4-COVERING MAPS ON ELLIPTIC CURVES WITH TORSION SUBGROUP $Z_2 \times Z_8$

SAMUEL IVY, BRETT JEFFERSON, MICHELE JOSEY, CHERYL OUTING, CLIFFORD TAYLOR, AND STACI WHITE

ABSTRACT. In this exposition we consider elliptic curves over $\mathbb{Q}$ with the torsion subgroup $Z_2 \times Z_8$. In particular, we discuss how to determine the rank of the curve $E : y^2 = (1-x^2)(1-k^2\,x^2)$, where $k = (t^4 - 6t^2 + 1)/(t^2+1)^2$ and $t = 9/296$. We use a 4-covering map $\widehat{C}'_{d_2} \to \widehat{C}_{d_2} \to E$ in terms of homogeneous spaces for $d_2 \in \{-1, 6477590, 2, 7, 37\}$. We provide a method to show that the Mordell-Weil group is $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$, which would settle a conjecture of Flores-Jones-Rollick-Weigandt and Rathbun.

1. INTRODUCTION

Given an elliptic curve E, we denote the set of $\mathbb{Q}$-rational points as $E(\mathbb{Q})$. Since $E(\mathbb{Q})$ is finitely generated, there exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and a nonnegative integer r such that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, where r is called the (Mordell-Weil) rank. Those elliptic curves with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ are birationally equivalent to

$$y^2 = (1-x^2)(1-k^2\,x^2) \quad \text{where} \quad k = \frac{t^4 - 6t^2 + 1}{(t^2+1)^2} \quad \text{for some } t \in \mathbb{Q}.$$

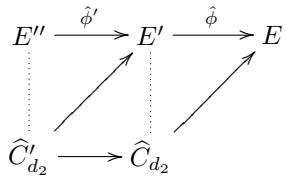
The highest known rank of curves with this torsion subgroup is $r = 3$. It is conjectured in [6] that this bound is obtained when $t = 9/296$; one knows that $2 \le r \le 3$ for this particular t. In this exposition, we focus on determining the exact rank of this particular elliptic curve. Our main result is as follows:

Theorem. *Assuming the Birch and Swinnerton-Dyer conjecture, the Mordell-Weil group of the elliptic curve*

$$E: \begin{aligned} Y^2 + X\,Y = X^3 &- 7181359868024838434108428477109624412 0\,X \\ &+ 2342384302041141813702521859646228641128533374139589904 00 \end{aligned}$$

is $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$*, where* $r = 3$*.*

We sketch the idea of the proof. Consider the diagram:



2000 *Mathematics Subject Classification.* Primary 14H52; Secondary 14J27.

E is 2-isogenous to E', which itself is 2-isogenous to E''. Using the connecting homomorphisms,

$$\widehat{\delta} : \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \qquad \text{and} \qquad \widehat{\delta}' : \frac{E'(\mathbb{Q})}{\hat{\phi}'(E''(\mathbb{Q}))} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2},$$

we may determine the rank r by finding $\mathbb{Q}$-rational points (z, w) on the homogeneous spaces

$$\widehat{C}_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2)(1 + d_2 \kappa^2 z^2) \qquad \text{where} \quad \kappa = \left(\frac{2t}{t^2 - 1}\right)^2;$$

$$\widehat{C}'_{d_2} : \quad d_2 w^2 = (1 + d_2 z^2)(1 + d_2 {k'}^2 z^2) \qquad \text{where} \quad k' = \frac{4(t^3 - t)}{(t^2 + 1)^2}.$$

When $t = 9/296$, we use Cremona's `mwrank` [4] to find that the images of these connecting homomorphisms are contained in the group generated by -1, 6477590, 2, 7, and 41. We find rational points on the homogeneous spaces for the first four generators; see Tables 2 and 3. Hence $2 \leq r \leq 3$. The (global) root number of E is $w_E = -1$, so that the rank r must be odd. Hence, assuming the conjecture of Birch and Swinnerton-Dyer, we see that $r = 3$.

Alternatively, it suffices then to find rational points on $\widehat{C}_{d_2}$ and $\widehat{C}'_{d_2}$ for $d_2 = 37$. The various maps in the diagram above involve quadratic polynomials; hence, we consider this diagram to be a "4-cover" of the elliptic curve E. In comparison to finding points on E, it should be half as difficult to find points on $\widehat{C}_{d_2}$ and a quarter as difficult to find points on $\widehat{C}'_{d_2}$.

The authors would like to thank the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI) at Miami University for the opportunity to conduct this research. They would also like to thank the National Science Foundation and the National Security Agency for their funding, as well as Residential Computing (ResComp) at Miami University and the Rosen Center for Advanced Computing (RCAC) at Purdue University for use of their machines. They are grateful to Michael Stoll for helpful conversations, Tom Farmer for careful reading of this document, Elizabeth Fowler for her constant support, and Edray Goins for his guidance.

2. Foundations

An elliptic curve E is a set of points which satisifies an equation of the form $Y^2 = X^3 + AX + B$, where A and B are rational numbers such that the discriminant $-16(4A^3 + 27B^2) \neq 0$. In particular, an elliptic curve is a type of nonsingular cubic curve. Define $E(\mathbb{Q})$ as the set of $\mathbb{Q}$-rational points, where we append a "point at infinity" $\mathcal{O}$.

We may use geometry to turn $E(\mathbb{Q})$ into a group. For $P, Q \in E(\mathbb{Q})$, draw a line through P and Q. (If $P = Q$, we choose the line tangent to the curve at P.) This line will intersect the curve at a third $\mathbb{Q}$-rational point $P * Q$ – which may possibly be $\mathcal{O}$. By reflecting this point about the x-axis, we obtain another $\mathbb{Q}$-rational point, denoted by $P \oplus Q$. For a graphical represention, see Figure 1. Formally define $P \oplus Q = (P * Q) * \mathcal{O}$. Under this operation, the set $E(\mathbb{Q})$ forms an abelian group with the identity element $\mathcal{O}$ and inverse $[-1]P = P * \mathcal{O}$. For more information, see [12].

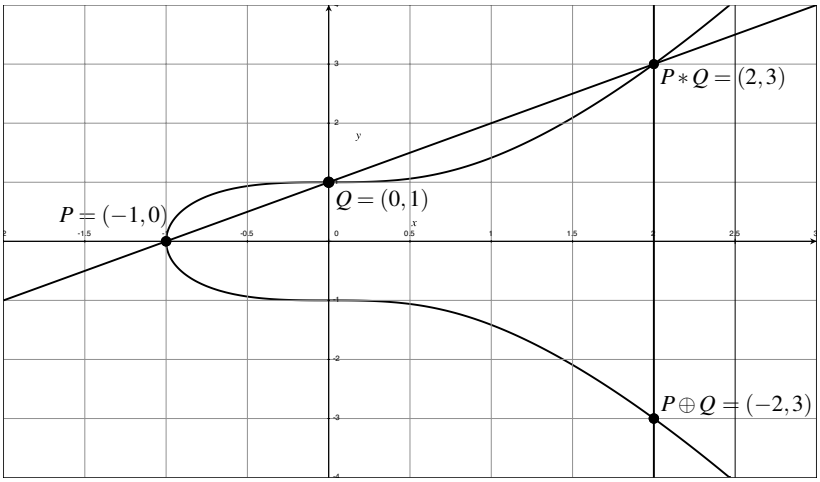


FIGURE 1. The Group Law on an Elliptic Curve

In 1901, Henri Poincaré conjectured [10] that this abelian group is finitely generated. This was proved by Louis Mordell in 1922.

Theorem 1 (Mordell, [9])**.** *If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated. Furthermore, there exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and a nonnegative integer r such that*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$

This motivates a few definitions. The set $E(\mathbb{Q})_{\text{tors}}$ is the collection of points with finite order; it is called the torsion subgroup of E. This implies that the quotient group $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}^r$ is a torsion-free group. The nonnegative integer r is called the Mordell-Weil rank of E; it signifies the number of independent generators having infinite order.

While the rank r is mysterious, the torsion subgroup is well-understood. In 1977, Barry Mazur completely classified the structure of torsion subgroups of elliptic curves.

Theorem 2 (Mazur, [8])**.** *If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

(i) Z_n, *with* $1 \leq n \leq 10$ *or* $n = 12$;
(ii) $Z_2 \times Z_{2m}$, *with* $1 \leq m \leq 4$.

Here we denote Z_n as the cyclic group of order n. We will focus more specifically on those elliptic curves with torsion subgroup $Z_2 \times Z_8$.

In contrast to the torsion subgroup, less is known about the rank r of an elliptic curve. As of 2006, the largest known rank satisfies $r \geq 28$. Andrej Dujella [5] has a listing of the largest known ranks among families of elliptic curves with prescribed torsion. Table 1 contains this information. Note that the highest known rank for curves E with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ is $r = 3$.

TABLE 1. Rank Records

Torsion Subgroup T	Lower Bound for $B(T)$	Author(s)
Z_1	28	Elkies (2006)
Z_2	18	Elkies (2006)
Z_3	13	Eroshkin (2007, 2008)
Z_4	12	Elkies (2006)
Z_5	6	Dujella - Lecacheux (2001)
Z_6	8	Eroshkin (2008) Dujella - Eroshkin (2008) Elkies (2008) Dujella (2008)
Z_7	5	Dujella - Kulesz (2001) Elkies (2006)
Z_8	6	Elkies (2006)
Z_9	3	Dujella (2001) MacLeod (2004) Eroshkin (2006) Eroshkin - Dujella (2007)
Z_{10}	4	Dujella (2005) Elkies (2006)
Z_{12}	3	Dujella (2001, 2005, 2006) Rathbun (2003, 2006)
$Z_2 \times Z_2$	14	Elkies (2005)
$Z_2 \times Z_4$	8	Elkies (2005) Eroshkin (2008) Dujella - Eroshkin (2008)
$Z_2 \times Z_6$	6	Elkies (2006)
$Z_2 \times Z_8$	3	Connell (2000) Dujella (2000, 2001, 2006) Campbell - Goins (2003) Rathbun (2003, 2006) Flores - Jones - Rollick - Weigandt (2007)

3. Computing The Mordell-Weil Rank

Mordell's proof [9] of Poincaré's conjecture began by considering the quotient group, $E(\mathbb{Q})/2E(\mathbb{Q})$. Although $E(\mathbb{Q})$ in general is an infinite group, the quotient group is always finite. In fact, if $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2m}$, then $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq Z_2^{r+2}$, where r is the Mordell-Weil rank. Hence, the basic idea to compute r is to calculate $|E(\mathbb{Q})/2E(\mathbb{Q})|$.

To this end, we will compute two smaller, yet related, quotient groups. One constructs quotient groups for elliptic curves by considering a special type of group homomorphism. For instance, let E and E' be two elliptic curves over $\mathbb{Q}$. We say that a group homomorphism $\phi : E \to E'$ is an m-isogeny if (1) the coordinates of ϕ involve rational functions with $\mathbb{Q}$-rational coefficients and (2) there are exactly

m points in the kernel $E(\mathbb{Q})[\phi]$ of the map. We will be interested in the case where $m = 2$.

Proposition 3. *Let E and E' be elliptic curves over $\mathbb{Q}$. Let $\phi : E \to E'$ and $\hat{\phi} : E' \to E$ be 2-isogenies such that $\hat{\phi} \circ \phi = [2]$ is the map which sends $P \mapsto P \oplus P$. Assume that $E'(\mathbb{Q})[\hat{\phi}] = \phi(E(\mathbb{Q})[2])$. Then,*

$$\left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = \left|\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right| \left|\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))}\right|.$$

It is easy to show that if E is an elliptic curve over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2m}$, then the criterion $E'(\mathbb{Q})[\hat{\phi}] = \phi(E(\mathbb{Q})[2])$ of Proposition 3 is always satisfied.

Proof. Using the isogeny $\hat{\phi}$, we have the exact sequence:

$$\{\mathcal{O}\} \longrightarrow \frac{E'[\hat{\phi}]}{\phi(E[2])} \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \xrightarrow{\hat{\phi}} \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \longrightarrow \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \longrightarrow \{\mathcal{O}\}.$$

From the assumption that the left-most quotient group is trivial, Lagrange's Theorem and the First Isomorphism Theorem imply the equalities:

$$\left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = \left|\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right| \left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \Big/ \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right| = \left|\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right| \left|\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))}\right|.$$

□

The standard theory of elliptic curves uses Galois cohomology to express elements in these quotient groups as square-free integers. One constructs injective maps having finite image, the so-called "connecting homomorphisms", denoted as follows:

$$\delta : \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \qquad \text{and} \qquad \widehat{\delta} : \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}.$$

These homomorphisms are constructed so that the primes which divide these square-free integers must also divide the discriminant of the elliptic curve. For more information, see [12].

To compute the Mordell-Weil rank r, it is sufficient to determine the number of elements in the image of both δ and $\widehat{\delta}$. Software such as `mwrank` can quickly find an upper bound on the number of generators for these images. That is, the flag `-s` uses an efficient algorithm to compute an upper bound on the rank r.

Instead of proving the existence of such homomorphisms in general, we will work with explicit examples for the remainder of the exposition.

4. 4-Covering Maps for Curves with Torsion Subgroup $Z_2 \times Z_8$

We explain how to determine the Mordell-Weil rank of the elliptic curve

$$E : \begin{aligned} Y^2 + XY &= X^3 - 7181359868024838434108428477109624412 0\,X \\ &\quad + 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

This curve has torsion subgroup $Z_2 \times Z_8$. Using ideas from the previous section, we wish to consider 2-isogenous curves to help us compute the rank.

Theorem 4 (Goins, [7])**.** *Say that E is an elliptic curve over $\mathbb{Q}$ with torsion subgroup $Z_2 \times Z_8$.*

(1) *There exists a rational number t such that E is birationally equivalent to the curve*

$$y^2 = (1-x^2)(1-k^2\,x^2) \quad \textit{where} \quad k = \frac{t^4-6t^2+1}{(t^2+1)^2}.$$

(2) *There exists a 2-isogeny $\phi : E \to E'$ in terms of the curve*

$$E' : \quad y^2 = (1+x^2)(1+\kappa^2 x^2) \quad \textit{where} \quad \kappa = \left(\frac{2t}{t^2-1}\right)^2.$$

Moreover, E' has torsion subgroup $Z_2 \times Z_4$.

(3) *There exists a 2-isogeny $\phi' : E' \to E''$, and hence a 4-isogeny $\phi' \circ \phi : E \to E''$, in terms of the curve*

$$E'' : \quad y^2 = (1+x^2)(1+{k'}^2 x^2) \quad \textit{where} \quad k' = \frac{4(t^3-t)}{(t^2+1)^2}.$$

Moreover, E'' has torsion subgroup $Z_2 \times Z_2$.

These three elliptic curves are related using the diagram:

$$E'' \xleftarrow{\ \phi'\ } E' \xleftarrow{\ \phi\ } E.$$

We focus on the case where $t = 9/296$, which was first considered in [6]. Weierstrass models corresponding to this value of t are as follows:

$$E' : \begin{array}{l} Y^2 + X\,Y = X^3 - 7182838410586195768223026686032504412 0\,X \\ \qquad + 2341371525751308852524074565174235775172724198311084304 00; \end{array}$$

$$E'' : \begin{array}{l} Y^2 + X\,Y = X^3 - 8791041401157870064556943644005177212 0\,X \\ \qquad + 1215293335280977803803190858716511058206567605433869568 00. \end{array}$$

With these models, the 2-isogeny $\phi : E \to E'$ sends

$$X \mapsto \frac{X^2 - 4892734605697550640\,X + 29570851227146682291964178457600 00}{X - 4892734605697550640};$$

$$Y \mapsto \frac{\left(\begin{array}{l} X^2\,Y - 9785469211395101280\,X\,Y \\ \qquad - 29570851227146682291964178457600 00\,X \\ \qquad + 23935894836667651667393174877518649600\,Y \\ \qquad + 72341163559497227029837401483265662394086546432000 00 \end{array}\right)}{\left(X - 4892734605697550640\right)^2}.$$

Theorem 5. *Using the 2-isogenies $\phi : E \to E'$ and $\hat{\phi} : E' \to E$, define the maps:*

$$\delta : \quad \frac{E'(\mathbb{Q})}{\phi\big(E(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^\times}{\left(\mathbb{Q}^\times\right)^2}, \qquad (X:Y:1) \quad \mapsto \quad 4X + 39141876845580405121;$$

$$\widehat{\delta} : \quad \frac{E(\mathbb{Q})}{\hat{\phi}\big(E'(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^\times}{\left(\mathbb{Q}^\times\right)^2}, \qquad (X:Y:1) \quad \mapsto \quad X - 4892734605697550640.$$

Both δ and $\widehat{\delta}$ are injective group homomorphisms with finite images. To be precise, let $\Sigma(k) = \{82207, 87697, 92863\}$ and $\Sigma(\kappa) = \{2, 3, 5, 7, 37, 41, 61\}$ be the set of

primes dividing k and κ, respectively, as in Theorem 4. Define the groups:

$$\Gamma(k) = \left\{ d_1 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \;\middle|\; d_1 \equiv \pm \prod_{\ell \in \Sigma(k)} \ell^{e(\ell)} \right\};$$

$$\Gamma(\kappa) = \left\{ d_2 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \;\middle|\; d_2 \equiv \pm \prod_{\ell \in \Sigma(\kappa)} \ell^{e(\ell)} \right\}.$$

Here, $e(\ell)$ is either 0 or 1. Then the connecting homomorphisms have the images:

$$\delta\left(\frac{E'(\mathbb{Q})}{\phi\big(E(\mathbb{Q})\big)}\right) = \left\{ d_1 \in \Gamma(k) \;\middle|\; \begin{array}{l} C_{d_1}:\ d_1\, w^2 = \big(1 - d_1\, z^2\big)\big(1 - d_1\, k^2\, z^2\big) \\ \textit{has a } \mathbb{Q}\textit{-rational point } (z, w) \end{array} \right\};$$

$$\widehat{\delta}\left(\frac{E(\mathbb{Q})}{\hat{\phi}\big(E'(\mathbb{Q})\big)}\right) = \left\{ d_2 \in \Gamma(\kappa) \;\middle|\; \begin{array}{l} \widehat{C}_{d_2}:\ d_2\, w^2 = \big(1 + d_2\, z^2\big)\big(1 + d_2\, \kappa^2\, z^2\big) \\ \textit{has a } \mathbb{Q}\textit{-rational point } (z, w) \end{array} \right\}.$$

The various curves introduced in this theorem fit together in the diagrams:

We consider these diagrams to be "2-covers" because the diagonal maps involve quadratic polynomials. Hence, it is half as difficult to find $\mathbb{Q}$-rational points on the "homogeneous spaces" C_{d_1} and $\widehat{C}_{d_2}$ than it is to find $\mathbb{Q}$-rational points on the elliptic curves E' and E, respectively.

Theorem 6. *Using the 2-isogenies $\phi' : E' \to E''$ and $\hat{\phi}' : E'' \to E'$, define the maps:*

$$\delta' : \quad \frac{E''(\mathbb{Q})}{\phi'\big(E'(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \qquad (X : Y : 1) \quad \mapsto \quad 4X + 40011942240487566721;$$

$$\widehat{\delta}' : \quad \frac{E'(\mathbb{Q})}{\hat{\phi}'\big(E''(\mathbb{Q})\big)} \hookrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \qquad (X : Y : 1) \quad \mapsto \quad X - 5001492780060945840.$$

Both δ' and $\widehat{\delta}'$ are injective group homomorphisms with finite images. To be precise, let $\Sigma(\kappa') = \{82207, 92863\}$ and $\Sigma(k') = \{2, 3, 5, 7, 37, 41, 61, 87697\}$ be the set of primes dividing $\kappa' = (1 - k')/(1 + k')$ and k', respectively, as in Theorem 4. Define the groups:

$$\Gamma(\kappa') = \left\{ d_1 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \;\middle|\; d_1 \equiv \pm \prod_{\ell \in \Sigma(\kappa')} \ell^{e(\ell)} \right\};$$

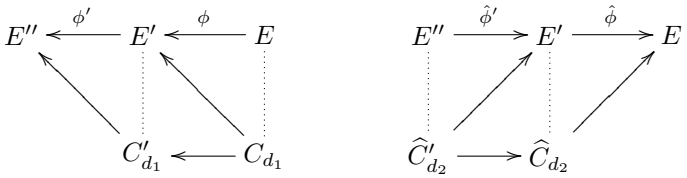
$$\Gamma(k') = \left\{ d_2 \in \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \;\middle|\; d_2 \equiv \pm \prod_{\ell \in \Sigma(k')} \ell^{e(\ell)} \right\}.$$

Then the connecting homomorphisms have the images:

$$\delta'\left(\frac{E''(\mathbb{Q})}{\phi'\big(E'(\mathbb{Q})\big)}\right) = \left\{ d_1 \in \Gamma(\kappa') \;\middle|\; \begin{array}{l} C'_{d_1}:\ d_1\, w^2 = \big(1 - d_1\, z^2\big)\left(1 - d_1\, \kappa'^2\, z^2\right) \\ \textit{has a } \mathbb{Q}\textit{-rational point } (z, w) \end{array} \right\};$$

$$\widehat{\delta}'\left(\frac{E'(\mathbb{Q})}{\hat{\phi}'\big(E''(\mathbb{Q})\big)}\right) = \left\{ d_2 \in \Gamma(k') \;\middle|\; \begin{array}{l} \widehat{C}'_{d_2}:\ d_2\, w^2 = \big(1 + d_2\, z^2\big)\left(1 + d_2\, k'^2\, z^2\right) \\ \textit{has a } \mathbb{Q}\textit{-rational point } (z, w) \end{array} \right\}.$$

The various curves introduced in this theorem fit together in the diagrams:



We consider these diagrams to be "4-covers" because they both contain pairs of diagonal maps, each involving quadratic polynomials. In the diagram on the right, a $\mathbb{Q}$-rational point on E (E', respectively) will correspond to a $\mathbb{Q}$-rational point on $\widehat{C}_{d_2}$, ($\widehat{C}'_{d_2}$, respectively) having half as many digits. We will use the 2-isogeny $\phi : E \to E'$ to construct a map $\widehat{C}'_{d_2} \to \widehat{C}_{d_2}$.

Sketch of proof. First, we show that δ, $\widehat{\delta}$, δ', and $\widehat{\delta}'$ are group homomorphisms.

Lemma 7. *Let E be an elliptic curve over $\mathbb{Q}$ in the form $Y^2+XY = X^3+AX+B$. Let e be a rational number that is a root of the polynomial*

$$\psi_2(X) = 4X^3 + X^2 + 4AX + 4B,$$

and define the map

$$\delta: \qquad E(\mathbb{Q}) \to \frac{\mathbb{Q}^\times}{\left(\mathbb{Q}^\times\right)^2}, \qquad (X:Y:1) \quad \mapsto \quad X - e \pmod{\left(\mathbb{Q}^\times\right)^2}.$$

Then δ is a group homomorphism.

Proof of Lemma. Consider the $\mathbb{Q}$-rational points

$$P = (X_1 : Y_1 : 1), \quad Q = (X_2 : Y_2 : 1), \quad \text{and} \quad P \oplus Q = (X_3 : Y_3 : 1).$$

We want to show that $\delta(P)\cdot\delta(Q) = \delta(P \oplus Q)$, so it suffices to show that $\delta(P)\cdot\delta(Q)\cdot\delta(P \oplus Q)$ is a perfect square. Write E as the zero locus of the cubic polynomial

$$F(X, Y) = Y^2 + XY - X^3 - AX - B.$$

Upon completing the square, $4F(X, Y) = (2Y + X)^2 - \psi_2(X)$; note that $\psi_2(e) = 0$. Now we consider the line $Y = mX + b$ through the points P and Q. As this line goes through P, Q, and $P * Q$, we have the factorization

$$F(X, mX + b) = (X_1 - X)(X_2 - X)(X_3 - X).$$

Letting $X = e$ implies that

$$\delta(P) \cdot \delta(Q) \cdot \delta(P \oplus Q) = F(e, me + b) = \left(me + b + \frac{e}{2}\right)^2.$$

□

The polynomial $\psi_2(X)$ is the 2-division polynomial of E. It is easy to check that $\psi_2(e) = 0$ whenever we have

$$\left.\begin{aligned} e &= 4892734605697550640 \\ A &= -7181359868024838434108428477109624412 0 \\ B &= 234238430204114181370252185964622864112853337413958990400 \end{aligned}\right\} \text{ for } E;$$

$$\left.\begin{aligned} e &= -39141876845580405121/4 \quad \text{or} \quad 5001492780060945840 \\ A &= -7182838410586195768223026686032504412 0 \\ B &= 234137152575130885252407456517423577517272419831108430400 \end{aligned}\right\} \text{ for } E';$$

$$\left.\begin{aligned} e &= -400119422404875667 21/4 \\ A &= -879104140115787006455694364400517721 20 \\ B &= 121529333528097780380319085871651105820656760543386956800 \end{aligned}\right\} \text{ for } E''.$$

This shows that δ, $\widehat{\delta}$, δ', and $\widehat{\delta}'$ are homomorphisms.

Second, we show that the images of δ, $\widehat{\delta}$, δ', and $\widehat{\delta}'$ correspond to points on quartic curves. If $d_1 = \delta(P)$ is the image of some $\mathbb{Q}$-rational point $P = (X : Y : 1)$ on E', then (z, w) is a $\mathbb{Q}$-rational point on C_{d_1}, where we have chosen

$$z = \frac{1}{7633988641}\,\sqrt{\frac{4\,X + 39141876845580405121}{d_1}};$$
$$w = \frac{4}{58711203558519893569}\,\frac{2\,Y + X}{\sqrt{d_1\,(4\,X + 39141876845580405121)}}.$$

If $d_2 = \widehat{\delta}(P)$ is the image of some $\mathbb{Q}$-rational point $P = (X : Y : 1)$ on E, then (z, w) is a $\mathbb{Q}$-rational point on $\widehat{C}_{d_2}$, where we have chosen

$$z = \frac{1}{14193792}\,\sqrt{\frac{X - 4892734605697550640}{d_2}};$$
$$w = \frac{1}{108758174363395200}\,\frac{2\,Y + X}{\sqrt{d_2\,(X - 4892734605697550640)}}.$$

If $d_1 = \delta'(P)$ is the image of some $\mathbb{Q}$-rational point $P = (X : Y : 1)$ on E'', then (z, w) is a $\mathbb{Q}$-rational point on C'_{d_1}, where we have chosen

$$z = \frac{1}{8623536769}\,\sqrt{\frac{4\,X + 40011942240487566721}{d_1}};$$
$$w = \frac{4}{58277782570917026881}\,\frac{2\,Y + X}{\sqrt{d_1\,(4\,X + 40011942240487566721)}}.$$

If $d_2 = \widehat{\delta}'(P)$ is the image of some $\mathbb{Q}$-rational point $P = (X : Y : 1)$ on E', then (z, w) is a $\mathbb{Q}$-rational point on $\widehat{C}'_{d_2}$, where we have chosen

$$z = \frac{1}{466386480}\sqrt{\frac{X - 5001492780060945840}{d_2}};$$

$$w = \frac{1}{3586868261390902320}\,\frac{2\,Y + X}{\sqrt{d_2\,(X - 5001492780060945840)}}.$$

Third, we show that the images of δ, $\widehat{\delta}$, δ', and $\widehat{\delta}'$ are finite groups.

Lemma 8. *Fix $k = p/q$ for integers p and q. Fix a square-free integer d, and consider*

$$C_d : \quad dw^2 = (1 \pm dz^2)(1 \pm dk^2z^2).$$

If $C_d(\mathbb{Q}) \neq \emptyset$, then any prime ℓ dividing d must also divide pq.

Proof of Lemma. Suppose ℓ is a prime that divides d but does not divide pq. We will find a contradiction.

Let $(z, w) \in C_d(\mathbb{Q})$, and write $z/q = x_1/x_0$ for some relatively prime integers x_1 and x_0. Denote $x_2 = wx_0^2$ so that

$$dx_2^2 = (x_0^2 \pm dq^2x_1^2)(x_0^2 \pm dp^2x_1^2).$$

Since the right-hand side of this equation is an integer and d is square-free, we see that x_2 is also an integer. From the identity

$$x_0^4 = d(x_2^2 \mp (p^2 + q^2)x_0^2x_1^2 \mp dp^2q^2x_1^2),$$

we see that ℓ divides x_0. Since ℓ divides both $(x_0^2 \pm dq^2x_1^2)$ and $(x_0^2 \pm dp^2x_1^2)$, we see that ℓ^2 divides dx_2^2. As ℓ divides d and d is square-free, ℓ must divide x_2. From the identity

$$d^2p^2q^2x_1^4 = dx_2^2 \mp d(p^2 + q^2)x_0^2x_1^2 \mp x_0^4,$$

we see that ℓ^3 divides $d^2p^2q^2x_1^4$. As ℓ does not divide pq, ℓ must divide x_1. This shows that ℓ divides both x_1 and x_2, which is a contradiction. □

Using this lemma, we see that the images of δ, $\widehat{\delta}$, δ', and $\widehat{\delta}'$ must be contained in the groups $\Gamma(k)$, $\Gamma(\kappa)$, $\Gamma(\kappa')$, and $\Gamma(k')$, respectively. □

Corollary 9. *The Mordell-Weil group of the elliptic curve*

$$E : \begin{aligned} Y^2 + XY &= X^3 - 7181359868024838434108428477109624412 0\,X \\ &\quad + 2342384302041141813702521859646228641128533374139589904 00 \end{aligned}$$

is $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$, where $r \leq 3$.

Proof. Using $t = 9/296$ in Proposition 4, we find the curve E as above. Hence, $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$, so $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq {Z_2}^{r+2}$, where r is the Mordell-Weil rank. Using Proposition 3 and Theorem 5,

$$2^{r+2} = \left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = \left|\delta\left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right)\right| \cdot \left|\widehat{\delta}\left(\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))}\right)\right|.$$

Using the software package `mwrank`, we find that

$$\delta\left(\frac{E'(\mathbb{Q})}{\phi\big(E(\mathbb{Q})\big)}\right) = \{1\} \qquad \text{and} \qquad \widehat{\delta}\left(\frac{E(\mathbb{Q})}{\hat{\phi}\big(E'(\mathbb{Q})\big)}\right) \subseteq \langle -1,\, 6477590,\, 2,\, 7,\, 37\rangle.$$

The notation $\langle S \rangle$ signifies the set generated by S. Putting all of this together, $2^{r+2} \leq 2^5$ so that $r \leq 3$. $\square$

5. Results

Recall from the previous section that we have the elliptic curve

$$\begin{aligned} E: \quad & Y^2 + X\,Y = X^3 - 7181359868024838434108428477109624412 0\,X \\ & + 2342384302041141813702521859646228641128533374139589904 00. \end{aligned}$$

From Corollary 9, we know that the Mordell-Weil group is $Z_2 \times Z_8 \times \mathbb{Z}^r$, where the rank $r \leq 3$. We explain why the rank is exactly 3.

First we give a bound on the rank r. The authors in [6] found the following four $\mathbb{Q}$-rational independent points on E:

$$P_1 = (4892533141966211376 : -2446266570983105688 : 1);$$

$$P_2 = (6793371071343566640 : 773920780858934092533330468 0 : 1);$$

$$\begin{aligned} P_3 = \big(& \tfrac{125691121567490117748583092936844134429 0}{16027875241^2} \\ & : \tfrac{786698395807855729596742215337306893212760400533639780}{16027875241^3} \ : \ 1\big); \end{aligned}$$

$$\begin{aligned} P_4 = \big(& \tfrac{419146355190134411415222739650581610769161840}{9255646526131^2} \\ & : \tfrac{10521138619277846984948896723190385415707300564677361287998 1880}{9255646526131^3} \ : \ 1\big). \end{aligned}$$

The torsion subgroup is generated by P_1 and P_2, and the points P_3 and P_4 have infinite order. This shows that $2 \leq r \leq 3$.

Here we note that we may use the conjecture of Byran Birch and H. P. F. Swinnerton-Dyer to determine the exact value of r; see [11] for more information. Using software such as `MAGMA` [1], we compute that the (global) root number is $w_E = -1$. The (weak) Birch and Swinnerton-Dyer Conjecture asserts that $w_E = (-1)^r$, so we see that r must be odd. We conclude that $r = 3$.

We explain another method to determine the value of the rank r without assuming the (weak) Birch and Swinnerton-Dyer Conjecture. Using Theorem 5, we may compute r by counting the number of elements in the image of the connecting homomorphism $\widehat{\delta}$. Using Corollary 9, the image is contained in $\langle -1,\, 6477590,\, 2,\, 7,\, 37 \rangle$. The idea is to show that this is precisely the image. To do this, it is sufficient to find a $\mathbb{Q}$-rational point (z, w) on the homogeneous space

$$\widehat{C}_{d_2}: \qquad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, \kappa^2\, z^2\right) \quad \text{where} \quad \kappa = \left(\frac{2t}{t^2 - 1}\right)^2,$$

determined by each generator $d_2 \in \{-1,\, 6477590,\, 2,\, 7,\, 37\}$. Recall that $t = 9/296$. Winding through the proof of Theorem 5, we find that there is a "2-covering map" $\widehat{\psi} : \widehat{C}_{d_2} \to E$ which sends a $\mathbb{Q}$-rational point (z, w) to a $\mathbb{Q}$-rational point $(X : Y : 1)$ in terms of

$$X = 4892734605697550640 + 201463731339264\, d_2\, z^2;$$

$$\begin{aligned} Y = & -2446367302848775320 \\ & - 100731865669632\, d_2\, z^2 + 771845452606881941299200\, d_2\, w\, z. \end{aligned}$$

From this map, we can use $\mathbb{Q}$-rational points (z, w) on $\widehat{C}_{d_2}$ to generate $\mathbb{Q}$-rational points P on E. Recall the "2-cover" of E:

TABLE 2. $\mathbb{Q}$-Rational Points on $\widehat{C}_{d_2}$

P on E	$d_2 = \widehat{\delta}(P)$	Point (z, w) on $\widehat{C}_{d_2}$
P_1	-1	$(1, 0)$
P_2	6477590	$\left(\frac{305}{7992}, \frac{8143806511}{200779379640}\right)$
P_3	2	$\left(\frac{116263507795895}{683172154272384}, \frac{11901847559384869074692786 1139}{16364473195892047458106771 0080}\right)$
P_4	7	$\left(\frac{9477908247062185}{147942254073677904}, \frac{28029307774484843020068373773711050 71}{73115686663783979123491473344662202 40}\right)$

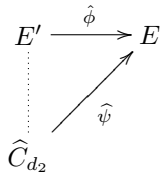


Table 2 contains information about the four known $\mathbb{Q}$-rational points on E, where the points (z, w) were chosen such that $P = \widehat{\psi}((z, w))$. Note that there are roughly half as many digits for (z, w) as there are for P.

Using the same ideas as in Corollary 9, `mwrank` [4] shows that the image of δ' is trivial, while the image of $\widehat{\delta}'$ is contained in $\langle -1,\ 6477590,\ 2,\ 3,\ 7,\ 37,\ 41\rangle$. We wish to find a $\mathbb{Q}$-rational point (z, w) on the homogeneous space

$$\widehat{C}'_{d_2}: \qquad d_2\, w^2 = \left(1 + d_2\, z^2\right)\left(1 + d_2\, k'^2\, z^2\right) \quad \text{where} \quad k' = \frac{4(t^3 - t)}{(t^2 + 1)^2},$$

determined by each generator $d_2 \in \{-1,\ 6477590,\ 2,\ 7,\ 37\}$. Similar to above, winding through the proof of Theorem 6, we find that there is another "2-covering map" $\widehat{\psi}' : \widehat{C}'_{d_2} \to E'$ which sends a $\mathbb{Q}$-rational point (z, w) to a $\mathbb{Q}$-rational point $(X : Y : 1)$ in terms of

$$X = 5001492780060945840 + 217516348726790400\, d_2\, z^2;$$

$$Y = -2500746390030472920 - 108758174363395200\, d_2\, z^2 + 836433431326911418524316800\, d_2\, w\, z.$$

From this map, we can use $\mathbb{Q}$-rational points (z, w) on $\widehat{C}'_{d_2}$ to generate $\mathbb{Q}$-rational points P' on E'. Since δ is trivial, we see that $P' = \phi(P)$ for some P on E. Recall the "4-cover" of E:

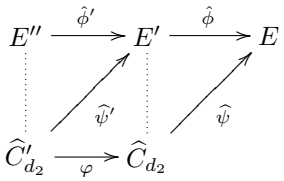


TABLE 3. $\mathbb{Q}$-Rational Points on $\widehat{C}'_{d_2}$

P' on E'	$d_2 = \widehat{\delta}'(P')$	Point (z, w) on $\widehat{C}'_{d_2}$
$\phi(P_1)$	-1	$\left(\frac{7690763809}{932772960},\ 0\right)$
$\phi(P_2)$	6477590	$\left(\frac{87697}{77731080},\ \frac{8623536769}{6816782522760}\right)$
$\phi(P_3)$	2	$\left(\frac{402721445539793209371967}{16689898742884224439568},\ -\frac{5467902969717297003714479983890732441446673297 63}{5319738216468998004248404711869988353017875184}\right)$
$\phi(P_4)$	7	$\left(\frac{14342982753770410499165500614 61}{78309867527655769246487587761},\ -\frac{4585213515870604645282106468737128527203408327078951513006492 4}{4198252795330174148975189867794797875973780167926165981777 77}\right)$

We define the map $\varphi : \widehat{C}'_{d_2} \to \widehat{C}_{d_2}$ via the composition $\widehat{\psi}' = \phi \circ \widehat{\psi} \circ \varphi$. Table 3 contains information about the four known $\mathbb{Q}$-rational points on E', where the points (z, w) were chosen such that $P' = \widehat{\psi}'\left((z, w)\right) = \phi(P)$.

Using our "2-cover", we seek a point P_5 such that $d_2 = \widehat{\delta}(P_5) = 37$. To be more precise, we seek a $\mathbb{Q}$-rational point (z, w) on the curve

$$\widehat{C}_{37}: \qquad 37\,w^2 = \left(1 + 37\,z^2\right)\left(1 + 37\,\kappa^2\,z^2\right) \quad \text{where} \quad \kappa = \frac{28387584}{7662376225}.$$

Alternatively, using our "4-cover", we seek a point $P'_5 = \phi(P_5)$ such that $d_2 = \widehat{\delta}'(P'_5) = \widehat{\delta}(P_5) = 37$. To be more precise, we seek a $\mathbb{Q}$-rational point (z, w) on the curve

$$\widehat{C}'_{37}: \qquad 37\,w^2 = \left(1 + 37\,z^2\right)\left(1 + 37\,k'^2\,z^2\right) \quad \text{where} \quad k' = \frac{932772960}{7690763809}.$$

We used John Cremona's algorithm `QuarticMinimise()` to find "minimal" integral models for $\widehat{C}_{37}$ and $\widehat{C}'_{37}$. That is, upon substituting

$$Z = \frac{28387584}{7662376225}\,z \qquad \text{and} \qquad W = 28387584\,w$$

we find the integral model

$$\widehat{C}_{37}: \quad \begin{aligned} W^2 &= 2172344348297474273125\,Z^4 \\ &\quad + 58712815268370607681\,Z^2 + 21779862847488; \end{aligned}$$

and similarly, upon substituting

$$Z = 932772960\,z \qquad \text{and} \qquad W = \frac{932772960}{7690763809}\,w$$

we find the integral model

$$\widehat{C}'_{37}: \quad \begin{aligned} W^2 &= 2188470374735494973797\,Z^4 \\ &\quad + 60017913360731350081\,Z^2 + 23515280943436800. \end{aligned}$$

We then ran Michael Stoll's program `ratpoints` [14] to find rational points on each curve. We used both Miami University's 128-node high-powered computing cluster, RedHawk, and Purdue University's Euler. After a week of computing time, we have yet to find any rational points.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Terris D. Brooks, Elizabeth A. Fowler, Katherine C. Hastings, Danielle L. Hiance, and Matthew A. Zimmerman. Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$: Does a Rank 4 Curve Exist? *SUMSRI Journal*, 2006.

[3] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[4] John Cremona. `mwrank` and related programs for elliptic curves over $\mathbb{Q}$. `http://www.maths.nott.ac.uk/personal/jec/mwrank/`, 2006.

[5] Andrej Dujella. High rank elliptic curves with prescribed torsion. `http://www.math.hr/~duje/tors/tors.html`, 2007.

[6] Jessica Flores, Kimberly Jones, Anne Rollick, James Weigandt. A Statistical Analysis of 2-Selmer Groups for Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$. *SUMSRI Journal*, 2007.

[7] Edray Herber Goins. SUMSRI Number Theory Research Seminar Lecture Notes. In preparation, 2008.

[8] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[9] L. J. Mordell. *Diophantine equations*. Academic Press, London, 1969.

[10] Henri Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de mathématiques pures et appliquées*, 7(5):161–233, 1901.

[11] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474 (electronic), 2002.

[12] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York-Berlin, 1986.

[13] John Stillwell. Elliptic curves. *Amer. Math. Monthly*, 102(9):831–837, 1995.

[14] Michael Stoll. `ratpoints-2.0.1`. `http://www.faculty.iu-bremen.de/stoll/programs/index.html/`, 2008.

Morehouse College, Atlanta, GA 30314
E-mail address: `samj_ivy@yahoo.com`

Morgan State University, Baltimore, MD 21251
E-mail address: `brjef1@mymail.morgan.edu`

North Carolina Central University, Durham, NC 27707
E-mail address: `mjosey@mail.nccu.edu`

Spelman College, Atlanta, GA 30314
E-mail address: `c1_outing@earthlink.net`

Grand Valley State University, Allendale, MI 49401
E-mail address: `taylocli@student.gvsu.edu`

Shawnee State University, Portsmouth, OH 45662
E-mail address: `whites2@shawnee.edu`