ON MORDELL-WEIL GROUPS OF ELLIPTIC CURVES INDUCED BY DIOPHANTINE TRIPLES

Andrej Dujella
University of Zagreb, Croatia

Abstract. We study the possible structure of the groups of rational points on elliptic curves of the form $y^2 = (ax+1)(bx+1)(cx+1)$, where a, b, c are non-zero rationals such that the product of any two of them is one less than a square.

Dedicated to Professor Sibe Mardešić on the occasion of his 80th birthday.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. By Mordell-Weil theorem, the group $E(\mathbb{Q})$ of rational points on E is a finitely generated abelian group. Hence, it is the product of the torsion group and $r \geq 0$ copies of infinite cyclic group:

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

By Mazur's theorem, we know that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. On the other hand, it is not known which values of rank r are possible. The folklore conjecture is that a rank can be arbitrary large, but it seems to be very hard to find examples with large rank. The current record is an example of elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found by Elkies in May 2006 (see [25, 21]).

In the present paper, we will study a special case of this problem. Namely, we will consider only elliptic curves of the form $y^2 = (ax+1)(bx+1)(cx+1)$, where $\{a, b, c\}$ is a rational Diophantine triple. Although this is a very special case, it has some relevance for the more general problem of determining which ranks are possible for elliptic curves with prescribed torsion group. In

---

2000 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic curves, rank, torsion group, Diophantine triple.

particular, we will show in Section 6 that every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by some rational Diophantine triple.

A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero integers (rationals) is called *a (rational) Diophantine m-tuple* if $a_i \cdot a_j + 1$ is a perfect square for all $1 \le i < j \le m$. Diophantus of Alexandria found a rational Diophantine quadruple $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$, while the first Diophnatine quadruple in integers, the set $\{1, 3, 8, 120\}$, was found by Fermat (see [11, 12, 27]). The famous conjecture is that there does not exist a Diophantine quintuple (in non-zero integers) (see e.g. [31, 43]). In 1969, Baker and Davenport [2] proved that the Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. Recently, it was proved in [20] that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples.

Let $\{a, b, c\}$ be a (rational) Diophantine triple. We define nonnegative rational numbers r, s, t by

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2.$$

In order to extend this triple to a quadruple, we have to solve the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{1.1}$$

It is natural idea to assign to the system (1.1) the elliptic curve

$$E: \quad y^2 = (ax + 1)(bx + 1)(cx + 1). \tag{1.2}$$

Properties of elliptic curves obtained in this manner and connections between solutions of the system (1.1) and the equation (1.2) were studied in [16, 18, 23], but this was mainly for the case when a, b, c are positive integers. In this paper, we will assume that a, b, c are non-zero rationals, and we will call $\{a, b, c\}$ a Diophantine triple (hence, omitting the word *rational*).

The coordinate transformation $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ applied on the curve E leads to the elliptic curve

$$\begin{aligned} (1.3)\ E': \quad y^2 &= (x + bc)(x + ac)(x + ab) \\ &= x^3 + (ab + ac + bc) + (a^2bc + ab^2c + abc^2)x + a^2b^2c^2 \end{aligned}$$

in the Weierstrass form. There are three rational points on E' of order 2:

$$T_1 = [-bc, 0], \quad T_2 = [-ac, 0], \quad T_3 = [-ab, 0],$$

and also other obvious rational points

$$P = [0, 1], \quad Q = [1, rst].$$

It is easy to verify that $Q = 2R$, where

$$R = [rs + rt + st + 1, (r + s)(r + t)(s + t)].$$

In general, we may expect that the points P and R will be two independent points of infinite order, and therefore that $\operatorname{rank} E(\mathbb{Q}) \ge 2$. Thus, assuming various standard conjectures, we may expect that the most of elliptic curves induced by Diophantine triples with the above construction will have the Mordell-Weil group $E(\mathbb{Q})$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}^2$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}^3$.

The main purpose of this paper is to study which other groups are possible here. Namely, we will investigate situations in which P or R have finite order, or they are dependent, and in particular we would try to construct curves with more independent points of infinite order.

According to Mazur's theorem, for the torsion group $E(\mathbb{Q})_{\rm tors}$ we have at most four possibilities: $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ with $m=1,2,3,4$. In [18], it was shown that if a,b,c are positive integers, then the cases $m=2$ and $m=4$ are not possible. However, in the present paper we will show that for a,b,c non-zero rationals all four groups are indeed possible.

Let us also note that every Diophantine pair $\{a,b\}$ can be extended to a Diophantine triple by a very simple extension: $c=a+b+2r$. This construction was known already to Euler (and maybe even to Diophantus). The direct computation shows that for triples of the form $\{a,b,a+b+2r\}$, the points P and R are not independent, since $2P=-2R$.

2. Search for elliptic curves with high rank

In last few years, several authors considered the problem of construction of elliptic curves with some prescribed property and relatively high rank. This includes curves with given torsion group (see [17, 36] and the references given there), curves $y^2=x^3-n^2x$ related to congruent numbers [41], curves of the form $y^2=x^3+dx$ [24], curves $x^3+y^3=m$ related to the taxicab problem [26], curves $y^2=(ax+1)(bx+1)(cx+1)(dx+1)$ induced by Diophantine quadruples $\{a,b,c,d\}$ [15], etc.

Let G be an admissible torsion group for an elliptic curve over the rationals (according to Mazur's theorem). Let us define

$$B(G)=\sup\{\mathrm{rank}\,(E(\mathbb{Q}))\,:\,E(\mathbb{Q})_{\rm tors}=G\}.$$

The conjecture is that $B(G)$ is unbounded for all G. In the following table we give the best known lower bounds for $B(G)$.

G	$B(G) \geq$	Author(s)
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	18	Elkies (2006)
$\mathbb{Z}/3\mathbb{Z}$	12	Eroshkin (2006)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	6	Dujella & Lecacheux (2001)
$\mathbb{Z}/6\mathbb{Z}$	7	Dujella (2001,2006)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	3	Dujella (2001), MacLeod (2004), Eroshkin (2006)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	3	Dujella (2001,2005,2006), Rathbun (2003,2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	14	Elkies (2005)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (2005)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006), Campbell & Goins (2003), Rathbun (2003,2006)

Details on the record curves appearing in the above table and full list of the references can be found on the author's web page [17].

We will now briefly describe the main steps in the construction of high rank curves with prescribed properties. These steps have been already applied, with various modifications, in obtaining curves from the above table, and we will also apply them in the following sections.

The first step is to find a parametric family of elliptic curves over $\mathbb{Q}$ which contains curves with relatively high rank (i.e. an elliptic curve over the field of rational functions $\mathbb{Q}(T)$ with large generic rank) which satisfy the prescribed property. Here it is not always the best idea to use the family with largest known generic rank, since these families usually contain curves with very large coefficients for which it is very hard to compute the rank.

In the second step we want to find, in the given family of curves, the best candidates for higher rank. The main idea here is that a curve is more likely to have large rank if $\#E(\mathbb{F}_p)$ is relatively large for many primes p. We will use the following realization od this idea. For a prime p, we put $a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. For a fixed integer N, we define

$$S(N,E) = \sum_{p \leq N,\ p \text{ prime}} \left(1 - \frac{p-1}{\#E(\mathbb{F}_p)}\right) \log(p) = \sum_{p \leq N,\ p \text{ prime}} \frac{-a_p + 2}{p + 1 - a_p}\ \log(p).$$

It is experimentally known (see [38, 39, 19]) that we may expect that high rank curves have large $S(N,E)$. In [7], some arguments were given which show that the Birch and Swinnerton-Dyer conjecture gives support to this observation. The sum $S(N,E)$ can be very efficiently computed (e.g. using PARI [3]) for $N < 10000$. After this sieving method, we may continue to investigate the best, let us say, %1 of curves. Since, we are working with curves with torsion points of order 2, we may compute the Selmer rank for these curves, which is well-known upper bound for the actual rank of the curve. This can be done using an appropriate option in Cremona's program *mwrank* [10].

Only for the curves for which that upper bound is satisfactory large, we try to compute the rank exactly. Again, the best available software for this purpose is *mwrank* which uses 2-descent (via 2-isogeny if possible) to determine the rank, obtain a set of points which generate $E(\mathbb{Q})$ modulo $2E(\mathbb{Q})$, and finally saturate to a full $\mathbb{Z}$-basis for $E(\mathbb{Q})$. The program package *APECS* [9] and a program that implements LLL reduction on the lattice of points of E, provided by Rathbun [40], is used to reduce the heights of the generators. In the cases when 4-descent is appropriate to perform (for curves with a torsion point of order 4, and with a generator of very large height) we used an implementation of 4-descent in *MAGMA* [4].

3. Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

In [14], we have constructed a parametric family of elliptic curve with the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the generic rank ≥ 4. The construction starts with a Diophantine triple $\{a, b, c\}$. We assign to this triple the elliptic curve E' as in (1.3), and define $d = x(P+Q)$, $e = x(P-Q)$. If $d, e \neq 0$, then $\{a, b, c, d\}$ and $\{a, b, c, e\}$ are Diophantine quadruples (see [18]). If $ed + 1$ is a perfect square (and in [14] a parametric solution to this equation was found), then we may expect that the elliptic curve $y^2 = (bx+1)(dx+1)(ex+1)$, induced by the Diophantine triple $\{b, d, e\}$, has at least four independent points of infinite order, namely, points with x-coordinates 0, a, c and $1/(bde)$. By a specialization, we found an elliptic curve of rank 7 in that family. Here we will improve that result and construct several elliptic curves od the form (1.2) which have rank equal to 8 or 9.

The well-known family of Diophantine quadruples

$$\{k-1, k+1, 4k, 16k^3-4k\}, \quad (k \in \mathbb{Z},\ k \geq 2) \tag{3.4}$$

has been studied by several authors. In [13], it was proved that the fourth element in this quadruple in unique, i.e. if $\{k-1, k+1, 4k, d\}$ is an (integer) Diophantine quadruple, then $d = 16k^3 - 4k$ (see also [28, 6]). It seems natural to consider the families of elliptic curves induced by (3.4). However, in [16] it was shown that the triple $\{k-1, k+1, 4k\}$ induces an elliptic curve over $\mathbb{Q}(k)$ with generic rank equal to 1 (this agrees with the fact that $\{k-1, k+1, 4k\}$ is of the form $\{a, b, a+b+2r\}$). Therefore, we tried to obtain curves with the higher rank induced by other subtriples of (3.4).

We first consider the family of Diophantine triples

$$\{k-1, k+1, 16k^3-4k\}, \quad (k \in \mathbb{Q}).$$

Applying the strategy described in Section 2, we found a curve with the rank equal to 9 for $k = 3593/2323$. We have the Diophantine triple

$$\left\{ \frac{1270}{2323}, \frac{5916}{2323}, \frac{664593861324}{12535672267} \right\},$$

and the corresponding elliptic curve (its minimal Weierstrass equation)

$$\begin{aligned} y^2 &= x^3 - 263759257625979218346701293692x \\ &\quad + 43309770676275925610968063087567021709640976. \end{aligned}$$

Torsion points are

$$\mathcal{O}, [391223566189142, 0], [-581574668058484, 0], [190351101869342, 0],$$

while independent points of infinite order are

$$\begin{gathered} [13382356740992, 6307332780932304905700], \\ [137392393772492, 3108820636640783206800], \\ [151121694899342, 2627033807399227434000], \\ [182390949979797, 1126929502996358494505], \\ [-100285963891570, 8291713851182161095696], \\ [638038681834022, 11608723965551290530480], \\ [-570129376204450, 2892670061337006977376], \\ [-581493416436883, 246987048216416159925], \\ [395944953729830, 974097947650374250704]. \end{gathered}$$

We also found several examples with the rank equal to 8 in this family: $k = 286/69$, $69/1144$, $1169/1268$, $1225/1959$, $1443/1156$, $1981/1941$, $2447/50$, $4350/1159$, $5781/782$.

Next we consider the family

$$\{k - 1, 4k, 16k^3 - 4k\}, \quad (k \in \mathbb{Q}).$$

Note that the triples of the form $\{k+1, 4k, 16k^3 - 4k\}$ induce the same family (by the correspondence $k \leftrightarrow -k$). In this case we found a curve with the rank equal to 9 for $k = -2673/491$, and several examples with the rank equal to 8: $k = 65/521$, $161/7572$, $864/1415$, $909/2741$, $1500/2339$, $1610/4401$, $1914/2969$, $2645/7649$, $3656/5127$, $4312/9957$, $4435/3378$, $5329/7430$, $5346/8611$, $5863/6141$, $5989/6203$, $6648/3473$, $7712/3235$, $-175/2098$, $-291/674$, $-338/911$, $-470/889$, $-535/5178$, $-559/807$, $-705/1703$, $-1120/6329$, $-1224/4555$, $-1241/6164$, $-1443/964$, $-1610/1629$, $-2123/4703$, $-2209/2927$, $-3135/6928$.

We also considered rational Diophantine triples of the form $\{1, 3, c\}$. Here we found two examples with rank equal to 8 for

$$c = \frac{5043716589720}{9928996362961} \quad \text{and} \quad c = \frac{507857302680}{1680262081}.$$

Let us mention that Gibbs discovered 46 examples of rational Diophantine sextuples ([29, 30]). We have computed the ranks for all curves of the form $y^2 = (ax+1)(bx+1)(cx+1)$, where $\{a, b, c\}$ is a subtriple of some of the Gibbs's sextuples, and in that way we found a curve of rank 8 for the Diophantine triple

$$\left\{\frac{494}{35}, \frac{1254396}{665}, \frac{11451300}{5067001}\right\}.$$

Of course, the curves with rank less than 7 (and greater than 0) are easy to find, and they already appeared in the literature (see [16, 22, 14]). Therefore, we can summarize the results from this section in the following proposition:

PROPOSITION 3.1. *For each $1 \le r \le 9$, there exist a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the rank equal to r.*

4. Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

In this section, we consider elliptic curves with a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. It follows from the 2-descent proposition (see [33, 4.1, p.37], [34, 4.2, p.85]), that such curve has the equation of the form

$$y^2 = x(x + x_1^2)(x + x_2^2), \quad x_1, x_2 \in \mathbb{Q} \tag{4.5}$$

(the point $[0, 0]$ is a double point of order 2). Translating the elliptic curve (1.3) induced by the Diophantine triple $\{a, b, c\}$, we obtain the equation

$$y^2 = x(x + ac - ab)(x + bc - ab). \tag{4.6}$$

Therefore, if we can find a, b, c such that $ac - ab$ and $bc - ab$ are perfect squares, then the elliptic curve induced by $\{a, b, c\}$ will have a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

A simple way to fulfill these conditions is to choose a and b such that $ab = -1$. Then $ac - ab = ac + 1 = s^2$ and $bc - ab = bc + 1 = t^2$. It remains to find c such that $\{a, -1/a, c\}$ is a Diophantine triple. Using the standard extension $c = a + b + 2r$, we may take $c = a - \frac{1}{a}$. However, it is easy to prove, using Shioda's formula ([42]), that the family of elliptic curves

$$y^2 = x^3 + (a^4 + 1)x^2 + a^4 x,$$

obtained with this construction, has the generic rank equal to 0. We may ask what happened with the points $P = [0, abc]$ and $Q = [1, rst]$. It is easy to see that $2P = Q = T_3$. Hence, in this case P and Q are indeed points of finite order. We were able to find examples with rank equal to $0, 1, 2, 3, 4$ is this family, but in order to find curves with higher rank, we will consider some other constructions.

We are searching for parametric solutions of the system

$$ac + 1 = \square, \quad -\frac{c}{a} + 1 = \square. \tag{4.7}$$

Multiplying these two conditions, we obtain

$$a(ac+1)(a-c)=\square, \tag{4.8}$$

which, for given c, may be regarded as an elliptic curve. We already know one (non-torsion) parametric solution of (4.8), namely $a=T$, $c=T-\frac{1}{T}$. By duplicating the corresponding point on the elliptic curve (4.8), we obtain another solution $a=\frac{(T^2+1)^2(T^2-1)}{4T^3}$, with the same c. By the 2-descent proposition, these values of a and c also satisfy the original system (4.7). We have again that $Q=T_3$, but now the point P has infinite order.

By the search for curves with high rank in this family of elliptic curves, with the methods described in Section 2, we were able to find two curves with rank equal to 5, for $T=12/5$ and $T=24/7$, corresponding to the Diophantine triples

$$\left\{\frac{3398759}{864000},\ -\frac{864000}{2298759},\ \frac{119}{60}\right\},$$

$$\left\{\frac{205859375}{18966528},\ -\frac{18966528}{205859375},\ \frac{527}{168}\right\}.$$

We will improve this result by considering a different parametric solution of the system (4.7). Inserting $ac+1=s^2$ into $-\frac{c}{a}+1=t^2$, we obtain

$$1-s^2+a^2=\square.$$

which has the solution of the form

$$a=\frac{\alpha T+1}{T-\alpha},\quad s=\frac{T+\alpha}{T-\alpha}.$$

We take $\alpha=2$, which gives

$$a=\frac{2T+1}{T-2},\quad b=\frac{2-T}{2T+1},\quad c=\frac{8T}{(2T+1)(T-2)}.$$

This yields again the family of elliptic curves with generic rank ≥ 1. We were able to find in this family several examples of curves with rank equal to 6, e.g. for $T=399/160$, $452/173$, $698/561$, $1212/661$, $1253/974$, $1263/707$, $1463/1081$.

We give some detail only for $T=399/160$. We obtain the Diophantine triple

$$\left\{\frac{958}{79},\ -\frac{79}{958},\ \frac{255360}{37841}\right\},$$

and the corresponding elliptic curve (its minimal Weierstrass equation) is

$$\begin{aligned} y^2 &= x^3-x^2-46646306956505964064 00x \\ &\quad +12261165772114501874084165440000 0. \end{aligned}$$

Torsion points:

$$\mathcal{O}, [39113956000, 0], [-78863002400, 0], [39749046401, 0],$$
$$[31069796800, -2770416472639200], [31069796800, 2770416472639200],$$
$$[48428296002, 3207868011028802], [48428296002, -3207868011028802].$$

Independent points of infinite order:

$$[28260480960, 3654766624544480],$$
$$[-12857421920, 13433587750450560],$$
$$[13143969210, 7973123554358270],$$
$$[34512505410, 1652834075535170],$$
$$[91860783045, 21662718643569190],$$
$$[38608886722, 260090980468158].$$

We note that this is the curve with the second smallest conductor among all known curves with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank equal to 6 (see [17]).

Hence, we have proved the following result.

Proposition 4.1. *For each $0 \leq r \leq 6$, there exist a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the rank equal to r.*

5. Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

General form of curves with the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is

$$y^2 = (x+\alpha^2)(x+\beta^2)\left(x + \frac{\alpha^2\beta^2}{(\alpha-\beta)^2}\right)$$

(then the point $[0, \alpha^2\beta^2/(\alpha-\beta)]$ is of order 3; see [35]). Let us force a Diophantine triple equation

$$y^2 = (x+bc)(x+ac)(x+ab) \tag{5.9}$$

to have this form.

Comparison gives

$$\alpha^2 + 1 = bc + 1 = t^2, \tag{5.10}$$

$$\beta^2 + 1 = ac + 1 = s^2, \tag{5.11}$$

$$\alpha^2\beta^2 + (\alpha-\beta)^2 = \square. \tag{5.12}$$

The first two conditions (5.10) and (5.11) have parametric solutions

$$\alpha = \frac{2u}{u^2-1}, \quad \beta = \frac{v^2-1}{2v}.$$

Inserting this into (5.12), we obtain the equation $F(u,v) = z^2$, where

$$\begin{aligned} (5.13)\ F(u,v) &= (v^4 - 2v^2 + 1)u^4 + (-8v^3 + 8v)u^3 \\ &\quad + (2v^4 + 2 + 12v^2)u^2 + (-8v + 8v^3)u + v^4 - 2v^2 + 1. \end{aligned}$$

The condition $F(u,v) = z^2$ is satisfied e.g. for

$$u = \frac{v^3 + v}{v^2 - 1}.$$

Indeed, then $F(u,v) = \frac{(v^6 - v^4 + 3v^2 + 1)^2}{(v-1)^2(v+1)^2}$. Hence, for

$$\alpha = \frac{2T^5 - 2T}{T^6 + T^4 + 3T^2 - 1}, \quad \beta = \frac{T^2 - 1}{2T},$$

we obtain the parametric family of Diophantine triple equations with the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. It is easy to check that the point $[1, rst]$ on (5.9) has an infinite order (by finding a suitable specialization, or by listing explicitly all 12 torsion points on (5.9) over $\mathbb{Q}(T)$. Hence, we found an elliptic curves over $\mathbb{Q}(T)$ with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and the generic rank ≥ 1, which ties the current record ([7, 35, 37]).

Since the constructed curve over $\mathbb{Q}(T)$ has very large coefficients, it is not surprising that we were able to compute the rank only for few specializations, and among them we found examples with rank equal to $1, 2, 3$. Rank 3 is obtained for $T = 7$, which corresponds for the Diophantine triple

$$\left\{ \frac{721176}{193193}, \frac{20580000}{829322351}, \frac{662376}{210343} \right\}.$$

Instead of using a parametric solution, we could also try to search for solutions u, v of the equation (5.13) with small heights, and to compute the rank of corresponding elliptic curves. Using this approach we were able to find a curve with rank equal to 4. It is obtained for $u = 34/35$ and $v = 8$, i.e. for the Diophantine triple

$$\left\{ \frac{39123}{96976}, \frac{12947200}{418209}, \frac{42427}{1104} \right\}.$$

The curve is

$$\begin{aligned} y^2 + xy &= x^3 - 2404664908479524358995256239 0x \\ &\quad + 1435226116741326558309046453105518735800100. \end{aligned}$$

Torsion points:

$$\begin{gathered}\mathcal{O}, [-179058763357620, 89529381678810],\\ [89873668514380, -44936834257190],\\ [356740379372959/4, -356740379372959/8],\\ [92726794888780, -5240587359724741559 0],\\ [92726794888780, 5240578087045252681 0],\\ [86369148214060, 5117989943863301641 0],\\ [154777835944300, 11921506158324961140 10],\\ [37033400507980, -7716782092566717227 90],\\ [86369148214060, -5117998580778123047 0],\\ [154777835944300, -11921507706103320583 10],\\ [37033400507980, 7716781722232712148 10].\end{gathered}$$

Independent points of infinite order:

$$\begin{gathered}[35387651068492, 792834860571692154586],\\ [-39964997451020, -1527225651415581670190],\\ [-8547561811220, -1280680222922667973190],\\ [90070190194252, 684191408652585442 6].\end{gathered}$$

PROPOSITION 5.1. *For each $1 \leq r \leq 4$, there exist a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and the rank equal to r.*

6. TORSION GROUP $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

Finally, we consider the largest possible torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. As we have already noted in Section 6, the torsion group of elliptic curves induced by Diophantine triples of the form

$$\{a, -\frac{1}{a}, a - \frac{1}{a}\}$$

contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In that case, the points of order 4 on

$$y^2 = (x+ab)(x+ac)(x+bc)$$

are $P = [0, abc]$, $P + T_1$, $P + T_2$, $P + T_3$, where $T_1 = [-bc, 0]$, $T_2 = [-ac, 0]$, $T_3 = [-ab, 0]$. Hence, our elliptic curve will have the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if some of the points $P, P+T_1, P+T_2, P+T_3$ is a double point. We will use 2-descent proposition again. Consider the point $P+T_2$. It will be a double point iff $(b-a)(b-c)$ and $b(b-a)$ are both perfect squares.

These conditions leads to a single condition that $a^2 + 1$ is a perfect square. Therefore, we have proved that all Diophantine triples of the form

$$\left\{ \frac{2T}{T^2 - 1}, -\frac{1 - T^2}{2T}, \frac{6T^2 - T^4 - 1}{2T(T^2 - 1)} \right\}, \quad t \in \mathbb{Q},$$

induce elliptic curves with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. The induced curves have the equation of the form

$$y^2 = x(x + s^2)(x + t^2) = \left(x + \left(\frac{2T}{T^2 - 1} \right)^2 \right) \left(x + \left(\frac{T^2 - 1}{2T} \right)^2 \right). \tag{6.14}$$

But, according to [35], *every* elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ has an equation of the form (6.14). Therefore, every such curve is induced by a Diophantine triple. This fact has been independently proved by Campbell and Goins in [8].

Thus, we are left with the question which ranks are possible for the elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. It is known that there exist infinitely many such curves with rank ≥ 1 (see [1, 8, 35, 37]), although no such parametric family (curve over $\mathbb{Q}(T)$) is known. It is easy to find examples with rank equal to $0, 1, 2$. The first example with rank equal to 3 was found in 2000, independently, by Connell [9] and the author [17]. It was the curve

$$\begin{aligned} y^2 + xy &= x^3 - 15745932530829089880x \\ &\quad + 24028219957095969426339278400, \end{aligned}$$

with torsion points:

$$\begin{gathered} \mathcal{O}, [-4581539664, 2290769832], [-1236230160, 203972501847720], \\ [2132310660, 12167787556920], [2452514160, 12747996298920], \\ [9535415580, 860741285907000], [2132310660, -12169919867580], \\ [-1236230160, -203971265617560], [9535415580, -860750821322580], \\ [2452514160, -12750448813080], [2346026160, -1173013080], \\ [1471049760, 63627110794920], [1471049760, -63628581844680], \\ [3221002560, -82025835631080], [3221002560, 82022614628520], \\ [8942054015/4, -8942054015/8], \end{gathered}$$

and independent points of infinite order:

$$\begin{gathered} [2188064030, -7124272297330], \\ [396546810000/169, 1222553114825160/2197], \\ [16652415739760/3481, 49537578975823615480/205379]. \end{gathered}$$

The curve is induced by the Diophantine triple

$$\left\{\frac{408}{145}, -\frac{145}{408}, -\frac{145439}{59160}\right\}.$$

In the meantime, several other curves with rank equal to 3 were found by Rathbun [40], Campbell and Goins [8], and the author (see also [5]). Here we will mention our findings. Using a similar search procedure, as in the previous sections, we have discovered elliptic curves with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the rank equal to 3, which correspond to the following Diophantine triples:

$$\left\{\frac{1692}{1885}, -\frac{1885}{1692}, -\frac{690361}{3189420}\right\},$$

$$\left\{\frac{79040}{35409}, -\frac{35409}{79040}, \frac{4993524319}{2798727360}\right\},$$

$$\left\{\frac{77556}{59917}, -\frac{59917}{77556}, \frac{2424886247}{4646922852}\right\},$$

$$\left\{\frac{128760}{176111}, -\frac{176111}{128760}, -\frac{14435946721}{22676052360}\right\},$$

$$\left\{\frac{424580}{799029}, -\frac{799029}{424580}, -\frac{458179166441}{339251732820}\right\},$$

$$\left\{\frac{451352}{974415}, -\frac{974415}{451352}, -\frac{745765964321}{439804159080}\right\}.$$

We give some details on the curve corresponding to the last triple, since this case was the most technically involved and time consuming. Its minimal Weierstrass equation is

$$\begin{aligned} y^2 + xy = x^3 &- 16188503722614063108729139735755154904562292360x \\ &+ 78686342180820646396991349549089246934687470944705359290136652576160 0. \end{aligned}$$

Torsion points are:

$$
\begin{gathered}
\mathcal{O}, [12694211377166339810192\,0, 2788268057400124024570423636339724\,0], \\
[1269421137716633981019 20, -278826805741281823594758997614991 60], \\
[302282645996304248787 20, -180314742477593435572519451048011 60], \\
[302282645996304248787 20, 180314742477291152926523146799224 40], \\
[422083239655931288586 320, -262963676295121325354530570456161 160], \\
[853927741259869946781 80, -521152175438976912754545148140172 0], \\
[-616136338580429707986 40, 393750660831784609709563126480948 40], \\
[619060751627782799418 20, 468435613507118054294629969450484 0], \\
[853927741259869946781 80, 521152175430437635341946448672354 0], \\
[422083239655931288586 320, 262963676294699242114874639167574 840], \\
[619060751627782799418 20, -468435613513308661810907797444666 0], \\
[-616136338580429707986 40, -393750660831168473370982696772962 00], \\
[682098693468748096320 16, -341049346734374048160 08], \\
[785851891856469114903 20, -392925945928234557451 60], \\
[-58718023413008688448934 5/4, 58718023413008688448934 5/8],
\end{gathered}
$$

while independent points of infinite order are:

$$
\begin{aligned}
P_1 &= [66119657073815781066800, -235533912891856596972107638410484 0], \\
P_2 &= [40116928726567283455086750008 0/76335169, \\
&\quad -1766991837439446436075441826081025535317266548 0/666940371553],
\end{aligned}
$$

$$
\begin{aligned}
P_3 = {} & [2896876482219215018082911215320035879728511402808525430701422369503553764372274905368126231831 20/ \\
& 171569146751947991648728128956962969086159771786235917146627023348729558 81, \\
& -161795490883472534487019560345841603273179322736323582039456980965774463381 9\ldots \\
& \ldots 656062208905822304087388210043858968407239618913517436708870237508440/ \\
& 710654952840031353548423631635783739978236980380973194 8\ldots \\
& \ldots 0954479040616074792502966798554498341539450071275232779].
\end{aligned}
$$

In this case, we were not able to compute the exact rank using *mwrank* (we obtained that rank is equal to 2 or 3). Namely, the coordinates of the points P_3 are to large to be found by 2-descent. Therefore, here we used 4-descent implemented in *MAGMA*.

Let us summarize the results from this section.

PROPOSITION 6.1. *For each $0 \leq r \leq 3$, there exist a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the rank equal to r.*

ACKNOWLEDGEMENTS.
The author was supported by the Ministry of Science, Education and

Sports, Republic of Croatia, Grant 0037110. The experiments reported in this paper were performed on the computers of the Laboratory for Advanced Computations, Department of Mathematics, University of Zagreb. The author would like to thank Randall Rathbun for his generous help with computations involving 4-descent, which were essential in computing the exact rank for two curves of rank equal to 3 in Section 6.

References

[1] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), 399–405.

[2] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) **20** (1969), 129–137.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, The Computer Algebra System PARI - GP, Université Bordeaux I, 1999, `http://pari.math.u-bordeaux.fr/`

[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265 (1997).

[5] T. D. Brooks, E. A. Fowler, K. C. Hastings, D. L. Hiance, M. A. Zimmerman, *Elliptic curves with torsion subgroup* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*: does a rank* 4 *curve exist?*, The Journal of the SUMSRI, Summer 2006.

[6] Y. Bugeaud, A. Dujella and M. Mignotte, *On the family of Diophantine triples* $\{k-1, k+1, 16k^3 - 4k\}$, preprint.

[7] G. Campbell, Finding Elliptic Curves and Families of Elliptic Curves over $\mathbb{Q}$ of Large Rank, Dissertation, Rutgers University, 1999.

[8] G. Campbell and E. H. Goins, *Heron triangles, Diophantine problems and elliptic curves*, preprint.

[9] I. Connell, APECS, `ftp://ftp.math.mcgill.ca/pub/apecs/`

[10] J. Cremona, Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge, 1997.

[11] L. E. Dickson, History of the Theory of Numbers, Vol. 2, Chelsea, New York, 1966, pp. 513–520.

[12] Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers, (ed. I. G. Bashmakova), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

[13] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

[14] A. Dujella, *Diophantine triples and construction of high-rank elliptic curves over* $\mathbb{Q}$ *with three non-trivial* 2*-torsion points*, Rocky Mountain J. Math. **30** (2000), 157–164.

[15] A. Dujella, *Irregular Diophantine m-tuples and elliptic curves of high rank*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), 66–67.

[16] A. Dujella, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.

[17] A. Dujella, *High rank elliptic curves with prescribed torsion*, `http://web.math.hr/~duje/tors/tors.html` (2000–2006)

[18] A. Dujella, *Diophantine* m*-tuples and elliptic curves*, J. Theor. Nombres Bordeaux **13** (2001), 111–124.

[19] A. Dujella, *An example of elliptic curve over* $\mathbb{Q}$ *with rank equal to* 15, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), 109–111.

[20] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[21] A. Dujella, *History of elliptic curves rank records* , `http://web.math.hr/~duje/tors/rankhist.html` (2006)

[22] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[23] A. Dujella and A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.

[24] N. D. Elkies, *Algorithmic Number Theory: Tables and Links*, `http://www.math.harvard.edu/~elkies/compnt.html` (2002–2006)

[25] N. D. Elkies, $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$, *etc.*, Number Theory Listserver, May 2006.

[26] N. D. Elkies and N. F. Rogers, *Elliptic curves* $x^3 + y^3 = k$ *of high rank*, Proceedings of ANTS-6 (ed. D. Buell), Lecture Notes in Comput. Sci. **3076** (2004), 184–193.

[27] P. Fermat, Observations sur Diophante, Oeuvres de Fermat, Vol. 1 (eds. P. Tannery and C. Henry), 1891, p. 303.

[28] Y. Fujita, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, preprint.

[29] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), to appear.

[30] P. Gibbs, *A generalised Stern-Brocot tree from regular Diophantine quadruples*, preprint, `math.NT/9903035`.

[31] R. K. Guy, Unsolved Problems in Number Theory, 3rd edition, Springer-Verlag, New York, 2004, Section D29, p. 310.

[32] T. L. Heath, Diophantus of Alexandria. A Study of the History of Greek Algebra, Dover, New York, 1964, pp. 179–182.

[33] D. Husemöller, Elliptic Curves, Springer-Verlag, New York, 1987.

[34] A. Knapp, Elliptic Curves, Princeton Univ. Press, 1992.

[35] L. Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over* $\mathbb{Q}$, Acta Arith. **108** (2003), 339–356.

[36] L. Kulesz and C. Stahlke, *Elliptic curves of high rank with nontrivial torsion group over* $\mathbb{Q}$, Experiment. Math. **10** (2001), 475–480.

[37] O. Lecacheux, Personal communications, 2002.

[38] J.-F. Mestre, *Construction de courbes elliptiques sur* $\mathbb{Q}$ *de rang* ≥ 12, C. R. Acad. Sci. Paris Ser. I **295** (1982) 643–644.

[39] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993) 291–293.

[40] R. Rathbun, Personal communications, 2003–2006.

[41] N. F. Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. **9** (2000), 591-Ű594.

[42] T. Shioda, *On the Mordell - Weil lattices*, Comment. Math. Univ. St. Pauli **39** (1990), 211–240.

[43] M. Waldschmidt, Open Diophantine problems, *Moscow Math. J.* **4** (2004), 245–305.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb
Croatia
E-mail: `duje@math.hr`