Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Andrej Dujella and Juan Carlos Peral

Abstract. We show the existence of families of elliptic curves over $\mathbb{Q}$ whose generic rank is at least 2 for the torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Also in both cases we prove the existence of infinitely many elliptic curves, which are parameterized by the points of an elliptic curve with positive rank, with such torsion group and rank at least 3.

These results represent an improvement of previous results by Campbell, Kulesz, Lecacheux, Dujella and Rabarison where families with rank at least 1 were constructed in both cases.

1. Introduction

The construction of families of elliptic curves having high rank often is based in two basic strategies as mentioned by Elkies in [**El**].

a) The Néron method studies the pencil of cubics passing through a set of nine rational random points and then looks for independence. See [**Sh**] for a detailed description of the method. Families of rank up to 10 where constructed in this way.

b) The Mestre method uses polynomial identities forcing the existence of rational points in the curve and then searches for independence conditions. In this way Mestre was able to construct a rank 11 curve over $\mathbb{Q}(u)$, see [**Me**].

In our case we want the curve to have a predetermined torsion group, $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, so we start from the general model for such torsion and then try to impose the existence of new points. One way to do this is by looking for good quadratic sections. Also, the method developed by Lecacheux [**Le1**], [**Le2**], can be used in these cases. In her method Lecacheux uses fibrations of the corresponding surfaces, as the ones given explicitly in Beauville [**Be**]. Other fibrations such as the ones in Bertin and Lecacheux [**BL**] or in Livné and Yui [**LY**], can also be used in order to find elliptic curves with positive rank over $\mathbb{Q}(u)$. Another useful tool in the search for high rank curves over $\mathbb{Q}(u)$ are diophantine triples. In fact, for the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we have constructed a rank 4 family using such triples, this is the current record for this torsion group, see the preprint [**DP**].

Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ and rank at least 1 over $\mathbb{Q}(u)$ have been found by several authors, see [**Ku**], [**Le1**], [**Le2**] and [**Ra**]. In this paper we prove the existence of two elliptic curves having this torsion group and rank at least

2010 *Mathematics Subject Classification.* 11G05.

A. D. was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821 and by the Croatian Science Foundation under the project no. 6422. J. C. P. was supported by the UPV/EHU grant EHU 10/05.

2 over $\mathbb{Q}(u)$, and we also show the existence of infinitely many elliptic curves over $\mathbb{Q}$ with this torsion group and rank at least 3, parametrized by the points of an elliptic curve with positive rank.

Elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 1 over $\mathbb{Q}(u)$ have been constructed by several authors, see [**Ca**], [**Ku**], [**Le1**], [**Du1**] and [**Ra**]. Here we prove the existence of three elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and whose rank over $\mathbb{Q}(u)$ is at least 2. We prove also the existence of infinitely many elliptic curves with this torsion group and rank at least 3 over $\mathbb{Q}$, parametrized by the points of an elliptic curve of positive rank.

The paper is organized as follows. First, we describe the model for the elliptic curves having each of these torsion groups. Then, in both cases, we show the existence of several families having rank at least 1 over $\mathbb{Q}(u)$. In another section we show the existence of two families in the $\mathbb{Z}/8\mathbb{Z}$ case and three families in the case of torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ having rank at least 2 over $\mathbb{Q}(u)$. In all the cases we describe the coefficients of the families and the coordinates of independent points. We give also the details for the rank 3 results. Finally we exhibit some examples of curves with high rank. The current records both for families and for individual curves can be found in [**Du2**]. One way to find high rank elliptic curves over $\mathbb{Q}$ is the construction of elliptic curves with positive rank over $\mathbb{Q}(u)$, as high as possible, and then searching for good specializations with adequate sieving tools such as the Mestre-Nagao sums and the Selmer group for example.

2. Torsion group

2.1. Curves with torsion group $\mathbb{Z}/8\mathbb{Z}$. The Tate normal form for an elliptic curve is given by

$$E(b,c): \quad y^2 + (1-c)xy - by = x^3 - bx^2$$

(see [**Kn**]). It is nonsingular if and only if $b \neq 0$. Using the adition law for $P = (0,0)$ and taking $d = b/c$ we have

$$\begin{aligned} 4P =&(d(d-1), d^2(c-d+1)),\\ -4P =&(d(d-1), d(d-1)^2) \end{aligned}$$

so P is a torsion point of order 8 for b and c as follows

$$\begin{aligned} b =&(2v-1)(v-1),\\ c =&\frac{(2v-1)(v-1)}{v} \end{aligned}$$

with v a rational, see [**Kn**]. For these values of b and c we can write the curve in the form $y^2 = x^3 + A_8(v)x^2 + B_8(v)x$ where

$$\begin{aligned} A_8(v) =&1 - 8v + 16v^2 - 16v^3 + 8v^4,\\ B_8(v) =&16(-1+v)^4v^4. \end{aligned}$$

Writing the curve in this form is a convenient way to search for candidates for new rational points. In fact their x-coordinates should be either divisors of B or rational squares times divisors of B.

2.2. Curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Using again the Tate normal form and the addition law for the point $P=(0,0)$ we find

$$\begin{aligned} 3P &= (c, b-c), \\ -3P &= (c, c^2). \end{aligned}$$

It follows that P will be a torsion point of order 6 for $b=c+c^2$. For this value of b we write the curve in the form $y^2=x^3+A_6(c)x^2+B_6(c)x$, where

$$\begin{aligned} A_6(c) &= -1+6c-3c^2, \\ B_6(c) &= -16c^3. \end{aligned}$$

In the new coordinates the torsion point of order 6 becomes $(-4c, 4c(1+c))$. Now we use the fact that the curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ have a model $y^2=x(x-m)(x-n)$. So in order to get a curve with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ it is enough that in the family above the polynomial

$$x^3+A_6(c)x^2+B_6(c)x = x(-16c^3+x+6cx-3c^2x+x^2)$$

factorizes into linear factors. So the discriminant $\Delta=(1+c)^3(1+9c)$ of the second order polynomial must be a square. Hence we have to parametrize the conic $(1+c)(1+9c)=$ Square and we get

$$c=\frac{-v^2+1}{2(3v-5)}.$$

For these values of c the corresponding curves have torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and can be written as $y^2=x^3+A_{26}(v)x^2+B_{26}(v)x$ where

$$\begin{aligned} A_{26}(v) &= 37-84v+102v^2-36v^3-3v^4, \\ B_{26}(v) &= 32(-1+v)^3(1+v)^3(-5+3v). \end{aligned}$$

The torsion point of order 6 transforms into

$$(8(-1+v)(1+v)(-5+3v), 8(-3+v)^2(-1+v)(1+v)(-5+3v)).$$

Remark 2.1. The cases treated here, jointly with the general curve having torsion $\mathbb{Z}/7\mathbb{Z}$ and whose model is

$$y^2=x^3+x^2(1-2t+3t^2+6t^3+t^4)+x(-8t^2(1+t)(-1+t+t^2))+16t^4(1+t)^2,$$

are the three cases in which the general model for such torsion group is a $K3$ surface, see [**El**].

3. Search for new rational points

Here we explain how we get new points in our families of curves. The idea is as follows:

1) All the curves in the paper have a model $y^2=x^3+Ax^2+Bx$. This is due to the fact that all of them have at least one torsion point of order two.

2) In these cases it is well known that the x-coordinates of rational points should be either divisors of B or rational squares times divisors of B.

3) We know some of the divisors of B, namely the polynomial factors of B.

4) So we construct the list of all such known divisors of B and we look for those that become a new point after parametrizing a conic.

If d is a divisor of B, we try to force d to be the x-coordinate of a new point, so we have to impose that $d^3 + Ad^2 + Bd = d^2(d + A + B/d)$ is a square. So for every known divisor of B we consider the equation

$$d + A + \frac{B}{d} = \text{Square}$$

In same cases this equation is equivalent to solving a conic and in this way we get a new point in the curve.

Now we try the same with a divisor of B, say d, times a rational square, say $\frac{U^2}{V^2}$, and we get the following equations

$$d^3\frac{U^6}{V^6} + Ad^2\frac{U^4}{V^4} + Bd\frac{U^2}{V^2} = \frac{d^2U^2}{V^6}\left(dU^4 + AU^2V^2 + V^4\frac{B}{d}\right) = \text{Square}$$

These equations describe the homogeneous spaces corresponding to the pair (U, V). Again in some cases this equation is equivalent to solving a conic and in this way we get a new point in the curve.

We do the same for the associated curve $y^2 = x^3 - 2Ax^2 + (B^2 - 4A)x$.

Finally we check the independence of the new point with the respect to the old ones.

4. Rank 1 families

4.1. The case of torsion group $\mathbb{Z}/8\mathbb{Z}$. For this torsion group we show ten conditions upon v leading to rank 1 families. Some of them were already known: the fourth family was found by Kulesz [**Ku**] and the third and seventh family were found by Lecacheux [**Le1**]. Also, Rabarison [**Ra**] found a family which is not in our list. We first list eight values of x_i which becomes the x-coordinate of a new point once we specialize to the corresponding values of v_i, $i = 1\ldots, 8$. We include another two values, v_9 and v_{10}, found by Lecacheux by using an adequate fibration of the general model with torsion group $\mathbb{Z}/8\mathbb{Z}$.

$$x_1 = \frac{-16v^4(1-4v+2v^2)}{(-1+4w)^2}, \qquad v_1 = \frac{1+w^2}{3-2w+w^2},$$

$$x_2 = \frac{-(-1+v)^4(-5+8v)(-5+18v)}{4(-2+3v)^2}, \qquad v_2 = \frac{5(1+w^2)}{2(9+4w^2)},$$

$$x_3 = \frac{-4(-3+v)(-1+v)^2v^4(-1+3v)}{(1-4v+2v^2)^2}, \qquad v_3 = \frac{1+3w^2}{3+w^2},$$

$$x_4 = 16(-1+v)^2v^2(1-2v+2v^2), \qquad v_4 = \frac{(-2+w)w}{-2+w^2},$$

$$x_5 = \frac{-64(-1+v)^2v^2(-1-v+v^2)}{(-1-4v+4v^2)^2}, \qquad v_5 = \frac{(-2+w)w}{1+w^2},$$

$$x_6 = -(-1+v)^2(1-6v+4v^2), \qquad v_6 = \frac{2-2w+w^2}{4+w^2},$$

$$x_7 = 4v^4, \qquad v_7 = \frac{-5+w^2}{4(1+w)},$$

$$x_8 = \frac{-(-1+v)^2(-5+2v)^2(25-70v+36v^2)}{(-7+6v)^2}, \qquad v_8 = \frac{34-6w+w^2}{36+w^2}.$$

$$v_9 = \frac{w^2+12}{2(w^2+4)}, \quad v_{10} = \frac{-2w}{1-w+w^2}.$$

Details of one of these cases is given in Section 5. In every case the new point is of infinite order so the rank of the corresponding curve is at least 1 over $\mathbb{Q}(w)$.

4.2. The case of torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. We have found several conditions upon v leading to rank 1 families. In the next table we list nine values of x_i which becomes the x-coordinate of a new point once we specialize to the value of $v_i, i = 1 \ldots, 9$. Families with this torsion group and rank at least 1 have been found by several authors. The third family was found by Kulesz [**Ku**]. Other families were found by Lecacheux [**Le2**], Rabarison [**Ra**] and Dujella [**Du1**].

$$x_1 = 8(-1+v)^3(1+v), \qquad v_1 = \frac{3(-1+w)(1+w)}{-29-8w+w^2},$$

$$x_2 = 4(1+v)^3, \qquad v_2 = \frac{3(-3+w)(3+w)}{-45-24w+w^2},$$

$$x_3 = 2(-1+v)(1+v)^2(-5+3v), \qquad v_3 = \frac{-7+w^2}{1-4w+w^2},$$

$$x_4 = -16(-1+v)^2(1+v), \qquad v_4 = \frac{-11+w^2}{5-4w+w^2},$$

$$x_5 = 16(-5+3v)(3v-7)^2, \qquad v_5 = \frac{3(261+w^2)}{153-24w+w^2},$$

$$x_6 = 16(1+v)(v-5)^2, \qquad v_6 = \frac{135-w^2}{141+24w+w^2},$$

$$x_7 = \frac{4(-1+v)^2(1+v)^2(41-54v+49v^2)}{(-1+3v)^2}, \qquad v_7 = \frac{41-w^2}{2(27+7w)},$$

$$x_8 = (-5+3v)(3v-1)^2, \qquad v_8 = \frac{3}{5-w^2},$$

$$x_9 = \frac{2(v-1)(v+1)^3(3v-1)^2}{(2v+2)^2}, \qquad v_9 = \frac{-7-2w^2}{3(-3+2w^2)}.$$

More details are given in Section 6. In every case the new point is of infinite order so the rank of the curve is at least 1 over $\mathbb{Q}(w)$.

5. Rank 2 families for the torsion group $\mathbb{Z}/8\mathbb{Z}$

5.1. A family with rank 1. We present here some details for the family in which we have found two subfamilies with torsion $\mathbb{Z}/8\mathbb{Z}$ and generic rank at least 2. It corresponds to the third entry in the table of Section 4.1 of rank 1 families above and it is a reparametrization of one of the families in [**Le1**]. By inserting in the general family $y^2 = x^3 + A_8(v)x^2 + B_8(v)x$ the value $v = v_3(w)$ we get the rank 1 family given by $y^2 = x^3 + AA_8(w)x^2 + BB_8(w)x$ where

$$\begin{aligned} AA_8(w) =& -31 - 148w^2 + 214w^4 - 116w^6 + 337w^8, \\ BB_8(w) =& 256(-1+w)^4(1+w)^4(1+3w^2)^4. \end{aligned}$$

By searching on several homogeneous spaces of the associated curve we have found the possibility of imposing two new conditions which lead to new points. Observe that the associated curve is $y^2 = x^3 + AAS_8(w)x^2 + BBS_8(w)x$ where,

$$\begin{aligned} AAS_8(w) =& -2(-31 - 148w^2 + 214w^4 - 116w^6 + 337w^8), \\ BBS_8(w) =& (3+w^2)^2(-1+5w^2)^4(-7-26w^2+49w^4). \end{aligned}$$

For the homogeneous space $(U, V) = (2, 1)$, we find that forcing

$$2^2(3+w^2)(-1+5w^2)^2$$

to be the x-coordinate of a new point in the associated curve is equivalent to solve $11 + 25w^2 =$ Square, so we have $w_1 = \frac{11-u^2}{10u}$.

For the homogeneous space $(U, V) = (2w, 1)$, we find that forcing

$$(2w)^2(3+w^2)^2(-1+5w^2)$$

to be the x-coordinate of a new point in the associated curve is equivalent to solve $7 + 29w^2 =$ Square, so we get $w_2 = \frac{29-12u+u^2}{-29+u^2}$.

Equivalently, for the the initial curve the x-values that become the x-coordinate of a new point, and the specialization values of w are x_1, w_1 and x_2, w_2 given by:

$$\begin{aligned} x_1 &= \frac{(-1+w)^2(1+w)^2(5+7w^2)^2(11+25w^2)}{16}, & w_1 &= \frac{11-u^2}{10u}, \\ x_2 &= \frac{(-1+w)^2(1+w)^2(1+11w^2)^2(7+29w^2)}{16w^2}, & w_2 &= \frac{29-12u+u^2}{-29+u^2}. \end{aligned}$$

With these substitutions we get two families of rank at least 2 over $\mathbb{Q}(u)$.

5.2. First family with rank 2 and torsion group $\mathbb{Z}/8\mathbb{Z}$. Once we insert w_1 into the coefficients AA_8, BB_8 we get as new coefficients AAA_8, BBB_8 given by

$$\begin{aligned} AAA_8 =& 337u^{16} - 41256u^{14} + 4047356u^{12} - 288332632u^{10} + 2363813190u^8 \\ & - 34888248472u^6 + 59257339196u^4 - 73087520616u^2 + 72238942897, \\ BBB_8 =& 256\,(363+34u^2+3u^4)^4\,(11+u)^4\,(-11+u)^4\,(-1+u)^4\,(1+u)^4. \end{aligned}$$

The x-coordinates of two independent infinite order points are

$$X_1 = \frac{2^{12}5^2(-11+u)^2(-1+u)^2u^2(1+u)^2(11+u)^2(-11+u^2)^2(363+34u^2+3u^4)^4}{(102487-303468u^2+43482u^4-2508u^6+7u^8)^2},$$

$$X_2 = \frac{(-11+u)^2(-1+u)^2(1+u)^2(11+u)^2(11+u^2)^2(847+346u^2+7u^4)^2}{64u^2}.$$

The x-coordinate of the torsion point of order 8 is:

$$T = -8(-11+u)(-1+u)(1+u)(11+u)(363+34u^2+3u^4)^3.$$

That the rank of this curve is at least 2 over $\mathbb{Q}(u)$ can be proved using a specialization argument. For example, take $u = 3$. The curve is

$$Y^2 = X^3 + (-20767901155328)X^2 + (114143545210464322134736896)X$$

and its rank is 2. The points with the x-coordinate above, for $u = 3$, are

$$\left(\frac{31240494485235302400}{12061729}, \frac{5520859784048816447930184499920}{41890384817}\right)$$

and

$$\left(\frac{102874768998400}{9}, \frac{2485293332380726066720}{27}\right)$$

Since they are independent, it follows that the family has rank at least 2 over $\mathbb{Q}(u)$.

5.3. Second family with rank 2 and torsion group $\mathbb{Z}/8\mathbb{Z}$. Once we insert w_2 into the coefficients AA_8, BB_8 we get as new coefficients aaa_8, bbb_8 given by

$$\begin{aligned}
aaa_8 = {} & 500246412961 - 2069985157080u + 3162080774436u^2 - 2895517882032u^3 + \\
& 1873181389706u^4 - 906769167048u^5 + 333391978480u^6 - 93284915496u^7 + \\
& 19860033555u^8 - 3216721224u^9 + 396423280u^{10} - 37179432u^{11} + \\
& 2648426u^{12} - 141168u^{13} + 5316u^{14} - 120u^{15} + u^{16}, \\
bbb_8 = {} & 256(-6+u)^4u^4(-29+6u)^4(841 - 522u + 137u^2 - 18u^3 + u^4)^4.
\end{aligned}$$

The x-coordinates of two independent infinite order points are

$$X_1 = \frac{64(-6+u)^2u^2(-29+6u)^2(-29+u^2)^2(29-12u+u^2)^2 \times (841-522u+137u^2-18u^3+u^4)^4}{(707281 - 292668u - 200158u^2 + 168432u^3 - 46685u^4 + 5808u^5 - 238u^6 - 12u^7 + u^8)^2},$$

$$X_2 = \frac{(-6+u)^2u^2(-29+6u)^2(87-29u+3u^2)^2(2523-1914u+541u^2-66u^3+3u^4)^2}{4(29-12u+u^2)^2}.$$

The x-coordinate of the torsion point of order 8 is:

$$T = 8(-6+u)u(-29+6u)(841 - 522u + 137u^2 - 18u^3 + u^4)^3.$$

That the rank of this curve is at least 2 over $\mathbb{Q}(u)$ can be proved using a specialization argument. For example, take $u = 4$. The curve is

$$Y^2 = X^3 + (-122007679)X^2 + (3778019983360000)X$$

and its rank is 2. The points with the x-coordinate above, for $u = 4$, are

$$\left(\frac{897870061670400}{14753281}, \frac{3325049714905607270400}{56667352321}\right)$$

and

$$\left(\frac{648211600}{9}, \frac{3056977617200}{27}\right)$$

Since they are independent, it follows that the family has rank at least 2 over $\mathbb{Q}(u)$.

REMARK 5.1. When we use $w_3 = \frac{(-3+u)(3+u)}{7-6u}$ and $w_4 = \frac{(-3+u)(3+u)}{11-6u}$ in the family of rank at least 1 corresponding to v_{10} we get two families of rank at least 2. They are a reparametrization of the two families above. So we have the following observation: when we specialize in the general family with torsion group $\mathbb{Z}/8\mathbb{Z}$ to $v_3 = \frac{1+3w^2}{3+w^2}$ and to $v_{10} = \frac{-2w}{1-w+w^2}$ we get two families having rank at least 1. When we use in the first the values $w_1 = \frac{11-u^2}{10u}$ and $w_2 = \frac{29-12u+u^2}{-29+u^2}$ we get two families of rank at least 2 that are a reparametrization of the rank 2 families that we get by using v_{10} followed by $w_3 = \frac{(-3+u)(3+u)}{7-6u}$ and $w_4 = \frac{(-3+u)(3+u)}{11-6u}$.

So at the end with the changes v_3 followed by w_1 and w_2 and v_{10} followed by w_3 and w_4 we reach the same families of rank at least 2.

5.4. Rank 3 for the torsion group $\mathbb{Z}/8\mathbb{Z}$. It can be proved that there exist infinitely many elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ and rank at least 3 parametrized by the points of a positive rank elliptic curve. In fact it is enough to see that the equation $w_1(r) = w_2(s)$, i.e.:

$$\frac{11-r^2}{10r} = \frac{29-12s+s^2}{-29+s^2}$$

has infinitely many solutions. This is the same as to solve

$$319 + 290r - 29r^2 - 120rs - 11s^2 + 10rs^2 + r^2s^2 = 0$$

in rational terms, so the discriminant $\Delta = 3509 + 62r^2 + 29r^4$ has to be a square. But $t^2 = 3509 + 62r^2 + 29r^4$ has a rational solution, $(r,t) = (1,60)$ for example, hence it is equivalent to the cubic $y^2 = x^3 - 463x^2 + 45936x$ whose rank is 2, as proved with `mwrank` [**Cr**], with generators $(116, -812)$ and $(1764, 64260)$. This, jointly with the independence of the corresponding points, implies the existence of infinitely many solutions parametrized by the points of the elliptic curve, see [**Le1**] or [**Ra**] for this kind or argument. We can give more direct proof of this statement by using the Silverman specialization theorem. It suffices to find a specialization of

$$y^2 = x^3 + AA_8(w)x^2 + BB_8(w)x$$

for which three points with x-coordinates $1024w^2(1+3w^2)^4(-1+w)^2(w+1)^2/(-1-22w^2+7w^4)^2)$, $(-1+w)^2(1+w)^2(5+7w^2)^2(11+25w^2)/16$ and $(-1+w)^2(1+w)^2(1+11w^2)^2(7+29w^2)/(16w^2)$ are independent. The generator $(1764, 64260)$ induces the parameters $r = 13/5$, $s = 21/2$ and $w = w_1(r) = w_2(s) = 53/325$. Thus, we get the curve

$$\begin{aligned} Y^2 \quad = \quad & X^3 - \frac{43299084010471507 71968}{124470630035400390625}X^2 + \\ & \frac{484054656642691258897127599126881821 6288256}{154929377414095178479328751564025878 90625}X, \end{aligned}$$

with three independent points with x-coordinates

$$2009762599042291154977913179314 5856/14305621723743455689172170410 15625,$$

$$97708512674480666388111 36/525888411899566650390625,$$

$$1010824660737616205201 8176/3496379997694396972 65625.$$

6. Rank 2 families for the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

6.1. A family with rank 1. We present here some details for the family of rank 1 in which we have found two subfamilies of generic rank at least 2. It corresponds to the eighth entry in the table of Section 4.2. We have found the possibility of converting $x_8 = (-5+3v)(3v-1)^2$ in the $x-$coordinate of a new point by considering the homogenous space $(U,V) = (3v-1,1)$ of the initial family

$$y^2 = x^3 + (37 - 84v + 102v^2 - 36v^3 - 3v^4)x^2 + (32(-1+v)^3(1+v)^3(-5+3v))x.$$

The condition that has to be fulfilled is that $v(-3+5v)$ converts into a square, hence we get $v_8 = \frac{3}{5-w^2}$. Once we insert v_8 in the preceding family and take off denominators we have the family $y^2 = x^3 + AA_{26}(w)x^2 + BB_{26}(w)x$ where

$$\begin{aligned} AA_{26}(w) &= 9472 - 7808w^2 + 2688w^4 - 488w^6 + 37w^8, \\ BB_{26}(w) &= 32(-8+w^2)^3(-5+w^2)(-2+w^2)^3(-16+5w^2). \end{aligned}$$

The point of infinite order is

$$\begin{aligned} P = \Big(& -(-5+w^2)(4+w^2)^2(-16+5w^2), \\ & 27(-2+w)^2 w(2+w)^2(-5+w^2)(4+w^2)(-16+5w^2)\Big) \end{aligned}$$

and the torsion point of order 6 is

$$\begin{aligned} T = \Big(& 8(-8+w^2)(-5+w^2)(-2+w^2)(-16+5w^2), \\ & 72(-2+w)^2(2+w)^2(-8+w^2)(-5+w^2)(-2+w^2)(-16+5w^2)\Big). \end{aligned}$$

By searching on homogeneous spaces corresponding to the pairs $(U,V) = (Mw^2+Nw+P, Qw^2+Rw+S)$ where M,N,P,Q,R,S are integers with absolute value less than 4, we have found the possibility of imposing two new conditions which lead to new points, hence, in case of independence, to a couple of rank 2 families. We have found such possibility with $(U,V) = (1,1)$ and $2(-8+w^2)^2(-2+w^2)^3$ and with $(U,V) = (w^2,1)$ and $(-8+w^2)(-5+w^2)(-16+5w^2)$. In the first case we get a new point with x-coordinate $2(-8+w^2)^2(-2+w^2)^3$ for $2w^2-7 =$ Square and in the second case the new point will have the x-coordinate $w^4(-8+w^2)(-5+w^2)(-16+5w^2)$ if $5w^2-4 =$ Square, so the values x_1 and x_2 jointly with the specialization of the parameter are

$$\begin{aligned} x_1 &= 2(-8+w^2)^2(-2+w^2)^3, & w_1 &= \frac{2(7+u^2)}{-7-2u+u^2}, \\ x_2 &= (-8+w^2)(-5+w^2)(-16+5w^2)w^4, & w_2 &= \frac{5-2u+u^2}{-5+u^2}. \end{aligned}$$

6.2. First family with rank 2. In order to force $2(-8+w^2)^2(-2+w^2)^3$ to be the x-coordinate of a new point it is enough to solve $2w^2-7 = M^2$. This is achieved with $w_1 = \frac{2(7+u^2)}{-7-2u+u^2}$, and the corresponding family is $y^2 = x^3 + AAA_{26}(u)x^2 +$

$BBB_{26}(u)x$ where

$$\begin{aligned}AAA_{26}(u) =& -2(5764801 + 6588344u - 21647416u^2 + 29445864u^3 - 9604u^4+\\ &27969592u^5 - 44631944u^6 + 9779112u^7 + 5909830u^8 - 1397016u^9\\ &- 910856u^{10} - 81544u^{11} - 4u^{12} - 1752u^{13} - 184u^{14} - 8u^{15} + u^{16}),\\ BBB_{26}(u) =&(-7 - 10u + u^2)^3(-7 + 2u + u^2)^3(49 + 140u - 106u^2 - 20u^3 + u^4)\\ &(49 - 28u + 38u^2 + 4u^3 + u^4)^3(49 - 112u + 110u^2 + 16u^3 + u^4).\end{aligned}$$

The x-coordinates of the two infinite order points are

$$\begin{aligned}X_1 =&(49 + 140u - 106u^2 - 20u^3 + u^4)(49 + 14u + 2u^2 - 2u^3 + u^4)^2\times\\ &(49 - 112u + 110u^2 + 16u^3 + u^4),\\ X_2 =&\frac{(-7 - 10u + u^2)^2(-7 + 2u + u^2)^2(49 - 28u + 38u^2 + 4u^3 + u^4)^3}{(-7 - 2u + u^2)^2},\end{aligned}$$

and the x-coordinate of the torsion point of order 6 is

$$\begin{aligned}T =&(-7 - 10u + u^2)(-7 + 2u + u^2)(49 + 140u - 106u^2 - 20u^3 + u^4)\times\\ &(49 - 28u + 38u^2 + 4u^3 + u^4)(49 - 112u + 110u^2 + 16u^3 + u^4).\end{aligned}$$

The specialization for $u = 2$ gives the elliptic curve

$$y^2 = x^3 + (1723160926)x^2 + (8550207293988769)x$$

whose rank is 2. The specialized points are

$$(-706250975, 22387192082640)$$

and

$$\left(\frac{3803011153}{49}, \frac{-1163721412818000}{343}\right).$$

Since they are independent, the fact that specialization is a homomorphism implies that the rank of the curve $y^2 = x^3 + AAA_{26}(u)x^2 + BBB_{26}(u)x$ is at least 2 over $\mathbb{Q}(u)$.

6.3. Second family with rank 2. Imposing $(-8 + w^2)(-5 + w^2)(-16 + 5w^2)w^4$ as the x-coordinate of a new point is equivalent to solve $5w^2 - 4 = M^2$. This is achieved with $w_2 = \frac{5-2u+u^2}{-5+u^2}$.

The corresponding family is $y^2 = x^3 + aaa_{26}(u)x^2 + bbb_{26}(u)x$ where

$$\begin{aligned}aaa_{26}(u) =&1523828125 + 1171250000u - 3482125000u^2 - 1970850000u^3+\\ &3530367500u^4 + 1221154000u^5 - 2018502200u^6 - 238418640u^7+\\ &632792782u^8 - 47683728u^9 - 80740088u^{10} + 9769232u^{11}+\\ &5648588u^{12} - 630672u^{13} - 222856u^{14} + 14992u^{15} + 3901u^{16},\\ bbb_{26}(u) =&128(-7 + 2u + u^2)^3(-25 - 10u + 7u^2)^3(25 + 5u - 16u^2 + u^3 + u^4)\times\\ &(25 + 20u - 34u^2 + 4u^3 + u^4)^3(275 + 100u - 230u^2 + 20u^3 + 11u^4).\end{aligned}$$

The x-coordinates of the two infinite order points are

$$\begin{aligned}X_1 =& -4(25+5u-16u^2+u^3+u^4)(125-20u-26u^2-4u^3+5u^4)^2\times\\&(275+100u-230u^2+20u^3+11u^4),\\X_2 =&\frac{-4(5-2u+u^2)^4(-7+2u+u^2)(-25-10u+7u^2)}{(-5+u^2)^2}\times\\&(25+5u-16u^2+u^3+u^4)(275+100u-230u^2+20u^3+11u^4),\end{aligned}$$

and the x-coordinate of the torsion point of order 6 is

$$\begin{aligned}T =&32(-7+2u+u^2)(-25-10u+7u^2)(25+5u-16u^2+u^3+u^4)\times\\&(25+20u-34u^2+4u^3+u^4)(275+100u-230u^2+20u^3+11u^4).\end{aligned}$$

For $u=4$ the specialized curve

$$y^2 = x^3 + (561927462493)x^2 + (302043946753390368985 6)x$$

has rank 2. The specialized points for $u=4$ are

$$(-202832527484, 118999553078706300)$$

and

$$\left(\frac{-10855040006564}{121}, \frac{790738006691647287 00}{1331}\right)$$

They are independent, so the family $y^2 = x^3 + aaa_{26}(u)x^2 + bbb_{26}(u)x$ has rank at least 2 over $\mathbb{Q}(u)$.

6.4. Third family with rank 2. A variant of the model for torsion group $\mathbb{Z}/6\mathbb{Z}$ described by Hadano in [**H**] will be used here for the construction of another family of curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and rank at least 2. The curves with torsion group $\mathbb{Z}/6\mathbb{Z}$ in [**H**] have the equation

$$Y^2 = X^3 + X^2(a^2+2ab-2b^2) - X(2a-b)b^3.$$

For this model we first force the existence of a new point in order to have a family with this torsion and rank at least 1, then we choose the parameters that give complete factorization of the above cubic polynomial in X, and so the torsion subgroup is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Finally, in the resulting family for this torsion and rank 1, we impose a second independent point with a quadratic section.

Observe that by choosing $b = -\frac{(-1+a^2-v)(-1+a^2+v)}{4(-a+a^3-v)}$ we have a new point in the curve with X coordinate given by

$$X = -\frac{(1-4a+3a^2-v)(-1+a^2+v)^3}{16(-a+a^3-v)^2}.$$

Once we clear denominators, this family can be written as $Y^2 = X^3 + A_{61}(a,v)X^2 + B_{61}(a,v)X$ where

$$\begin{aligned}A_{61} &= 2(-1+8a^2-10a^4+3a^8+4av+8a^3v-12a^5v+2v^2+6a^4v^2-4av^3-v^4),\\B_{61} &= (-1+a^2-v)^3(1-4a+3a^2-v)(-1+a^2+v)^3(1+4a+3a^2+v).\end{aligned}$$

The new point becomes

$$P = (-(1-4a+3a^2-v)(-1+a^2+v)^3, 4(1-4a+3a^2-v)(-a+a^3-v)(-1+a^2+v)^3).$$

For fixed $a \neq 1$, then for all but finitely many values of v, P is of infinite order as a consequence of the Silverman specialization theorem, so the curve has rank at least 1 over $\mathbb{Q}(a, v)$. Now we observe that the complete factorization of the cubic is equivalent to forcing the discriminant of a second degree polynomial to be a square.

The condition is $a(-a + a^3 - v)(-1 + a^2 - av + v^2) =$ square. This can be achieved with $a = v + 1$ followed by $v = \frac{1-w^2}{-3+2w}$. Once we perform these changes we get $Y^2 = X^3 + a_{26}(w)X^2 + b_{26}(w)X$ where

$$a_{26} = 2(-24 - 216w + 1008w^2 - 1596w^3 + 1319w^4 - 648w^5 + 198w^6 - 36w^7 + 3w^8),$$
$$b_{26} = (-4 + w)^3(-3 + w)(-2 + w)^3(-1 + w)^3 w(1 + w)^3(-7 + 3w)(-2 + 3w).$$

With these changes the x-coordinate of the infinite order point is

$$X = -\frac{(-4 + w)^3(-2 + w)^3(-1 + w)^2 w(1 + w)^2(-2 + 3w)}{(2 - 2w + w^2)^2}.$$

So we have a curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank at least 1 over $\mathbb{Q}(w)$.

Now we see that $(-4 + w)(-3 + w)(-1 + w)^3(1 + w)^2(-7 + 3w)$ will be a new point on the curve if we force $4 - 9w + 3w^2$ to be a square. This is the same as choosing $w = -\frac{9+4u}{-3+u^2}$. Once we perform this change and clear denominators we get the following coefficients for the new family

$$\begin{aligned}
A_{263} =& -2(157464 - 1889568u - 13594392u^2 - 38047968u^3 - \\
& 62500248u^4 - 69622416u^5 - 57719412u^6 - 38941344u^7 - \\
& 23353995u^8 - 12980448u^9 - 6413268u^{10} - 2578608u^{11} - \\
& 771608u^{12} - 156576u^{13} - 18648u^{14} - 864u^{15} + 24u^{16}), \\
B_{263} =& -(-6 + u)^3 u(2 + u)^3(-1 + 2u)^3(3 + 2u)^3(4 + 3u)(9 + 4u) \\
& (6 + 4u + u^2)^3(3 + 4u + 2u^2)^3(21 + 12u + 2u^2)(6 + 12u + 7u^2).
\end{aligned}$$

The x-coordinates of the non-torsion points are

$$\begin{aligned}
X_1 =& (-6 + u)^2 u(2 + u)^2(-1 + 2u)(3 + 2u)(4 + 3u) \times \\
& (6 + 4u + u^2)^3(6 + 12u + 7u^2), \\
X_2 =& -\frac{(-6 + u)^2(2 + u)^2(-1 + 2u)^3(3 + 2u)^3(9 + 4u)}{(45 + 48u + 22u^2 + 8u^3 + 2u^4)^2} \times \\
& (6 + 4u + u^2)^2(3 + 4u + 2u^2)^3(21 + 12u + 2u^2).
\end{aligned}$$

A specialization argument, as in Section 6.2 and Section 6.3, shows that these two points are independent so this curve has rank at least 2 over $\mathbb{Q}(u)$ and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. For $u = 2$ the specialized curve given by

$$y^2 = x^3 + (83034141712)x^2 + (1585911434996821524480)x$$

has rank 2. The specialized points for $u = 2$ are

$$(36369285120, 14683880651489280)$$

and

$$\left(\frac{-4747100799200256}{105625}, \frac{8169564894870713525452 8}{34328125}\right).$$

They are independent, so the family $y^2 = x^3 + A_{263}x^2 + B_{263}x$ has rank at least 2.

6.5. Digression. The condition for complete factorization in the construction of the third family above was:

$$a(-a+a^3-v)(-1+a^2-av+v^2) = \text{square}.$$

We used $a = v+1$ followed by $v = \frac{1-w^2}{-3+2w}$ as a solution, but there are many others, for example $v = 2a+2$ followed by $a = \frac{2}{1-3w^2}$ or $v = 2a(a-1)$ followed by $a = -\frac{1+w^2}{2(1+2w)}$. In a more systematic way with $v = -\frac{a^2-a^4+X}{a}$ the condition becomes

$$Y^2 = X^3 - a^2(-3+2a^2)X^2 + (-1+a)^3a^2(1+a)^3X. \tag{6.1}$$

But (6.1) is an elliptic curve curve with rank at least 1 over $\mathbb{Q}(a)$. In fact the point

$$\left(\frac{(1+3a^2)^2}{9}, \frac{(1+3a^2)(-1+21a^2)}{27}\right)$$

is a point of infinite order in the curve.

Then for almost all a we have infinitely many solutions of the initial condition and eventually infinitely many families with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and rank at least 1.

Examples of substitutions leading to torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and rank at least 1 are the following:

$$\begin{aligned} v =& -\frac{1+15a^2}{9a} \\ v =& -3(a-1)a(a+1) \\ v =& \frac{3(-1+a)a(1+a)(-1+3a)(1+3a)(5+3a^2)}{(1+15a^2)^2} \end{aligned}$$

6.6. Rank 3 for the torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Now we prove the existence of infinitely many elliptic curves with rank at least 3 and torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ parametrized by the points of a positive rank elliptic curve. In fact it is enough to see that the equation $w_1(r) = w_2(s)$, i.e.:

$$\frac{2(7+r^2)}{-7-2r+r^2} = \frac{5-2s+s^2}{-5+s^2}$$

has infinitely many solutions. This is the same as solving

$$-35+10r-15r^2-14s-4rs+2r^2s+21s^2+2rs^2+r^2s^2 = 0$$

in rational terms, so the discriminant $\Delta = 49-7r+20r^2+r^3+r^4$ has to be a rational square. But $t^2 = 49-7r+20r^2+r^3+r^4$ has a rational solution, $(r,t) = (1,8)$ for example, hence it is birationally equivalent to the cubic $y^2 = x^3-43x^2+280x$ whose rank is 1, as proved with `mwrank` [**Cr**], with a generator of Mordell-Weil group $(7,14)$. This and the independence of the corresponding points, implies the existence of infinitely many solutions parametrized by the points of the elliptic curve. Indeed, by the Silverman specialization theorem, it suffices to find a specialization of

$$y^2 = x^3 + AA_{26}(w)x^2 + BB_{26}(w)x$$

for which the three points with x-coordinates $-(-5+w^2)(4+w^2)^2(-16+5w^2)$, $2(-8+w^2)^2(-2+w^2)^3$ and $(-8+w^2)(-5+w^2)(-16+5w^2)w^4$ are independent. The generator $(7,14)$ induces the parameters $r = 217/33$, $s = 89/35$ and $w = w_1(r) = w_2(s) = 1954/449$. Thus, we get the curve

$$\begin{aligned} Y^2 \quad &= \quad X^3 + \frac{3751225473815816788782317056}{1651850457757840166401} X^2 + \\ &\quad \frac{6093398988276060562100593380074120656232097157460131 84}{27286099347947860999792175083246953692928 01} X, \end{aligned}$$

with three independent points with x-coordinates

$$-9534455364726581694113216 00/1651850457757840166401,$$

$$3873537944675284771901748455672 32/3330147041344383353866080 01,$$

$$1433276751300744738847166707777792/333014704134438335386608001.$$

7. Examples of curves with high rank

7.1. The case of torsion group $\mathbb{Z}/8\mathbb{Z}$. The highest known rank of an elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/8\mathbb{Z}$ is rank 6 curve found by Elkies in 2006. See [**Du2**] for the details of this curve.

The following list includes examples of rank 5 curves found in the rank 1 families of subsection 4.1. The first column indicates the number of the family and the second the value(s) of the parameter producing a rank 5 curve. The indication (L) means that this curve has been previously found by Lecacheux.

Family number	w values
2	$\frac{287}{109}$,
3	$\frac{73}{83}$, $\frac{37}{157}$,
4	$-\frac{87}{28}$, $\frac{245}{12}$,
5	$\frac{317}{10}$,
6	$-\frac{28}{79}$, $\frac{100}{29}$ (L), $\frac{304}{55}$.

7.2. The case of torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The highest known rank of an elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ was found by Elkies in 2006. See [**Du2**] for the details of this curve. It has rank 6 and it can be seen to correspond to the value $u = -\frac{16}{3}$ in the family with rank 2 included in subsection 6.2. For $u = \frac{5}{13}$ we get a curve with rank 5.

The following list includes examples of rank 5 curves found in the rank 1 families of subsection 4.2. The first column indicates the number of the family and the second the value(s) of the parameter producing a rank 5 curve. The indication (L) and (D) means that in these cases the curves were found previously by Lecacheux and Dujella respectively.

Family number	w values
1	$\frac{306}{11}$
3	$\frac{53}{90}$ (D), $-\frac{127}{74}$ (L)
5	$\frac{31}{42}$
6	$\frac{13}{43}$, $-\frac{431}{33}$
7	$\frac{115}{6}$, $-\frac{142}{33}$ (D), $-\frac{391}{387}$, $-\frac{1011}{551}$
8	$\frac{302}{161}$
9	$\frac{44}{61}$, $\frac{40}{57}$, $\frac{172}{191}$, $\frac{214}{163}$, $\frac{284}{197}$

Acknowledgement. The authors would like to thank the anonymous referee for careful reading and useful comments on the previous version of this paper.

References

[Be] A. Beauville, Les familles stables des courbes elliptiques sur P^1 admettent quatre fibres singulières, C.R. Acad. Sc. Paris. Serie I 294 (1982), 657-660.

[BL] M.J. Bertin, O. Lecacheux, Elliptic fibrations on the modular surface associated to $\Gamma_1(8)$, Arxiv: 1105.6312v1 (2011)

[Ca] G. Campbell, Finding elliptic curves defined over $\mathbb{Q}$ of high rank, African Americans in Mathematics (Piscataway, NJ, 1996) DIMACS Ser. Discrete Math. Theoret. Compt. Sci., vol 34, AMS, Providence, RI, 1997, p. 107-109.

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

[Du1] A. Dujella, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, Glas. Mat. Ser. III 42 (2007), 3–18.

[Du2] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/~duje/tors/tors.html`.

[DP] A. Dujella, J.C. Peral, High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples, preprint available on `http://web.math.hr/~duje/papers1.html`.

[El] N. Elkies, Three lectures on elliptic surfaces and curves of high rank, Arxiv: 0709.2908v1 (2007)

[H] T. Hadano, Elliptic curves with the torsion point, Nagoya Math. J., 66 (1977) 99-108.

[Kn] A. Knapp, Elliptic curves, Mathematical Notes, Princeton University Press, (1992)

[Ku] L. Kulesz, Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$, Acta Arith. 108 (2003), no. 4, 339-356.

[Le1] O. Lecacheux, Rang de courbes elliptiques dont le groupe de torsion est non trivial, Ann. Sci. Math. Quebec 28 (2004), no 1-2, 145-151.

[Le2] O. Lecacheux, Personal comunication.

[LY] R. Livné, N. Yui, The modularity of certain non-rigid Calabi-Yau threefolds, J. Math. Kyoto Univ. 45 (2005), no. 4, 645-665.

[Me] J.F. Mestre, Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(t)$, C.R. Acad. Sc. Paris. Serie I 313 (1991), 139-142.

[Ra] P. Rabarison, Construction of elliptic curves with high rank and large torsion group, (preprint) (2009)

[Sh] T. Shioda, An infinite family of elliptic curves over $\mathbb{Q}$ with large rank via Neron's method, Invent. Math. 106 (1991), 109-119.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address, A. Dujella: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain

E-mail address, J. C. Peral: juancarlos.peral@ehu.es