IN SEARCH OF AN 8: RANK COMPUTATIONS ON A FAMILY OF QUARTIC CURVES

KATHLEEN P. ANSALDI, ALLISON R. FORD, JENNIFER L. GEORGE, KEVIN M. MUGO, AND CHARLES E. PHIFER

ABSTRACT. We consider the family of elliptic curves $y^2 = (1-x^2)(1-k^2x^2)$ for rational numbers $k \neq -1, 0, 1$. Every rational elliptic curve with torsion subgroup either $Z_2 \times Z_4$ or $Z_2 \times Z_8$ is birationally equivalent to this quartic curve for some k. We use this canonical form to search for such curves with large rank.

Our algorithm consists of the following steps. We compute a list of rational k by considering those associated to a given list of rational points (x, y). We then eliminate certain k by considering the associated 2-Selmer groups. Finally, we use Cremona's `mwrank` to find the ranks. Using these steps, we found two elliptic curves with Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}^6$.

1. INTRODUCTION

In this paper, we consider rational elliptic curves of the form

$$E : y^2 = (1-x^2)(1-k^2x^2), \qquad k \neq -1, 0, 1. \tag{1}$$

Upon writing $k = p/q$, this curve is birationally equivalent to the integral cubic curve $Y^2 = X^3 + AX + B$ in terms of the integers

$$A = -27(p^4 + 14p^2q^2 + q^4), \qquad B = -54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6). \tag{2}$$

Every rational elliptic curve with torsion subgroup either $Z_2 \times Z_4$ or $Z_2 \times Z_8$ is birationally equivalent to this quartic curve for some k. We are interested in finding rational elliptic curves with torsion subgroup $Z_2 \times Z_4$ having large rank. Recently, Elkies [5] found such a curve of rank 8; it corresponds to $k = 556536737101/589636934451$. We are motivated instead by an example of Dujella [4] – a curve of rank 6 corresponding to $k = 76369/185907$. We consider curves of rank 6, rather than curves of rank 8, simply due to the computational complexity of finding curves with high rank.

Using an idea of Rogers [8], which in turn is based on a suggestion of Rubin and Silverberg [9], we perform the following steps:

(1) Compute a list of rational k such that the curve $y^2 = (1-x^2)(1-k^2x^2)$ has positive rank.
(2) Eliminate those k's of small logarithmic height.
(3) Eliminate those k's such that $4A^3 + 27B^2$ has few prime divisors.
(4) Eliminate those k's such that the 2-Selmer rank of the curve is less than 6.
(5) Return those k's such that the (Mordell-Weil) rank is at least 6.

2000 *Mathematics Subject Classification.* Primary 14H52; Secondary 11D25.
Key words and phrases. Elliptic curves, Rank, Selmer group.

Using this algorithm, we found two new curves of rank 6, corresponding to $k = 307100/384569$ and $94939/471975$.

We would like to thank the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI), Miami University, the National Science Foundation, and the National Security Agency for the funding and opportunity to do this research. Special thanks to Edray Goins and Lakeshia Legette for their guidance with our project.

2. Quartic Form of Elliptic Curves

Let us begin by reviewing some results on elliptic curves. We introduce the particular curve that is the focus of our study.

Proposition 1. *Given a rational number k, consider the quartic curve:*

$$E : y^2 = (1 - x^2)(1 - k^2x^2). \tag{3}$$

Then E is a rational elliptic curve if $k \neq -1, 0, 1$. In particular, E is birationally equivalent to the cubic curve

$$Y^2 = X^3 - 27\left(k^4 + 14k^2 + 1\right)X - 54\left(k^6 - 33k^4 - 33k^2 + 1\right). \tag{4}$$

The motivation for such a birational transformation can be found in Cassels [1].

Proof. By using the transformation

$$X = \frac{(15k^2 - 3)x + 15 - 3k^2}{x - 1} \qquad \text{and} \qquad Y = \frac{(54 - 54k^2)y}{(x - 1)^2} \tag{5}$$

we see that (3) is equivalent to the cubic curve above. An elliptic curve can be defined by an equation of the form $Y^2 = X^3 + AX + B$ where $4A^3 + 27B^2 \neq 0$. Hence the curve above is an elliptic curve precisely when $-8503056k^2(k^2 - 1)^4 \neq 0$, which happens precisely when $k \neq -1, 0, 1$. □

Say we are given two rational points P_1 and P_2 on E, the quartic curve. Denote $P_1 * P_2$ as the point of intersection with the projective curve E and the parabola through the three points $\mathcal{O} = (1, 0)$, P_1 and P_2. Define the composition law $\oplus$ by $P_1 \oplus P_2 = (P_1 * P_2) * \mathcal{O}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group. In particular,

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r \tag{6}$$

for some nonnegative integer r. For more information, see [12].

Proposition 2 (Goins, [6])**.** *Fix a rational number $k \neq -1, 0, 1$ and consider the elliptic curve*

$$E : y^2 = (1 - x^2)(1 - k^2x^2). \tag{7}$$

Then $E(\mathbb{Q})_{tors}$ is either $Z_2 \times Z_4$ or $Z_2 \times Z_8$. Moreover, any rational elliptic curve with one of these torsion subgroups is birationally equivalent to E for some rational k.

We give an example of this. Recently, Elkies [5] discovered the rational elliptic curve

$$\begin{aligned} E : Y^2 &+ 589636934451XY + 139812405617053971435280225498920 0Y \\ &= X^3 + 237116092035908004920 0X^2 \end{aligned} \tag{8}$$

which has Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}^8$. Using the transformation

$$\begin{aligned} X &= -\frac{4742321840718160098400x}{x-1} \\ Y &= -\frac{69906202808526985717640112749460 0(y+x^2-1)}{(x-1)^2}, \end{aligned} \tag{9}$$

we find the quartic form of the equation

$$y^2 = (1-x^2)(1-k^2x^2), \qquad \text{where} \qquad k = \frac{556536737101}{589636934451}. \tag{10}$$

Proposition 2 follows from a careful analysis of the list of allowed torsion subgroups for a rational elliptic curve, as in [7]. The following proposition allows us to distinguish between the two torsion subgroups in Proposition 2.

Proposition 3 (Goins, [6])**.** *If E is a rational elliptic curve with $E(\mathbb{Q})_{tors} \simeq Z_2 \times Z_8$ then there exists $t \in \mathbb{Q}$ such that E is birationally equivalent to the quartic curve*

$$y^2 = (1-x^2)(1-k^2x^2) \qquad \textit{with} \qquad k = \frac{t^4-6t^2+1}{(t^2+1)^2}. \tag{11}$$

3. Finding Elliptic Curves With High Rank

In [4], Dujella lists the highest known ranks for elliptic curves classified by their torsion subgroups. Some of these records are shown in Table 1. For curves with torsion subgroup isomorphic to $Z_2 \times Z_4$, the highest known rank is 8. As mentioned before, this curve corresponds to $k = 556536737101/589636934451$. For curves with torsion subgroup isomorphic to $Z_2 \times Z_8$, the highest known rank is 3. There are five such examples, corresponding to

$$k = \frac{t^4-6t^2+1}{(t^2+1)^2}, \qquad \text{where} \qquad t = \frac{5}{29}, \frac{18}{47}, \frac{15}{76}, \frac{47}{219}, \text{ and } \frac{19}{220}. \tag{12}$$

Table 1. Rank Records of Elliptic Curves With Prescribed Torsion

$E(\mathbb{Q})_{tors}$	Highest Rank	Found By	Year
0	24	Martin-McMillen	2000
Z_2	17	Elkies	2005
Z_3	11	Elkies-Rogers	2004
Z_4	11	Elkies	2005
Z_5	6	Dujella-Lecacheux	2001
Z_6	7	Dujella	2001
Z_7	5	Dujella-Kulesz	2001
Z_8	5	Dujella-Lecacheux	2002, 2003
Z_9	3	Dujella, MacLeod	2001, 2003
Z_{10}	3	Dujella, Rathbun	2001, 2003
Z_{12}	3	Dujella, Rathbun	2001, 2003
$Z_2 \times Z_2$	11	Elkies	2005
$Z_2 \times Z_4$	8	Elkies	2005
$Z_2 \times Z_6$	5	Dujella-Lecacheux	2002
$Z_2 \times Z_8$	3	Connell, Dujella, Campbell-Goins, Rathbun	2000, 2001 2003, 2003

We wish to find rational elliptic curves E with torsion subgroup $Z_2 \times Z_4$ and rank at least 6. To this end, we perform the following steps:

(1) Compute a list of rational k such that the curve $y^2 = (1-x^2)(1-k^2x^2)$ has positive rank.
(2) Eliminate those k's of small logarithmic height.
(3) Eliminate those k's such that $4A^3 + 27B^2$ has few prime divisors.
(4) Eliminate those k's such that the 2-Selmer rank of the curve is less than 6.
(5) Return those k's such that the (Mordell-Weil) rank is at least 6.

We discuss these steps in more detail below.

3.1. **Step 1: Choosing k Intelligently.** Using an idea of Rogers [8], which in turn is based on a suggestion of Rubin and Silverberg [9], we observe that it should be easier to find rational points on curves with higher rank. To this end, finding an initial list of k's can be done using the following assertion.

Theorem 4. *Fix a rational number $0 < k < 1$ and consider the elliptic curve*

$$E : y^2 = (1-x^2)(1-k^2x^2). \tag{13}$$

Assume that $\sqrt{1-k^2}$ is not a rational number. If (x, y) is a rational affine point on E such that $xy \neq 0$ then E has positive rank.

This theorem tells us that if we have a point (x, y) on the elliptic curve $y^2 = (1-x^2)(1-k^2x^2)$, we know that this curve has positive rank whenever $xy \neq 0$. Thus, to find k's corresponding to curves of positive rank, we first generate rational points (x, y), and then solve for k.

Proof. We note the identity

$$k = \frac{t^4 - 6t^2 + 1}{(t^2+1)^2} \qquad \Longrightarrow \qquad \sqrt{1-k^2} = \frac{4(t^3-t)}{(t^2+1)^2}. \tag{14}$$

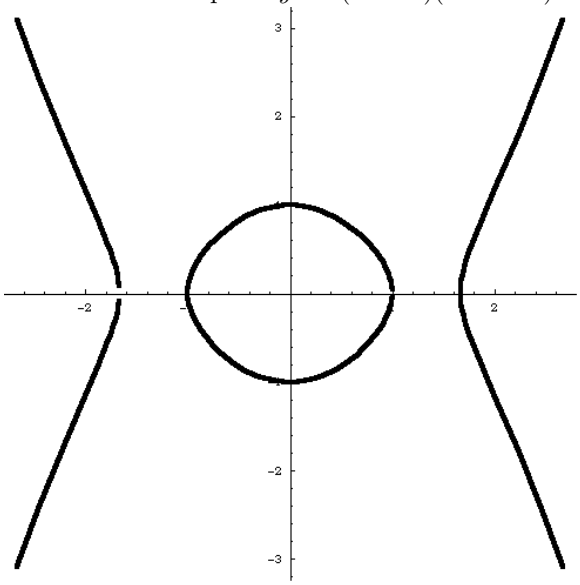
We conclude that if $\sqrt{1-k^2}$ is not rational, then by Propositions 2 and 3, we see that $E(\mathbb{Q})_{tors} \simeq Z_2 \times Z_4$.

The torsion elements on E can be precisely determined. Table 2 explicitly lists the points of finite order on $y^2 = (1-x^2)(1-k^2x^2)$. Note that the (affine) points of order 2 satisfy $y = 0$, whereas the (affine) points of order 4 satisfy $x = 0$. By assumption, there exists a rational point (x, y) such that $xy \neq 0$, so this must be a point of infinite order. □

TABLE 2. Torsion Points on $y^2 = (1-x^2)(1-k^2x^2)$

Order of Point	Torsion Point on Quartic
1	$(1, 0)$
2	$(1/k, 0)$
2	$(-1/k, 0)$
2	$(-1, 0)$
4	$(0, 1)$
4	$(0, -1)$
4	[pt. at infinity]
4	[pt. at infinity]

FIGURE 1. Graph of $y^2 = (1-x^2)(1-k^2x^2)$



We choose a grid of rational points (x, y) on the curve $y^2 = (1-x^2)(1-k^2x^2)$. By symmetry, we may assume both x and y are positive. More precisely, upon considering the graph in Figure 1, we may assume $0 < x < 1$ and $0 < y < 1$. We let $x = a/c$ and $y = b/c$, where a, b, and c are positive integers such that $1 \leq a < c$ and $1 \leq b < \sqrt{c^2 - a^2}$. Upon solving for k, we find that

$$k = \frac{cd}{a(c^2-a^2)}, \qquad \text{where} \qquad d = \sqrt{(c^2-a^2)(c^2-a^2-b^2)}. \tag{15}$$

For each point (a, b, c) in the grid, we compute d. If d is an integer, we add k to our list.

3.2. **Step 2: Logarithmic Height and Rank Bounds.** To find a lower bound on the rank r, we make use of the following conjecture:

Conjecture 5. *Let $k \neq -1, 0, 1$ be a rational number. Write $k = p/q$, and define its logarithmic height as $h(k) = \max\{\log|p|, \log|q|\}$. Let $r(k)$ denote the rank of the elliptic curve $y^2 = (1-x^2)(1-k^2x^2)$. There exists a positive real number m such that for all such k we have $h(k) \geq m \cdot r(k)$.*

A plot of $h(k)$ versus $r(k)$ for nearly 4000 rational $k \neq -1, 0, 1$ (counting multiplicities) can be found in Figure 2. These k were chosen as explained in the previous section. We can determine the least height $h(k)$ corresponding to curves of ranks 1, 2, 3, and 4. This data can be found in Table 3; a plot of this data can be found in Figure 3. Using linear regression on this data, we expect $m = 0.61776 \pm 0.01771$. Regardless of the veracity of the conjecture, we exclude rational k with $h(k) < m \cdot r$.

3.3. **Steps 3 – 4: Selmer Group Computations.** Recall the following well-known short exact sequence:

$$0 \longrightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \longrightarrow \mathrm{Sel}^{(2)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q}). \tag{16}$$

FIGURE 2. Plot of $h(k)$ versus $r(k)$

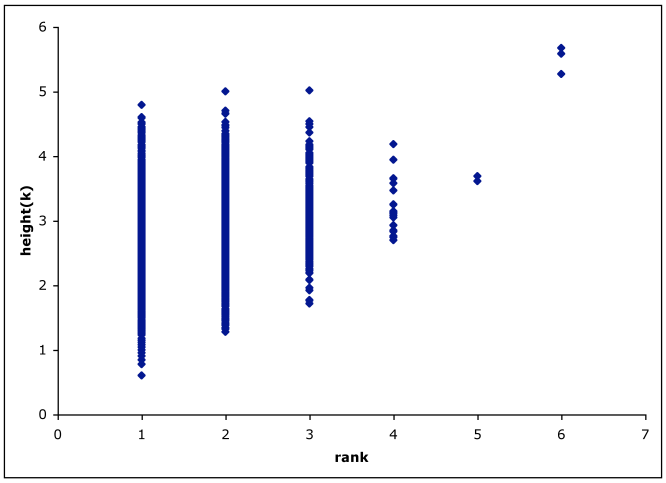


TABLE 3. Data for Least $h(k)$ for Each Rank r

k	Height $h(k)$	Rank r
$\frac{3}{4}$	0.602060	1
$\frac{7}{19}$	1.278754	2
$\frac{51}{52}$	1.716003	3
$\frac{281}{360}$	2.556303	4
$\frac{2697}{4088}$	3.611511	5

For more information, see [12]. Assuming $E[2] \subseteq E(\mathbb{Q})$, we have the cardinalities

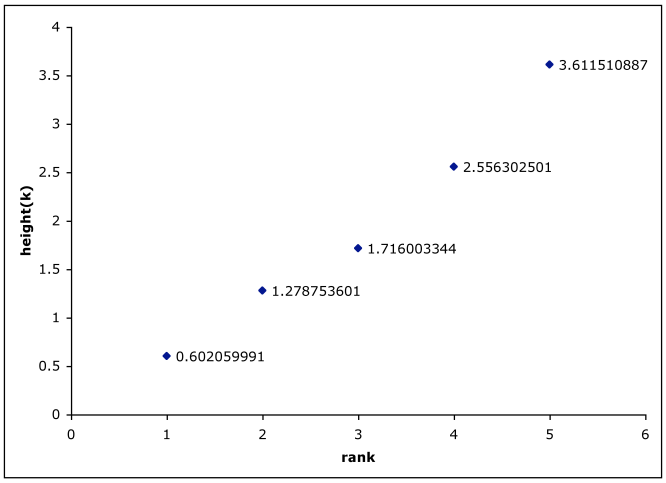
$$\left|\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right| = 2^{r+2} \qquad \text{and} \qquad \left|\text{Sel}^{(2)}(E/\mathbb{Q})\right| = 2^{s+2}, \tag{17}$$

where r is the Mordell-Weil rank and s is the "2-Selmer rank". Note that $r \leq s$. In particular, the size of the 2-torsion in the Shafarevich-Tate group is $|Ш(E/\mathbb{Q})[2]| = 2^{s-r}$.

In order to find an upper bound for the 2-Selmer rank s, we make the following observation. Consider an integral elliptic curve $E : Y^2 = X^3 + AX + B$ with discriminant $\Delta(E) = -16(4A^3 + 27B^2)$. Denote $\omega(d)$ as the number of primes dividing a non-zero integer d. It is easy to see that

$$r \leq s \leq 2 \cdot \omega(\Delta(E)). \tag{18}$$

FIGURE 3. Plot of Least $h(k)$ for Each Rank r



In other words, if the discriminant of E has a small number of prime factors, the rank must also be small. To find a curve E with large rank, $\Delta(E)$ must have a large number of prime factors. For more along this line of reasoning, see [10].

Express $k = p/q$ for integers p and q. Following the transformation in Proposition 1, it is easy to see that the quartic curve $y^2 = (1-x^2)(1-k^2x^2)$ is birationally equivalent to the integral cubic curve $Y^2 = X^3 + AX + B$ in terms of the integers

$$A = -27(p^4 + 14p^2q^2 + q^4), \qquad B = -54(p^6 - 33p^4q^2 - 33p^2q^4 + q^6). \tag{19}$$

We eliminate those k's such that $\omega\big(pq(p^2-q^2)\big)$ is small, i.e. less than 10. We also eliminate those k's such that $pq(p^2-q^2)$ has a prime factor larger than 10^6. This is purely a computational restriction associated with Cremona's `mwrank`.

Using the list of remaining k's, we pass the integral models $Y^2 = X^3 + AX + B$ to `mwrank`. We use the flag `-s` so that the software computes the 2-Selmer rank s. In practice, our coefficients are so large that it seems best to skip the second descent, i.e. we use the flag `-d` as well. We eliminate those k's with $s \leq 6$.

3.4. **Step 5: Rank Computations.** We use `mwrank` to compute the Mordell-Weil rank r of the remaining list of k's. In order to make sure the generators returned by the software are the true generators of the full Mordell-Weil group, we also use the flag `-S -1`. This guarantees saturation at all primes. For more details, see [2].

4. RESULTS

Our implementation of this algorithm found two curves of rank 6. We used personal computers at Miami University, as well as high-end machines at Harvard University and Purdue University. The longest runtime for the program was approximately 120 CPU hours.

4.1. **Curves of Rank 6.** The first curve is

$$\begin{aligned} Y^2 = X^3 &- 610300428445787829702626 7X \\ &+ 58000270527767498818390370456259916 26, \end{aligned} \tag{20}$$

which corresponds to $k = 307100/384569$. The generators for this curve are:

$$\begin{aligned}
&[2163523664640327 : 556078200897099270600 : 1331],\\
&[2889589925127 : 3506015239306639290 : 1],\\
&[6628502811663926 : 726601419375049946420 : 4913],\\
&[26165985283526847 : 115140606932837392613280 : 1331],\\
&[4546881938212050279 : 34353341747719623137040840 : 79507],\\
&[1461784359354504 : -1747413264343628597625 : 512].
\end{aligned} \tag{21}$$

The regulator for this curve is 26612.77.

The second curve is

$$\begin{aligned}
Y^2 = X^3 &- 21009531825277215961108 32X\\
&+ 232328512961429750343111862628528256,
\end{aligned} \tag{22}$$

which corresponds to $k = 94939/471975$. The generators for this curve are:

$$\begin{aligned}
&[-283847517694018164 : 352616142480375100052880 : 300763],\\
&[29419960772944815852 : 56877771215361605537574000 : 6967871],\\
&[7177905387912779196 : 122730545321166233308572 00 : 2048383],\\
&[5630923059584484 : 138746085894621294964875 : 314432],\\
&[-177675523009980 : 73616570450742310992 : 125],\\
&[-217894627787474076 : 61765176726680861926800 : 148877].
\end{aligned} \tag{23}$$

The regulator for this curve is 8988.402.

4.2. **Possible Improvements.** The largest known rank for rational elliptic curves with torsion subgroup $Z_2 \times Z_4$ was found by Elkies [5] only recently. Although his curve has rank 8, our examples supplement the rank 6 curve found by Dujella [4]. Though we did not find a rank 8 or larger curve with this algorithm, we expect that given more time, we would find such a curve.

We should mention that we attempted to implement a second algorithm, motivated by [8]. Step 1 in our new algorithm was the same, but the remaining steps were different. We computed a histogram of rational numbers k, and then considered only those k's which appeared most often. We used a hash table to create the histogram; the benefit of such a table is that its search time is independent of its size. Rogers constructed his hash table for integers, but we needed to construct one for rational numbers. For each rational $k = p/q$, we determined the integer $\overline{p} \equiv p \mod N$ for a fixed large prime N. Then k and its count were stored in the hash table at index $\overline{p}$. Once all the k's were determined, a histogram was constructed. This algorithm did not fare as well as the first algorithm, however; the highest rank found was 4.

5. Applications to Some Diophantine Problems

The study of elliptic curves of the form (3) yields several applications. By studying quartic curves of this form we can gain a better understanding of Heron triangles. We can also use high ranked elliptic curves to study rational Diophantine m-tuples.

5.1. **Heron Triangles.** Heron of Alexandria (c. 10–75AD) found the following formula for calculating the area of a triangle with sides of length a, b and c:

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \qquad \text{where} \qquad s = \frac{a+b+c}{2}. \tag{24}$$

In his honor, a triangle having rational sides of length a, b, and c and rational area A is said to be a *Heron triangle*.

Proposition 6. *Say that we have an isosceles Heron triangle with base b and area A. Then all Heron triangles of area A with sides of length a, b, and c correspond to rational points on the curve*

$$E : y^2 = (1-x^2)(1-k^2x^2), \qquad \textit{where} \qquad k = \sqrt{\frac{16A^2+b^4}{b^4}}. \tag{25}$$

This proposition essentially follows from [11]. The assumption that A is the area of an isosceles triangle forces k to be a rational number. The triangle of sides a, b, and c must necessarily have the same base as the isosceles triangle, but itself need not be isosceles.

Proof. By assumption, A is the area of an isosceles triangle. Say this triangle has sides of length ℓ, ℓ, and b, and height h. Then,

$$h = \sqrt{\ell^2 - \frac{b^2}{4}} \qquad \text{and} \qquad A = \frac{1}{2}\,b\,h \qquad \Longrightarrow \qquad k = \frac{2\,\ell}{b}. \tag{26}$$

Thus k is indeed rational.

We make the following substitution:

$$\left.\begin{aligned} x &= \frac{b}{a+c} \\ y &= \frac{a-c}{b}\,\frac{(a+c)^2-b^2}{(a+c)^2} \end{aligned}\right\} \iff \left\{\begin{aligned} \frac{a}{b} &= \frac{1+x\,y-x^2}{2\,(x-x^3)} \\ \frac{c}{b} &= \frac{1-x\,y-x^2}{2\,(x-x^3)} \end{aligned}\right. \tag{27}$$

This transforms (24) into (25). □

5.2. **Rational Diophantine m-Tuples.** A set $\{n_1, n_2, ..., n_m\}$ of m rational numbers is called a *rational Diophantine m-tuple* if $n_i n_j + 1$ is the square of a rational number for $i \neq j$. There are infinitely many rational Diophantine 3-tuples, some of which are easy to find. It is possible to extend a rational Diophantine 3-tuple to a tuple of greater length by considering the X-coordinates of certain rational points.

Theorem 7 (Dujella, [3])**.** *Given a rational Diophantine 3-tuple $\{n_1, n_2, n_3\}$, consider a rational point P on the elliptic curve*

$$E : Y^2 = (n_1X+1)(n_2X+1)(n_3X+1). \tag{28}$$

1. *Let n_4 denote the X-coordinate of the point $(0,1)\oplus[2]P$. Then $\{n_1, n_2, n_3, n_4\}$ is a rational Diophantine 4-tuple.*
2. *There exists $R \in E(\mathbb{Q})$ such that if n_5 is the X-coordinate of $(0,1) \oplus [2]Q$ in terms of $Q = R \oplus P$, then $\{n_1, n_2, n_3, n_4, n_5\}$ is a rational Diophantine 5-tuple.*

Question 8. *Do there exist rational Diophantine 7-tuples?*

Proposition 9. *Fix a rational number $t \neq -1, 0, 1$, and let $n_1 = t$, $n_2 = -1/t$, and $n_3 = n_1 + n_2$. Then $\{n_1, n_2, n_3\}$ is a rational Diophantine 3-tuple. A necessary condition to extend this 3-tuple to a 7-tuple is that there exists a rational point on the quartic curve*

$$y^2 = (1 - x^2)(1 - k^2 x^2), \qquad \textit{where} \qquad k = \frac{1 - t^2}{1 + t^2}. \tag{29}$$

Proof. Note the relations

$$n_1\, n_2 + 1 = 0^2, \qquad n_1\, n_3 + 1 = n_1^2, \qquad \text{and} \qquad n_2\, n_3 + 1 = n_2^2; \tag{30}$$

hence $\{n_1, n_2, n_3\}$ is a 3-tuple. Say that n_4, $n_5, \ldots$ form an extension of the 3-tuple. Then $X = n_i$ would be the X-coordinate of a rational point on the curve

$$E : Y^2 = (n_1\, X + 1)\,(n_2\, X + 1)\,(n_3\, X + 1)\,. \tag{31}$$

Make the substitution

$$\left.\begin{aligned} x &= 1 + \frac{2\,t}{t^2 - 1}\,\frac{1}{X} \\ y &= \frac{4\,t^2}{t^4 - 1}\,\frac{Y}{X^2} \end{aligned}\right\} \iff \begin{cases} X = \dfrac{2\,t}{t^2 - 1}\,\dfrac{1}{x - 1} \\ Y = \dfrac{t^2 + 1}{t^2 - 1}\,\dfrac{y}{(x - 1)^2} \end{cases} \tag{32}$$

This sends the relation in (31) to the quartic curve in (29). □

We give an example of this proposition by extending the rational Diophantine 3-tuple

$$\left\{\frac{2}{5}, -\frac{5}{2}, -\frac{21}{10}\right\} \qquad \text{with} \qquad t = \frac{2}{5} \tag{33}$$

to a rational Diophantine 5-tuple. To do so, we consider the elliptic curve

$$E : Y^2 = \left(\frac{2}{5}X + 1\right)\left(-\frac{5}{2}X + 1\right)\left(-\frac{21}{10}X + 1\right) \tag{34}$$

with rational point $P = (-40/21, 55/21)$. (The Mordell-Weil group of this curve is $E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}$, where P is a generator of the free part.) This curve corresponds to the quartic curve with $k = 21/29$.

First, we compute the point

$$(0, 1) \oplus [2]P = \left(\frac{528}{1445}, \frac{3731}{24565}\right) \qquad \Longrightarrow \qquad n_4 = \frac{528}{1445}. \tag{35}$$

Next, we compute the point $Q = (0, 1) \oplus P = (5/8, -15/32)$. (For any rational t, we may choose $R = (0, 1)$ as in Theorem **??**. Finally, we compute the point

$$(0, 1) \oplus [2]Q = \left(-\frac{2640}{1681}, -\frac{193372}{68921}\right) \qquad \Longrightarrow \qquad n_5 = -\frac{2640}{1681}. \tag{36}$$

Hence, we have constructed the rational Diophantine 5-tuple

$$\left\{\frac{2}{5}, -\frac{5}{2}, -\frac{21}{10}, \frac{528}{1445}, -\frac{2640}{1681}\right\}. \tag{37}$$

References

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

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[3] Andrej Dujella. Diophantine m-tuples and elliptic curves. *J. Théor. Nombres Bordeaux*, 13(1):111–124, 2001. 21st Journées Arithmétiques (Rome, 2001).

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

[5] Noam D. Elkies. $E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/4\mathbb{Z}) * \mathbb{Z}^8$. Electronic correspondence to `NMBRTHRY@LISTSERV.NODAK.EDU`, June 2005.

[6] Edray Herber Goins. $y^2 = (1 - x^2)(1 - k^2x^2)$. In preparation, 2005.

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

[8] Nicholas F. Rogers. Rank computations for the congruent number elliptic curves. *Experiment. Math.*, 9(4):591–594, 2000.

[9] Karl Rubin and Alice Silverberg. Ranks of elliptic curves in families of quadratic twists. *Experiment. Math.*, 9(4):583–590, 2000.

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

[11] David J. Rusin. Rational triangles with equal area. *New York J. Math.*, 4:1–15 (electronic), 1998.

[12] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

Loyola College in Maryland, Baltimore, MD 21210
E-mail address: `kpansaldi1@loyola.edu`

8804 Copperleaf Way, Fairfax Station, VA 22039
E-mail address: `fordar7093@mbc.edu`

Miami University, Oxford, OH 45056
E-mail address: `georgej1@muohio.edu`

Otterbein College, Westerville, OH 43081
E-mail address: `Kevin.Mugo@otterbein.edu`

3646 Occidental Ct., Decatur, GA 30034
E-mail address: `Phifer_domain@hotmail.com`