4-Covering Maps on Elliptic Curves with Torsion Subgroup $Z_2 \times Z_8$

Samuel Ivy (Morehouse College), Brett Jefferson (Morgan State University), Michele Josey (North Carolina Central)
Cheryl Outing (Spelman College), Clifford Taylor (Grand Valley State), Staci White (Shawnee State University)

Abstract

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 show that the Mordell-Weil group is

$$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$$

thereby proving a conjecture of Flores-Jones-Rollick-Weigandt and Rathbun.

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 (3) that this bound is obtained when

$$t = \frac{9}{296}.$$

One knows that $r \geq 2$ for this particular t. We focus on determining the exact rank of this particular elliptic curve.

Acknowledgements

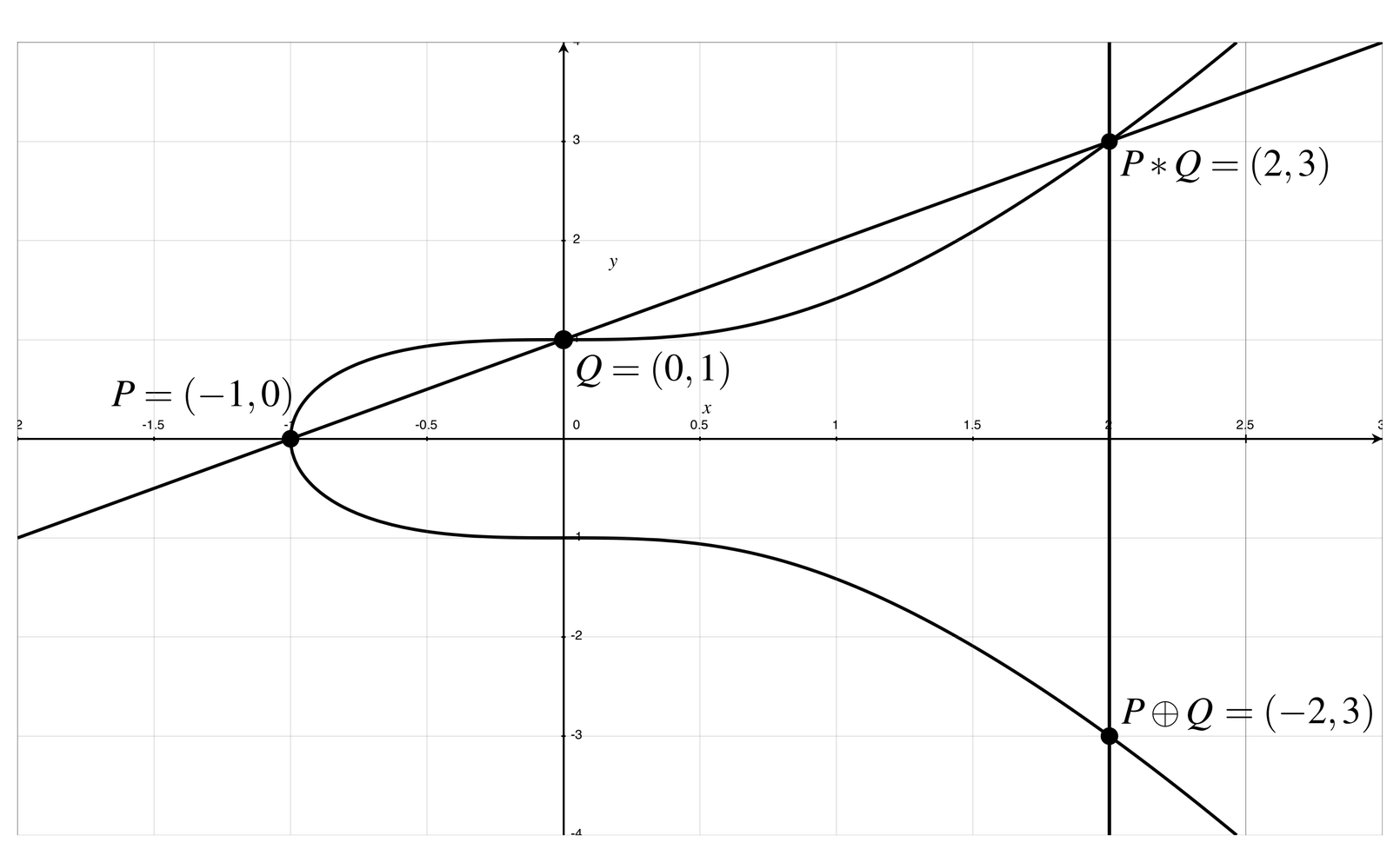
The authors would like to thank the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI) at Miami University for the opportunity to conduct this research. They would also like to thank the National Science Foundation and the National Security Agency for their funding, as well as Residential 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.

The Group Law for Elliptic Curves

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" $\mathcal{O}$.



The Group Law on an Elliptic Curve

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 the figure above. 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 (8).

Poincaré's Conjecture

In 1901, Henri Poincaré conjectured (7) that this abelian group is finitely generated. This was proved by Louis Mordell in 1922.

Theorem 1 (Mordell, (6)). 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

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

Mordell-Weil Group

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.

Mazur's Theorem

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, (5)). 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 curves with torsion subgroup $Z_2 \times Z_8$.

Example

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

has torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ generated by

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

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

Rank Records with Prescribed Torsion

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 (2) has a listing of the largest known ranks among families of elliptic curves with prescribed torsion. The table below contains this information.

Note that the highest known rank for elliptic curves E with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ is $r = 3$.

Torsion Subgroup	Highest Known Rank	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)

m-Isogenies and Quotient Groups

Mordell's proof (6) 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,

$$E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2m} \qquad \Longrightarrow \qquad \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq Z_2^{r+2},$$

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

(i) the coordinates of ϕ involve rational functions with $\mathbb{Q}$-rational coefficients, and

(ii) there are exactly m points in the kernel $E(\mathbb{Q})[\phi]$ of the map.

We will be interested in the case where $m = 2$.

Counting Cosets to Determine the Rank

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,

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

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

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

Using the assumption above, Lagrange's Theorem and the First Isomorphism Theorem imply the equalities:

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

□

If $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2m}$, then $E'(\mathbb{Q})[\hat{\phi}] = \phi(E(\mathbb{Q})[2])$ holds.

2-Isogenies for Quartic Models

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

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

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

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

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

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

(iii) 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

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

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

Example

We focus on the case where $t = 9/296$, which was first considered in (3). Weierstrass models are as follows:

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

$$E': \quad \begin{aligned} &Y^2 + X\,Y = X^3 - 7182838410586195768223026686032504412 0\,X \\ &\quad + 2341371525751308852524074565174235775172724198311084304 00;\end{aligned}$$

$$E'': \quad \begin{aligned} &Y^2 + X\,Y = X^3 - 8791041401157870064556943644005177212 0\,X \\ &\quad + 1215293335280977803803190858716511058206567605433869568 00.\end{aligned}$$

2-Covering Maps

Theorem 5. Using $\phi : E \to E'$ and $\hat{\phi} : E' \to E$, define the **connecting homomorphisms**:

$$\delta : \quad \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}, \qquad (X:Y:1) \longmapsto 4X + 39141876845580405121;$$

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

Both δ and $\widehat{\delta}$ are injective group homomorphisms with finite images. To be more 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. Then

$$\delta\left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right) = \left\{ d_1 \equiv \pm \prod_{\ell \in \Sigma(k)} \ell^{e(\ell)} \;\middle|\; \begin{array}{l} C_{d_1} :\ d_1\,w^2 = (1-d_1\,z^2)\,(1-d_1\,k^2\,z^2) \\ \text{has a } \mathbb{Q}\text{-rational point } (z,w) \end{array} \right\};$$

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

Here, $e(\ell)$ is either 0 or 1.

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.

4-Covering Maps

Theorem 6. Using $\phi' : E' \to E''$ and $\hat{\phi}' : E'' \to E'$, define the **connecting homomorphisms**:

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

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

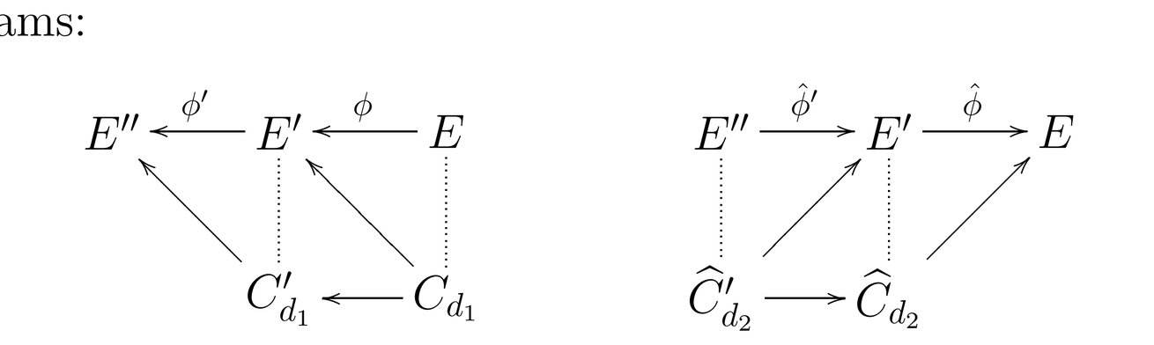
Both δ' and $\widehat{\delta}'$ are injective group homomorphisms with finite images. To be precise, let $\Sigma(\kappa') = \{82207, 92863\}$ and $\Sigma(k') = \{2,3,5,7,37,41,61,87697\}$ be the set of primes dividing $\kappa' = (1-k')/(1+k')$ and k', respectively, as in Theorem 4. Then

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

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

Here, $e(\ell)$ is either 0 or 1.

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 the elliptic curve E (E', respectively) will correspond to a $\mathbb{Q}$-rational point on the **homogeneous space** $\widehat{C}_{d_2}$, ($\widehat{C}'_{d_2}$, respectively) having half as many digits.

Proof of Main Result

By Theorem 4, the Mordell-Weil group of the elliptic curve

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

is $Z_2 \times Z_8 \times \mathbb{Z}^r$ for some r. It suffices to show that the rank $r = 3$. Using Cremona's `mwrank` (1) we find that

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

so by Proposition 3 and Theorem 5,

$$2^{r+2} = \left|\frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})}\right| = \left|\delta\left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right)\right| \left|\widehat{\delta}\left(\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))}\right)\right| \leq 2^5.$$

The authors in (3) found the following two $\mathbb{Q}$-rational points:

$$P_3 = \left(\frac{125691121567490117748583092936844134429 0}{16027875241^2} : \frac{786698395807855729596742215337306893212760400533639780}{16027875241^3} : 1\right);$$

$$P_4 = \left(\frac{4191463551901344114152227396505816107691618 40}{9255646526131^2} : \frac{105211386192778469849488967231903854157073005646773612879981880}{9255646526131^3} : 1\right).$$

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

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	$\left(\frac{116263507795895}{683172154272384}, \frac{119018475593848690746927861139}{163644731958920474581067710080}\right)$
P_4	7	$\left(\frac{9477908247062185}{147942254073677904}, \frac{280293077744848430200683737737110507 1}{731156866637839791234914733446622024 0}\right)$

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	$\left(\frac{40272144553979320937196 7}{166898987428842244395 68}, -\frac{546790296971729700371447998389073244144667329763}{531973821646899800424840471186998835301787518 4}\right)$
$\phi(P_4)$	7	$\left(\frac{1434298275377041049916550061461}{783098675276557692464875877 61}, -\frac{45852135158706046452821064687371285272034083270789515130064924}{41982527953301741489751898677947978759737801679261659817777 7}\right)$

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

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

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

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

We used John Cremona's algorithm `QuarticMinimise()` to find "minimal" integral models for $\widehat{C}_{37}$ and $\widehat{C}'_{37}$ then Michael Stoll's program `ratpoints` (9) to find rational points. We are running these on both Miami University's 128-node high-powered computing cluster, RedHawk, and Purdue University's Euler. □

REFERENCES

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

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

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.

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

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

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

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

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

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

This poster was prepared with Brian Wolven's Poster LaTeX macros v2.1.