the usual infinite place. 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.

Conjecture 1 ([Dok13], Parity Conjecture). Let E/K be an elliptic curve over a number field. Then

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

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

We were not able to find a point of infinite order on E' , which means that in order to try and control its rank, we will need to make use of the Parity Conjecture. Note that its discriminant is $\Delta(E') = 2^8 a^8 (a^2 - 2)^2 (a^2 + 2)^2$, which complicates things because recall the fact that $a^2 - 2$ and $a^2 + 2$ being simultaneously prime forces $a \equiv 0 \pmod{3}$. 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 $q \equiv 3 \pmod{4}$.

Theorem 4.3. Let $a = 3q$, with $q > 3$ prime, $q \equiv 3 \pmod{4}$ and $a^2 - 2, a^2 + 2$ are both prime. Then, assuming the Parity Conjecture, $\text{Rank}(E')$ is odd.

Proof. We have $\Delta(E') = 2^8 a^8 (a^2 - 2)^2 (a^2 + 2)^2$ 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 [BR22] 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 $bd \equiv 3 \pmod{4}$ and thus the reduction type is I_0^* . Since we have additive, potentially multiplicative reduction and $c'_6 \equiv 3 \pmod{4}$, Theorem 4.2 tells us that $w_2(E') = 1$. We should note that by Theorem 3.7 in [BR22], 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

$$y^2 \equiv x^3 + 2x^2 \pmod{p},$$

and since $\left(\frac{2}{3}\right) = -1$, we have non-split multiplicative reduction. Hence, by Theorem 4.2 $w_3(E') = 1$.

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

$$y^2 \equiv x^3 - 4x^2 \pmod{p},$$

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

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

Thus, by Theorem 4.2, $w_q(E') = 1$.

At the primes $a^2 - 2$ and $a^2 + 2$ the reduction has the same equation

$$y^2 \equiv x(x - 4)^2 \pmod{p},$$

which can be seen has split type (since 4 is a square) 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 2. There are infinitely many $3q$, with $q > 3$ and $q \equiv 3 \pmod{4}$ such that $9q^2 - 2$ and $9q^2 + 2$ are simultaneously prime.

This conjecture is an instance of Schinzel's Hypothesis H [SS58], with enough evidence supporting its validity.

5. Bounding the Difference in Heights

In this section our aim will be to prove the following inequality concerning the difference between the canonical heights on E_a

$$\left| \hat{h}_{E_a}(\varphi_1(P)) - \hat{h}_{E_a}(\varphi_2(P)) \right| \leq 49.39 + \log(9a^2 + 7).$$

As mentioned before, this will allow us to effectively find all the possible images of the points $P \in C_a(\mathbb{Q})$ under the maps φ_1 and φ_2 . Recall that we have explicit maps φ_1 and φ_2 and if we are concerned with bounding the quantity

$$\left| \hat{h}_{E_a}(\varphi_1(P)) - \hat{h}_{E_a}(\varphi_2(P)) \right|,$$

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:

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

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. 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 be verified through computer algebra systems such as Magma, for instance. $\square$

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 5.2. 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:

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

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 using the Euclidean algorithm for polynomials.

If we write $x = x(P) = \frac{r}{s}$ in lowest terms then we can write $x(\varphi_1(P)) = \frac{F_1(r, s)}{G_1(r, s)}$ and $x(\varphi_2(P)) = \frac{F_2(r, s)}{G_2(r, s)}$ as quotients of integers. We can restate the identities for our lemmas using this notation. For Lemma 5.1, we have

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

This implies that we have

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

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

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

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

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

We can do the exact same argument for the identities in Lemma 5.2 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 is all terms which are negative. We thus obtain,

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

Now, y can be negative, and if that is so it could potentially increase the value of the numerator. To deal with this, we simply use the inequality $|y| \leq y''$, where y'' is the same as above. This gives us the upper estimates:

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

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

$$\begin{aligned} x(\varphi_1(P)) &\leq \frac{2r^4 + (12a^2 + 6)r^2s^2 + 2s^4}{r^4 + 2r^2s^2 + s^4} \\ x(\varphi_2(P)) &\leq \frac{(a^2 + 2)r^4 + (6a^2 + 6)r^2s^2 + (a^2 + 2)s^4}{r^4 + 2r^2s^2 + s^4}. \end{aligned}$$

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:

$$\begin{aligned} H(\varphi_1(P)) &\leq \max\{(12a^2 + 10)H(P)^4, 4H(P)^4\} \\ h(\varphi_1(P)) &\leq \log(12a^2 + 10) + 4h(P) \end{aligned}$$

and

$$\begin{aligned} H(\varphi_2(P)) &\leq \max\{(8a^2 + 10)H(P)^4, 4H(P)^4\} \\ h(\varphi_2(P)) &\leq \log(8a^2 + 10) + 4h(P). \end{aligned}$$

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

Lemma 5.3. For $P \in C_a(\mathbb{Q})$, we have:

$$\begin{aligned} \log\left(\frac{1}{4}\right) + 4h(P) &\leq h(\varphi_1(P)) \leq \log(12a^2 + 10) + 4h(P) \\ \log\left(\frac{1}{4}\right) + 4h(P) &\leq h(\varphi_2(P)) \leq \log(8a^2 + 10) + 4h(P). \end{aligned}$$

Combining the inequalities from Lemma 5.3, we obtain the following inequality:

$$|h(\varphi_1(P)) - h(\varphi_2(P))| \leq \log(12a^2 + 10) - \log\left(\frac{1}{4}\right). \quad (3)$$

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

Lemma 5.4. Let $P \in E_a(\mathbb{Q})$. Then we have:

$$\left| \hat{h}_{E_a}(P) - h_{E_a}(P) \right| \leq 24. \quad (4)$$

Proof. This follows from writing E_a in short Weierstrass form, and using Proposition 1.2 in [GK05]. $\square$

Theorem 5.5. Let $P \in C_a(\mathbb{Q})$. Then we have

$$\left| \hat{h}_{E_a}(\varphi_1(P)) - \hat{h}_{E_a}(\varphi_2(P)) \right| \leq 49.39 + \log(12a^2 + 10).$$

Proof. This is a combination of the inequalities (3) and 4 from the above lemmas. $\square$

Example 1. Let $a = 237$. Note that this is of the form required by the conditions in Conjecture 2. By Theorem 5.5, we have that

$$\left| \hat{h}_{E_{237}}(\varphi_1(P)) - \hat{h}_{E_{237}}(\varphi_2(P)) \right| \leq 63.35.$$

Also, since $a = 237$, we have

$$E_{237} : y^2 = x^3 + 112338x^2 + 3154956557x$$

and using Magma we can find a generator for its free part, say R . We find $\hat{h}(R) = 5.29$. This implies that

$$|n^2 - m^2| \leq 11.96 \Rightarrow \max\{|n|, |m|\} \leq \frac{1}{2}(11.96 + 1) < 7.$$

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

- $P \in C_{237}(\mathbb{Q})$ such that $\varphi_1(P) \pm \varphi_2(P) \in E_{237}(\mathbb{Q})_{\text{tor}}$
- $P \in C_{237}(\mathbb{Q})$ such that $\varphi_1(P) = nR + T$ or $\varphi_2(P) = nR + T$ with $T \in E_{237}(\mathbb{Q})_{\text{tor}}$ and $|n| \leq 6$.

Even with the large coefficients on the equations, these calculations were carried out on Magma's online calculator in under 3 seconds and we find:

$$C_{237}(\mathbb{Q}) = \{(\pm 1 : \pm 4 : 1), (0 : \pm 1 : 1), (1 : \pm 1 : 0)\}.$$

Remark 3. When considering the values of $a \in [1, 1000]$, we found that 552 of them gave $\text{Rank}(E_a) = 1$ and $\text{Rank}(E') > 0$, so the method of Dem'yanenko–Manin can be used for many curves in this family in an automated way.

Acknowledgements

This work is part of the authors Ph.D. thesis. We would like to thank David Zureick-Brown for his introduction to the area and helpful conversations throughout graduate school. We would also like to thank Nathan Kaplan for his comments on an earlier version of this paper and to the anonymous referee for helpful feedback.

References

- [BCP97] 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.
- [Bom90] Enrico Bombieri. The Mordell conjecture revisited. *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze*, 17(4):615–640, 1990.
- [BR22] 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.
- [Cas68] JWS Cassels. On a theorem of Dem’yanenko. *Journal of the London Mathematical Society*, 1(1):61–66, 1968.
- [Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieure à l’unité. *CR Acad. Sci. Paris*, 212(882-885):1, 1941.
- [Col85] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765 – 770, 1985.
- [Dem68] Vadim Andreevich Dem’yanenko. Rational points of a class of algebraic curves. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 30(6):1373–1396, 1968.
- [Dok13] Vladimir Dokchitser. Notes on the parity conjecture, Springer, 2013, pp. 201–249.
- [Fal83] Gerd Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73:349–366, 1983.
- [GK05] Martine Girard and Leopoldo Kulesz. Computation of sets of Rational Points of Genus-3 Curves via the Dem’yanenko–Manin Method. *LMS Journal of Computation and Mathematics*, 8:267–300, 2005.
- [HS13] Marc Hindry and Joseph H Silverman. *Diophantine Geometry: An Introduction*, volume 201. Springer Science & Business Media, 2013.
- [KD23] Lilybelle Cowland Kellock and Vladimir Dokchitser. Root numbers and parity phenomena, 2023.
- [Kul99] Leopoldo Kulesz. Application de la méthode de Dem’yanenko–Manin à certaines familles de courbes de genre 2 et 3. *Journal of Number Theory*, 76(1):130–146, 1999.
- [Man69] Ju I Manin. The p -torsion of elliptic curves is uniformly bounded. *Selected Papers Of Yu I Manin*, 3:185, 1969.
- [Roh93] David E Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Mathematica*, 87(2):119–151, 1993.
- [Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2009.
- [SS58] Andrzej Schinzel and Waław Sierpiński. Sur certaines hypotheses concernant les nombres premiers. *Acta Arithmetica*, 4(3):185–208, 1958.
- [Voj91] Paul Vojta. Siegel’s theorem in the compact case. *Annals of Mathematics*, 133(3):509–548, 1991.