ELLIPTIC CURVES WITH TORSION SUBGROUP $Z_2 \times Z_8$: DOES A RANK 4 CURVE EXIST?

TERRIS D. BROOKS, ELIZABETH A. FOWLER, KATHERINE C. HASTINGS, DANIELLE L. HIANCE, AND MATTHEW A. ZIMMERMAN

Abstract. We consider elliptic curves over $\mathbb{Q}$ with torsion subgroup $Z_2 \times Z_8$. These curves are birationally equivalent to $y^2 = (1-x^2)(1-k^2x^2)$ where $k = (t^4 - 6t^2 + 1)/(t^2+1)^2$ for some rational number t. The largest known rank for such curves is 3. In this paper we search for a curve of rank at least 4 by computing ranks for $t = a/b$ with $|a|, |b| \leq 2000$.

1. Introduction

An elliptic curve is an object with two distinguishing features. First, such a curve has an equation that allows us to determine which of the solution points have rational coordinates. Second, its points form an abelian group so that one can ask about its algebraic structure. These two features complement one another. That is, given a few rational points one can find more such points using the group structure. Conversely, one can define the group structure by drawing lines through rational points.

If E is an elliptic curve over $\mathbb{Q}$, then the set $E(\mathbb{Q})$ of rational points forms a finitely generated abelian group. This means that there exists a finite group $E(\mathbb{Q})_{\text{tors}}$ and nonnegative integer r such that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$. This integer r is called the (Mordell-Weil) rank. Every such elliptic curve with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ is birationally equivalent to

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

for some rational number t. Currently, the highest known rank for this torsion subgroup is $r = 3$, and the known curves with this rank correspond to $t = \frac{5}{29}$, $\frac{18}{47}$, $\frac{15}{76}$, $\frac{47}{219}$, $\frac{19}{220}$, $\frac{87}{407}$, $\frac{143}{419}$, and $\frac{145}{444}$.

The goal of this project is to search for a curve with torsion subgroup $Z_2 \times Z_8$ and rank $r \geq 4$. To find such a curve, we use the following algorithm:

(1) Generate a list of candidate curves with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$.
(2) Compute the 2-Selmer ranks of these curves as upper bounds on the Mordell-Weil ranks.
(3) Use these upper bounds to reduce the list of candidate curves.
(4) Compute the Mordell-Weil ranks of the curves in the reduced list.

We generated a list of curves for $t = \frac{a}{b}$ with $|a|, |b| \leq 2000$. This yielded a list of 503955 curves. We distributed the computations over 32 processors on the high-powered computing cluster at Miami University and then eliminated those curves

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

Key words and phrases. Elliptic curves, Rank, Selmer group.

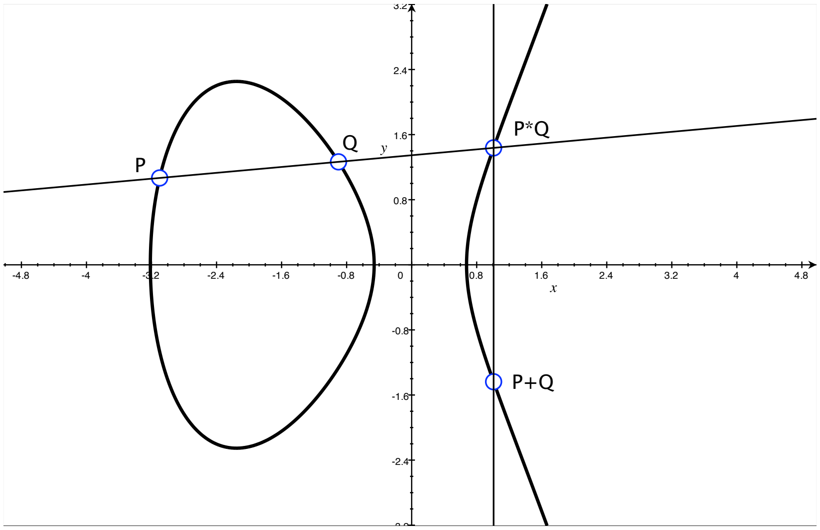

Figure 1. The Group Law on an Elliptic Curve

with 2-Selmer rank at most 3. This minimized our search space to only 17666 curves. After one week of computing time, we found 15 curves with Mordell-Weil rank $r \geq 2$; however, we could not determine whether any of these curves have rank 4.

The authors would like to thank the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI) at Miami University, the National Science Foundation, and the National Security Agency for their funding and this research opportunity. They would also like to thank Andrej Dujella for helpful conversations and William Stein for use of his computer at the University of Washington.

2. Foundations

An elliptic curve is a curve that is birationally equivalent to

$$E : Y^2 = X^3 + AX + B,$$

where $4A^3 + 27B^2 \neq 0$. We are interested in the case where A and B are integers. Viewed as a subset of projective space, we consider the set $E(\mathbb{Q})$ of rational points joined with the point at infinity $\mathcal{O}$. Let $P, Q \in E(\mathbb{Q})$ and denote $P * Q$ as the third point of intersection of E and the line through P and Q. Now, define $P \oplus Q = (P * Q) * \mathcal{O}$, i.e., the reflection of $P * Q$ about the x-axis. See Figure 1 for this geometry. The set $E(\mathbb{Q})$ under the operation $\oplus$ forms an abelian group with identity element $\mathcal{O}$ and inverses $[-1]P = P * \mathcal{O}$.

In 1901, Henri Poincaré [6] conjectured that the abelian group $E(\mathbb{Q})$ is finitely generated. Louis Mordell proved this in 1922.

Theorem 1 (Mordell, [5])**.** *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*

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

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	12	Eroshkin (2006)
Z_4	12	Elkies (2006)
Z_5	6	Dujella - Lecacheux (2001)
Z_6	7	Dujella (2001, 2006)
Z_7	5	Dujella - Kulesz (2001)
Z_8	6	Elkies (2006)
Z_9	3	Dujella (2001) MacLeod (2004)
Z_{10}	4	Dujella (2005) Elkies (2006)
Z_{12}	3	Dujella (2001, 2005, 2006) Rathbun (2003)
$Z_2 \times Z_2$	14	Elkies (2005)
$Z_2 \times Z_4$	8	Elkies (2005)
$Z_2 \times Z_6$	6	Elkies (2006)
$Z_2 \times Z_8$	3	Connell (2000) Dujella (2000, 2001, 2006) Campbell - Goins (2003) Rathbun (2003)

This nonnegative integer r is called the (Mordell-Weil) rank of E. The torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is the set of points of finite order. Barry Mazur completely classified the structure of this subgroup in 1977.

Theorem 2 (Mazur, [4])**.** *If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups:*

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

In this paper, we focus specifically on curves with torsion subgroup $Z_2 \times Z_8$.

In contrast to the torsion subgroup, the rank is not well understood. It is widely believed that for each of the torsion subgroups T given in Mazur's Theorem, the ranks of elliptic curves E with $E(\mathbb{Q})_{\text{tors}} \simeq T$ are unbounded. In attempting to verify this belief, one approach is to assume there is an absolute bound $B(T)$, and then search for a curve with torsion subgroup T and rank r greater than this bound. Since March 2001, Andrej Dujella [2] has been tracking the lower bounds of $B(T)$ by recording the highest known rank for each T. Table 1 summarizes the current records. The highest known rank for $T \simeq Z_2 \times Z_8$ is $r = 3$.

3. Objective

The aim of this paper is to examine the ranks of curves with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. To do so we must first classify these curves. The following theorems form a basis for the focus of this project.

Theorem 3 (Goins, [3]). *Fix a rational number $k \neq -1, 0, 1$ and consider the curve*

$$E : y^2 = (1 - x^2)(1 - k^2x^2).$$

(i) *E is an elliptic curve.*
(ii) *Its torsion subgroup is either $Z_2 \times Z_4$ or $Z_2 \times Z_8$.*
(iii) *Any elliptic curve over $\mathbb{Q}$ with torsion subgroup $Z_2 \times Z_4$ or $Z_2 \times Z_8$ is birationally equivalent to E for some rational number k.*

For example, in 2006, Dujella [2] discovered the elliptic curve

$$(*) \quad \begin{aligned} E : Y^2 + XY = X^3 &- 15343063417941874422081256126489574987160X \\ &+ 486503741336910955243717595559583892156442731284430865537600 \end{aligned}$$

with Modell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$. This curve is birationally equivalent to the quartic curve in the statement of Theorem 3 when $k = \frac{14435946721}{47594221921}$. This can be seen by using the substitutions

$$X = -\frac{6240(4083958238540477x + 3711823331862791 8)}{x - 1} \qquad \text{and}$$

$$Y = \frac{1560}{(x-1)^2}\begin{pmatrix} 8167911647708095 4x^2 + 6606855016017488 2x \\ + 196098624860342514999738 6795y - 7423646663725583 6 \end{pmatrix}.$$

Theorem 3 establishes a birational equivalence between curves E with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_4$ or $Z_2 \times Z_8$ and rational numbers k. To distinguish between the two cases, further restrictions may be placed upon k. The following theorem utilizes this idea to classify curves with torsion subgroup $Z_2 \times Z_8$.

Theorem 4 (Goins, [3]). *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*

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

(ii) *Moreover, upon writing $k = \frac{p}{q}$ for some integers p and q, the quartic curve above is birationally equivalent to the cubic curve*

$$Y^2 = X^3 - 27(p^4 + 14p^2q^2 + q^4)X - 54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6).$$

Proof. We will show part (ii) since (i) is shown in [3]. Given a point (x, y) on the quartic curve, the substitutions

$$X = \frac{3(5p^2 - q^2)x + 3(5q^2 - p^2)}{x - 1} \quad \text{and} \quad Y = \frac{54q(p^2 - q^2)y}{(x - 1)^2}$$

yield a point (X, Y) on the cubic curve. Conversely, given a point (X, Y) on the cubic curve, the subsitutions

$$x = \frac{X - 3(5q^2 - p^2)}{X - 3(5p^2 - q^2)} \quad \text{and} \quad y = \frac{6(p^2 - q^2)Y}{q(X - 3(5p^2 - q^2))^2}$$

yield a point (x, y) on the quartic curve. □

We consider the family of elliptic curves $E : y^2 = (1 - x^2)(1 - k^2x^2)$, where $k = \frac{t^4-6t^2+1}{(t^2+1)^2}$. Currently, there are eight known curves with Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$. They correspond to the following values of t:

$$\frac{5}{29}, \quad \frac{18}{47}, \quad \frac{15}{76}, \quad \frac{47}{219}, \quad \frac{19}{220}, \quad \frac{87}{407}, \quad \frac{143}{419}, \quad \frac{145}{444}.$$

Specifically, Dujella's curve of rank 3 in equation (∗) is birationally equivalent to the quartic curve in the statement of Theorem 4 when $t = \frac{145}{444}$. Our main focus is to find a curve with the torsion subgroup $Z_2 \times Z_8$ and a rank of 4 or higher.

4. Algorithm

To search for a curve with torsion subgroup $Z_2 \times Z_8$ and rank $r \geq 4$, we use the following algorithm:

(1) Generate a list of candidate curves with $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$.
(2) Compute the 2-Selmer ranks of these curves as upper bounds on the Mordell-Weil ranks.
(3) Use these upper bounds to reduce the list of candidate curves.
(4) Compute the Mordell-Weil ranks of the curves in the reduced list.

Here we discuss these steps in further detail and describe our results.

Step 1: Generate a List of Candidate Elliptic Curves. According to Theorem 4, every elliptic curve E with torsion subgroup $Z_2 \times Z_8$ is birationally equivalent to the quartic $y^2 = (1-x^2)(1-k^2x^2)$, where $k = \frac{t^4-6t^2+1}{(t^2+1)^2}$ for some rational number t. We generate a list of candidate curves based on the integer values a and b where $t = \frac{a}{b}$. A pseudocode for our algorithm is as follows.

```
(1) Input: Integer bound
(2) For integers $a$ and $b$ within this bound
    (i) Denote $t = \frac{a}{b}$ and $k = \frac{p}{q}$ in terms of the following integers
        $p = a^4 - 6a^2b^2 + b^4$        $A = -27(p^4 + 14p^2q^2 + q^4)$
        $q = (a^2 + b^2)^2$              $B = -54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6)$
    (ii) Record the elliptic curve $Y^2 = X^3 + AX + B$
(3) Output: List of elliptic curves
```

By considering symmetries of the expression $k = \frac{t^4-6t^2+1}{(t^2+1)^2}$, we can eliminate redundant curves from the list. The following result helps to decrease the runtime significantly.

Proposition 5. *Fix a rational number $k \neq -1, 0, 1$ and consider the curve*

$$E : y^2 = (1 - x^2)(1 - k^2x^2).$$

(i) *E is birationally equivalent to*

$$E' : Y^2 = (1 - X^2)\left(1 - \frac{1}{k^2}X^2\right).$$

In particular, we may assume that $0 < k < 1$.

(ii) *Suppose that $k = \frac{t^4-6t^2+1}{(t^2+1)^2}$ for some $t = \frac{a}{b}$. We can choose integers a and b such that $0 < (1 + \sqrt{2})a < b$.*

Proof. First we will show (i). Given a point (x, y) on E, the point $(X, Y) = (kx, y)$ is on E'. Conversely, given a point (X, Y) on E', the point $(x, y) = (\frac{1}{k}X, Y)$ is on E. Therefore, E and E' are birationally equivalent. It is clear that we may choose $k > 0$. If $k < 1$ we are done. If $k > 1$ then $\frac{1}{k} < 1$, and because E is equivalent to E' we are done.

Next we will show (ii). Write $k = \frac{a^4-6a^2b^2+b^4}{(a^2+b^2)^2}$. It is clear that we may assume $0 \leq a \leq b$. If $a = 0$ then $k = 1$. If $a = b$ then $k = -1$. Therefore, we may assume $0 < a < b$. The mapping ϕ: $(a, b) \mapsto (b - a, b + a)$ sends k to $-k$; ϕ is an involution since ϕ^2 is the identity. Denote $c = b - a$ and $d = b + a$. By assumption, $0 < a < b$, hence $0 < c < d$. Assume for the moment that $(1 + \sqrt{2})c > d$. This implies

$$\frac{b-a}{b+a} = \frac{c}{d} > \frac{1}{1+\sqrt{2}} \qquad \Longrightarrow \qquad (b - a)(1 + \sqrt{2}) > b + a.$$

After a bit of algebra we find

$$b\sqrt{2} > a(2 + \sqrt{2}) \qquad \Longrightarrow \qquad \frac{a}{b} < \frac{1}{1+\sqrt{2}}.$$

Hence $0 < (1 + \sqrt{2})a < b$, so we are done. On the other hand, if $(1 + \sqrt{2})c < d$ then we choose c and d instead of a and b. □

We implemented the pseudocode above using `Maple`. For a bound of 2000, in other words, $0 < (1 + \sqrt{2})a < b < 2000$, `Maple` generated 503955 curves in about four minutes. We recorded the elliptic curves $Y^2 = X^3 + AX + B$ in the form $[0, 0, 0, A, B]$ for processing in Step 2.

Step 2: Determine the 2-Selmer Ranks. We list some results from Galois cohomology. For an elliptic curve E defined over $\mathbb{Q}$, there is a well-known short exact sequence

$$0 \longrightarrow \frac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \longrightarrow \mathrm{Sel}^{(2)}(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})$$

where $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$ is the 2-Selmer group and $\text{Ш}(E/\mathbb{Q})$ is the Shafarevich-Tate group. The three nontrivial objects above are abelian groups; the first two are known to be finite. In fact, if E has Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^r$, then we have

$$\left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = 2^{r+2} \qquad \text{and} \qquad \left|\mathrm{Sel}^{(2)}(E/\mathbb{Q})\right| = 2^{s+2},$$

where r is the "Mordell-Weil" rank and s is the "2-Selmer" rank. Note that $r \leq s$. In particular, the number of elements of order two in the Shafarevich-Tate group is $|\text{Ш}(E/\mathbb{Q})[2]| = 2^{s-r}$. It is conjectured that this number is a perfect square, i.e., r and s are either both even or both odd. For more information, consult [8].

We used Cremona's `mwrank` to compute the ranks of the candidate elliptic curves from Step 1. We utilized the `-s` option in `mwrank` to compute the 2-Selmer ranks. We are initially interested in the 2-Selmer rank rather than the Mordell-Weil rank because it provides an upper bound on the Mordell-Weil rank, and can be computed by `mwrank` relatively quickly.

Miami University has a 128-node high-powered computing cluster known as RedHawk. We divided our list of 503955 candidate curves into 32 separate files of about 15750 curves each. We then ran `mwrank` on 32 processors simultaneously, as this was the maximum number of allowed jobs per user. Each machine took about 3 hours for a collective runtime of 96 CPU hours. The result was a calculated value for the 2-Selmer rank of each of the curves.

Step 3: Eliminate Curves with Small Rank. We wish to find curves with Mordell-Weil rank $r > 3$. Since the Mordell-Weil rank r is bounded above by the 2-Selmer rank s, we eliminate those curves with $s < 4$.

We implemented this process using `Maple`. This reduced the original 503955 candidate curves to 17666 curves. In practice, we had 32 files containing approximately 15750 candidate curves each, and `Maple` reduced each file to approximately 550 curves in less than a minute.

Step 4: Compute the Mordell-Weil Ranks. Our final step is to compute the Mordell-Weil ranks of the curves from Step 3. This should take the longest because `mwrank` runs slowly on elliptic curves with large coefficients. We wish to compute the Mordell-Weil ranks for 17666 curves.

We distributed this computation among 32 processors. Unfortunately, we did not find an elliptic curve with Mordell-Weil rank 4. The default settings within `mwrank` examined these curves within about a days time, yet `mwrank` only provided broad inequalities for the Mordell-Weil rank, e.g., $0 \leq r \leq 4$. Using the options `-b 12 -p 200`, which increased the search space for rational points on homogeneous spaces, it took about a week to process all 32 lists. This yielded 15 curves with $r \geq 2$.

Due to the limitations of `mwrank`, we turned to other software. We used William Stein's machine at the University of Washington as well as the high-powered computing cluster at Harvard University to run `Magma`. First, we tried the command `FourDescent()` in order to search for more rational points on the elliptic curves with $r \geq 2$. Unfortunately, this command found nontrivial points of order 2 in the Shafarevich-Tate group – thereby giving the strict inequality $r < s$. Using the conjecture that r and s are either both even or both odd, we expect $r = 2$ for these 15 curves. Second, we tried the command `AnalyticRank()` using the conjecture of Bryan Birch and Peter Swinnerton-Dyer to match the Mordell-Weil rank with the order vanishing of the L-series of the elliptic curve. Again we expect $r = 2$ for these 15 curves.

References

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

[2] Andrej Dujella. High rank elliptic curves with prescribed torsion. `http://www.math.hr/~duje/tors/tors.html`, 2003.

[3] Edray Herber Goins. SUMSRI Number Theory Research Seminar Lecture Notes. In preparation, 2006.

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

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

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

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

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

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

Central State University, Wilberforce, OH 45384
E-mail address: tbrooks1906@yahoo.com

Maryville College, Maryville, TN 37804
E-mail address: fowlerbeth4@aol.com

Baldwin-Wallace College, Berea, OH 44017
E-mail address: kchastings@sbcglobal.net

Campbellsville University, Campbellsville, KY 42718
E-mail address: danielle_hiance@yahoo.com

Central State University, Wilberforce, OH 45384
E-mail address: mattman27@gmail.com