

# HIGH RANK ELLIPTIC CURVES WITH PRESCRIBED TORSION GROUP OVER QUADRATIC FIELDS

JULIÁN AGUIRRE, ANDREJ DUJELLA, MIRELA JUKIĆ BOKUN,  
AND JUAN CARLOS PERAL

ABSTRACT. There are 26 possibilities for the torsion group of elliptic curves defined over quadratic number fields. We present examples of high rank elliptic curves with given torsion group which give the current records for most of the torsion groups. In particular, we show that for each possible torsion group, except maybe for  $\mathbb{Z}/15\mathbb{Z}$ , there exist an elliptic curve over some quadratic field with this torsion group and with rank  $\geq 2$ .

## 1. INTRODUCTION

Let  $K = \mathbb{Q}(\sqrt{d})$ ,  $d \in \mathbb{Z}$ , be a quadratic number field and  $E$  an elliptic curve defined over  $K$ . Then the torsion subgroup for  $E$  is one of:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, \quad 1 \leq m \leq 18, m \neq 17, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \quad 1 \leq m \leq 6, \\ &\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 2, \quad \text{only possible for } \mathbb{Q}(\sqrt{-3}), \\ &\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \text{only possible for } \mathbb{Q}(\sqrt{-1}) \end{aligned}$$

(see [10] and [11]). In [17], Rabarison gave a parametrization of the curves having such torsion groups. His results together with recent results from [4] show that for each possible torsion group there exist an elliptic curve over some quadratic field with this torsion group and positive rank. In this paper, we present examples of elliptic curves having high rank and given torsion group over a quadratic field. For most of the torsion groups our results give the current records. In particular, our results show that for each possible torsion group, except maybe for  $\mathbb{Z}/15\mathbb{Z}$ , there exist an elliptic curve over some quadratic field with this torsion group and with rank  $\geq 2$ .

For elliptic curves over  $\mathbb{Q}$ , by Mazur's theorem there are 15 possible torsion groups. The current rank records and the data on corresponding curves can be found in the table [6] (for previous records see e.g. [12]). It is known since 2003 that for each of these 15 torsion groups there exist a curve over  $\mathbb{Q}$  with this torsion group and with rank  $\geq 3$ , and this is still the best known result of that type. Namely, despite big efforts in last 10 years, no elliptic curve over  $\mathbb{Q}$  with torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$  and rank  $\geq 4$  has been found so far.

## 2. CURRENT RECORDS

We summarize the current records, including our results, in Table 1. For each torsion group  $T$  from the above list, we define  $B(T)$  as the supremum of the ranks of elliptic curves defined over any quadratic field and having torsion group  $T$  (for the trivial torsion group we put  $T = 0$ ). The third column in Table 1 (l.b.) gives a

---

2010 *Mathematics Subject Classification.* 11G05, 14H52, 11R11.

A. D. was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821. J. C. P. was supported by the UPV/EHU grant EHU 10/05.

lower bound of  $B(T)$  for  $T$  given in the first column, while the second column gives the discriminant  $d$  of the corresponding quadratic number field  $K$ . Numbers 4.x in the reference column correspond to the subsections of Section 4 of the present paper, where the details of the corresponding curve appear. The marks \* in the table refer to the curves obtained by an application of Mestre's general construction which produces quadratic fields with huge discriminants. In the case of torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , the discriminant  $d_2$  is too large to fit in the table, but will be given in Subsection 4.12. Values in boldface in the third column are conditional, assuming the Parity Conjecture.

TABLE 1. Current records

$T$	$d$	l.b.	Reference
0	*	30	[6, 8, 13]
$\mathbb{Z}/2\mathbb{Z}$	-1	28	4.1
$\mathbb{Z}/3\mathbb{Z}$	*	15	[6, 13]
$\mathbb{Z}/4\mathbb{Z}$	-25689	15	4.2
$\mathbb{Z}/5\mathbb{Z}$	*	10	[6, 13]
$\mathbb{Z}/6\mathbb{Z}$	3521	11	4.3
$\mathbb{Z}/7\mathbb{Z}$	*	7	[6, 13]
$\mathbb{Z}/8\mathbb{Z}$	-227	9	4.4
$\mathbb{Z}/9\mathbb{Z}$	-155	6	4.5
$\mathbb{Z}/10\mathbb{Z}$	-2495	7	4.6
$\mathbb{Z}/11\mathbb{Z}$	-3239	2	4.7
$\mathbb{Z}/12\mathbb{Z}$	2014	7	4.8
$\mathbb{Z}/13\mathbb{Z}$	193	2	[17]
$\mathbb{Z}/14\mathbb{Z}$	265	2	4.9, [17]
$\mathbb{Z}/15\mathbb{Z}$	-7	1	4.10, [4]
$\mathbb{Z}/16\mathbb{Z}$	1785	2	4.11
$\mathbb{Z}/18\mathbb{Z}$	26521	2	[4]
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$d_2$	19 <b>20</b>	4.12
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	-83201	13	4.13
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	624341	10	4.14
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	31230597	8	4.15
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	1065333545	4 <b>5</b>	4.16, [4]
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	2947271015	4	[4]
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	-3	7	[9]
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	-3	6	[9]
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	-1	7	[7]

### 3. METHODS OF SEARCH

In the case of the 15 possible torsion groups of elliptic curves over  $\mathbb{Q}$  (by Mazur's theorem), we consider curves with rational coefficients, and in order to determine their rank over a quadratic field  $\mathbb{Q}(\sqrt{d})$  we use the formula ([2], see also [20] or [21, Exercise 10.16])

$$(1) \quad \text{rank}(E(\mathbb{Q}(\sqrt{d}))) = \text{rank}(E(\mathbb{Q})) + \text{rank}(E^{(d)}(\mathbb{Q})),$$

where  $E^{(d)}$  denotes the  $d$ -quadratic twist of  $E$ . One way to get high rank curves over quadratic fields with one of these 15 torsion groups is to start with one of the record curves with this torsion over  $\mathbb{Q}$  (these curves are collected in the tables [6]), then search for a twist of this curve with high rank, and finally use (1). However, the record curves usually have very large coefficients, which makes it hard to compute the rank of its twist. Thus sometimes it is more profitable to start with curves

of rank slightly smaller than the corresponding record (many such curves are also available in [6]), and then use the full power of standard sieving methods for finding high rank curves in parametric families of elliptic curves. These methods include computations of Mestre-Nagao sums (they are indicators of good candidates of high rank, see e.g. [15]) and the Selmer rank (it gives an upper bound for the rank which is sometimes sharp). In some cases the root number is used either for reaching conditional results through the Parity Conjecture or as an additional sieving parameter. We implemented these sieving procedures in `Pari` [16]. For computing the rank we used Cremona's program `mwrnk` [5].

For the curves with record rank over  $\mathbb{Q}$ , we were usually able to compute the rank of the twists only up to  $d < 10^4$  or  $d < 10^5$ , so that gave the limitation for our search. On the other hand, for starting curves with small coefficients, we could search for high-rank twists up to  $d < 10^8$ . In order to make this search practical, we have chosen strong conditions for the Mestre-Nagao sum. As an illustration, we can mention the 31230597-twist of rank 5 in the case of torsion group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$  (for details see Subsection 4.15). Here the search procedure took around 10 days of CPU time on an Intel Xeon E5430.

We should mention a general result due to Mestre [13] (see also [22]) who proved that for any elliptic curve  $E$  over  $\mathbb{Q}$  there exist infinitely many quadratic twists with rank  $\geq 2$ . For some torsion groups of odd order (trivial,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$ ,  $\mathbb{Z}/7\mathbb{Z}$ ) the largest known ranks were obtained by applying Mestre's result [13] to the record curves over  $\mathbb{Q}$ . Thus we will not give further details for these cases. We mention also results announced by Mestre [14] and proved by Rubin and Silverberg [18, 19] that if the torsion group of  $E$  is  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ , resp.  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ , then there exist infinitely many quadratic twists of  $E$  with rank  $\geq 3$ , resp.  $\geq 4$ . However, our results for these two cases improve those obtained by direct application of results from [18, 19] to the record curves over  $\mathbb{Q}$ .

For the torsion groups of the form  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ , we may take the record curve with torsion  $\mathbb{Z}/2m\mathbb{Z}$  over  $\mathbb{Q}$ , and then determine the quadratic field over which this curve contains torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ .

Formula (1) can be also used for curves over a quadratic field, even if its torsion group is not one of the 15 which are possible for curves over  $\mathbb{Q}$ , when they admit a model with rational coefficients. Indeed, this was applied in [7, 9] for torsion groups  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  and  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ . For the remaining torsion groups, we use the parametrizations given in [17], and try to compute the rank (or at least to get some information on it) for curves corresponding to small parameters by using procedures available in `Magma` ([3]).

Let us mention that for torsion groups  $\mathbb{Z}/13\mathbb{Z}$  and  $\mathbb{Z}/18\mathbb{Z}$ , the current records with rank 2 might be very hard to improve, since it was recently proved in [4] that all such curves over quadratic fields have even rank.

#### 4. EXAMPLES

**4.1. Torsion  $\mathbb{Z}/2\mathbb{Z}$ .**  $B(\mathbb{Z}/2\mathbb{Z}) \geq 28$ . For this torsion group the highest rank known over  $\mathbb{Q}$  is an example of a curve with rank 19 found by Elkies (see [6]). For our purpose, it is more interesting to use an example due to Watkins (see [1, 6]), who found a curve with rank 14 and  $j$ -invariant 1728, namely

$$y^2 = x^3 - 402599774387690701016910427272483x.$$

It is isomorphic to its  $(-1)$ -twist. Hence, the rank of the  $(-1)$ -twist of this elliptic curve is also 14, and now it follows from (1) that this curve has rank 28 over  $\mathbb{Q}(\sqrt{-1})$ .

**4.2. Torsion  $\mathbb{Z}/4\mathbb{Z}$ .**  $B(\mathbb{Z}/4\mathbb{Z}) \geq 15$ . The curve with the highest known rank over  $\mathbb{Q}$  having this torsion group is an example with rank 12 found by Elkies in 2006 (see [6]). Since its coefficients are very large, we have considered also curves with rank 9, 10 and 11 from [6]. In that way, we found several curves with rank 14 over certain quadratic fields, and one example with rank 15. This example was found starting with the rank 9 curve:

$$y^2 = x^3 - x^2 - 63101137631999143241257265x \\ + 191341468112384598938400129107933347137$$

found by Eroshkin in 2008. Its twist by  $d = -25689$  has rank 6, so an application of (1) gives that  $B(\mathbb{Z}/4\mathbb{Z}) \geq 15$ .

**4.3. Torsion  $\mathbb{Z}/6\mathbb{Z}$ .**  $B(\mathbb{Z}/6\mathbb{Z}) \geq 11$ . In this case the highest known rank over  $\mathbb{Q}$  known for this torsion group is 8 (Dujella, Eroshkin, Elkies (2008), see [6]). We got the best result starting with a rank 7 curve, found by Dujella in 2001, which is given by

$$y^2 + xy = x^3 - x^2 - 45123702275641081919424x + 936989213947498862436000.$$

Its 3521-twist has rank at least 4 so the result follows again by (1).

**4.4. Torsion  $\mathbb{Z}/8\mathbb{Z}$ .**  $B(\mathbb{Z}/8\mathbb{Z}) \geq 9$ . For this torsion group the curve with highest known rank was found by Elkies in 2006 (see [6]) and has rank 6. For our search we use the curve with rank 5, found by Dujella & Lecacheux in 2002, which is given by

$$y^2 = x^3 + x^2 - 11849634571550798667743047864720x \\ + 15613761915399875450490670165233536220551598068.$$

Since its twist by  $d = -227$  has rank 4, the result follows.

**4.5. Torsion  $\mathbb{Z}/9\mathbb{Z}$ .**  $B(\mathbb{Z}/9\mathbb{Z}) \geq 6$ . Fisher found in 2009 a curve with torsion  $\mathbb{Z}/9\mathbb{Z}$  and rank 4 over  $\mathbb{Q}$  (see [6]). By applying the general result by Mestre, we get a curve of rank 6 over a quadratic field. However, this field has a huge discriminant, and an example of rank 6 with much smaller discriminant can be obtained starting with the elliptic curve

$$y^2 + xy + y = x^3 - x^2 - 41368267697099x + 102411668493915101147,$$

of rank 3 over  $\mathbb{Q}$  (Dujella 2001), and noting that its twist by  $d = -155$  also has rank 3 over  $\mathbb{Q}$ . Thus it has rank 6 over  $\mathbb{Q}(\sqrt{-155})$  by (1).

**4.6. Torsion  $\mathbb{Z}/10\mathbb{Z}$ .**  $B(\mathbb{Z}/10\mathbb{Z}) \geq 7$ . We use the curve with rank 4 and torsion  $\mathbb{Z}/10\mathbb{Z}$  which is the rank record for this torsion group (Dujella 2004, see [6]). The curve is

$$y^2 + xy = x^3 - 127381738643041574974581021420318985x \\ + 17495594046612039766866496413577998621609407092547225.$$

Its twist by  $d = -2495$  has rank equal to 3, so the result follows from (1).

Another examples with rank 7 and torsion  $\mathbb{Z}/10\mathbb{Z}$  over a quadratic field can be obtained by starting with curves with smaller rank. E.g. the curve

$$y^2 + xy = x^3 - 5313234280x + 149068288642400$$

(Womack 2000, see [23]) has torsion  $\mathbb{Z}/10\mathbb{Z}$ , rank 2 over  $\mathbb{Q}$  and its 318855485-twist has rank 5, while the curve

$$y^2 + xy = x^3 - 4281263352573652971565x + 107821663654697042219512111579217$$

(Dujella 2001, see [6]) has torsion  $\mathbb{Z}/10\mathbb{Z}$ , rank 3 over  $\mathbb{Q}$  and its 3007-twist has rank 4.

**4.7. Torsion  $\mathbb{Z}/11\mathbb{Z}$ .**  $B(\mathbb{Z}/11\mathbb{Z}) \geq 2$ . This torsion cannot appear over  $\mathbb{Q}$ . Rabarison [17] showed the existence of curves with torsion group  $\mathbb{Z}/11\mathbb{Z}$  and rank at least 1 over  $\mathbb{Q}(\sqrt{d})$  for  $d = -3239, -599, -47, 6, 7, 22, 73$  and 193. The curve over  $\mathbb{Q}(\sqrt{-3239})$  is

$$y^2 + \frac{5\sqrt{-3239} - 796}{9}xy + (45\sqrt{-3239} + 855)y = x^3 + (45\sqrt{-3239} + 855)x^2.$$

Rabarison stated that its rank over  $\mathbb{Q}(\sqrt{-3239})$  is 1. Since it has a point of infinite order  $([1 - \sqrt{-3239}, 2\sqrt{-3239} - 1082])$  and root number equal to 1, the Parity Conjecture implies that its rank should be at least 2. Unfortunately, we were not able to find the second independent point. We have also an example over  $\mathbb{Q}(\sqrt{1129})$  with conditional rank  $\geq 2$ . However, we were able to find one example with torsion  $\mathbb{Z}/11\mathbb{Z}$  and rank  $\geq 2$  over  $\mathbb{Q}(\sqrt{561})$ , unconditionally. Namely, the curve

$$y^2 + \frac{-10\sqrt{561} + 893}{1008}xy + \frac{-35\sqrt{561} + 210}{10368}y = x^3 + \frac{-35\sqrt{561} + 210}{10368}x^2$$

has the torsion group  $\mathbb{Z}/11\mathbb{Z}$  over  $\mathbb{Q}(\sqrt{561})$  and the following two independent points of infinite order:  $\left[ \frac{-\sqrt{561} - 869}{6912}, \frac{1709\sqrt{561} + 147421}{6967296} \right]$  and  $\left[ \frac{5\sqrt{561} - 65}{1344}, \frac{-1285\sqrt{561} + 32385}{2032128} \right]$ .

**4.8. Torsion  $\mathbb{Z}/12\mathbb{Z}$ .**  $B(\mathbb{Z}/12\mathbb{Z}) \geq 7$ . Although the highest known rank for this torsion is 4 (Fisher 2008, see [6]), we apply our procedure to several curves with rank 2 and 3. For the curve with rank 3 and torsion  $\mathbb{Z}/12\mathbb{Z}$  found by Rathbun in 2003 (see [6]) given by

$$y^2 + xy + y = x^3 - x^2 - 42403753582533569425032932x + 106274144228004532427905140464314177031,$$

we find that its twist by  $d = -106071$  has rank 4. Another curve with rank 3 and torsion  $\mathbb{Z}/12\mathbb{Z}$  is

$$y^2 + xy = x^3 - 544753256053055692212823356675x + 154756127532691562955214620687209364995464257,$$

found by Dujella in 2005. We find that its 2905-twist has rank 4. Finally, we consider a curve with rank 2:

$$y^2 + xy = x^3 - x^2 - 136659485377389900024x + 612767297917647098548240331268,$$

which has 2014-twist with rank 5. Again, an application of (1) gives the announced result.

**4.9. Torsion  $\mathbb{Z}/14\mathbb{Z}$ .**  $B(\mathbb{Z}/14\mathbb{Z}) \geq 2$ . In [17], Rabarison gave examples of elliptic curves with torsion group  $\mathbb{Z}/14\mathbb{Z}$  and rank  $\geq 1$  over the quadratic fields  $\mathbb{Q}(\sqrt{-23})$  and  $\mathbb{Q}(\sqrt{265})$ . The curve over  $\mathbb{Q}(\sqrt{265})$  is

$$y^2 + \frac{-18\sqrt{265} + 283}{145}xy + \frac{726\sqrt{265} - 12990}{21025}y = x^3 + \frac{726\sqrt{265} - 12990}{21025}x^2.$$

Using Magma [3], we find that this curve has rank equal to 2, with independent points with  $x$ -coordinates

$$\frac{-133118\sqrt{265} + 4584710}{36395145} \quad \text{and} \quad \frac{-246\sqrt{265} + 4902}{4205}.$$

**4.10. Torsion  $\mathbb{Z}/15\mathbb{Z}$ .**  $B(\mathbb{Z}/15\mathbb{Z}) \geq 1$ . In [4], an example with torsion group  $\mathbb{Z}/15\mathbb{Z}$  and positive rank is given over  $\mathbb{Q}(\sqrt{345})$ . Here we give such an example over  $\mathbb{Q}(\sqrt{-7})$ . This is the curve

$$y^2 + (-2\sqrt{-7} + 15)xy + (26\sqrt{-7} - 14)y = x^3 + (26\sqrt{-7} - 14)x^2,$$

obtained by inserting

$$t = (-\sqrt{-7} - 5)/8, \quad s = (\sqrt{-7} - 11)/16$$

in the general parametrization of curves with torsion  $\mathbb{Z}/15\mathbb{Z}$  given in [17]. This curve has a point of infinite order  $[6\sqrt{-7} - 98, 136\sqrt{-7} + 1064]$  over  $\mathbb{Q}(\sqrt{-7})$ .

**4.11. Torsion  $\mathbb{Z}/16\mathbb{Z}$ .**  $B(\mathbb{Z}/16\mathbb{Z}) \geq 2$ . In [17], Rabarison gave an example of elliptic curve with torsion  $\mathbb{Z}/16\mathbb{Z}$  and rank  $\geq 1$  over  $\mathbb{Q}(\sqrt{10})$ . We improve this result by finding an example with torsion  $\mathbb{Z}/16\mathbb{Z}$  and rank equal to 2 over  $\mathbb{Q}(\sqrt{1785})$ . The curve is

$$y^2 + \frac{-247\sqrt{1785} + 80605}{71680}xy + \frac{-203\sqrt{1785} - 11271}{917504}y = x^3 + \frac{-203\sqrt{1785} - 11271}{917504}x^2.$$

Using Magma [3], we find that this curve has rank 2 over  $\mathbb{Q}(\sqrt{1785})$ , with independent points with  $x$ -coordinates

$$\frac{10763581607\sqrt{1785} + 456934229139}{894936283136} \quad \text{and} \quad \frac{11\sqrt{1785} + 663}{50540}.$$

**4.12. Torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .**  $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 19$ . In this case the argument is different: we start with a curve having torsion  $\mathbb{Z}/2\mathbb{Z}$  over  $\mathbb{Q}$  and rank 19. This curve has the record rank for this torsion group and was found by Elkies in 2009 (see [6]). We write it in the form

$$y^2 = (x + 655364911965298267755181)g(x),$$

where  $g$  is a monic polynomial of degree 2 with integer coefficients whose discriminant is

$$d_2 = -3901785498412536920668361993073821511.$$

The curve has two additional 2-torsion points over  $\mathbb{Q}(\sqrt{d_2})$  and its torsion group over this field is  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . The rank is at least 19 over  $\mathbb{Q}(\sqrt{d_2})$ . Since the root number for the  $d_2$ -twist of the curve is  $-1$ , assuming the Parity Conjecture, we have that the rank should be at least 20.

4.13. **Torsion**  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ .  $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \geq 13$ . The record rank over  $\mathbb{Q}$  for this torsion is 8, due to Elkies (2005), Eroshkin (2008), Dujella & Eroshkin (2008) (see [6]). One of the known rank-record curves, found by Eroshkin, is given by

$$y^2 = x^3 + x^2 - 23686061832482481624168232900x + 1401294826072670363740983663536729053022048.$$

Its twists by  $d = -83201$  and  $d = 109499$  both have rank 5, so the result follows.

Another example is given by the curve

$$y^2 = x^3 - x^2 - 866893152450363503763740085700x + 61220734062068506723288644020689511073795652,$$

found by Dujella & Eroshkin. It has rank 8, while its 117589-twist has rank 5.

4.14. **Torsion**  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ .  $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}) \geq 10$ . Although the record rank over  $\mathbb{Q}$  for this torsion is 6 (Elkies, 2006), we use a curve having this torsion group and rank 5, found by Dujella & Lecacheux in 2002 (see [6]). The curve is given by

$$y^2 + xy = x^3 - 2353799432200918732090882185x + 39989567111692230080439457690563434811225.$$

The result follows from the fact that its 624341-twist has rank 5 over  $\mathbb{Q}$ .

4.15. **Torsion**  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ .  $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}) \geq 8$ . The highest known rank over  $\mathbb{Q}$  for curves with this torsion is 3. In total, there are 27 such curves known, found by many authors (see [6]). We use the curve with rank 3, found independently by Connell and Dujella in 2000:

$$y^2 + xy = x^3 - 15745932530829089880x + 24028219957095969426339278400.$$

The result is a consequence of the fact that its twist by  $d = 31230597$  has rank 5.

4.16. **Torsion**  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ .  $B(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}) \geq 4$ . This torsion group does not appear over  $\mathbb{Q}$ , so we apply an argument similar to the one used in Subsection 4.12. We start from a curve with rank 4 over  $\mathbb{Q}$  and torsion  $\mathbb{Z}/10\mathbb{Z}$  and we look for twists with additional torsion points. The starting curve is

$$y^2 + xy = x^3 - 186734461375182851611482374885236743900x + 979124235576847382684597033191041431087287234552438410000,$$

found by Dujella in 2008 (see [6]). We find that it has torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$  over the quadratic field  $\mathbb{Q}(\sqrt{1065333545})$ , so the result follows. Let us mention that a curve of rank  $\geq 4$  and torsion  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$  over  $\mathbb{Q}(\sqrt{55325286553})$  was found in [4] by the same method. However, here the corresponding twist has the root number  $-1$ , so assuming the Parity Conjecture, this curve has rank  $\geq 5$ .

**Acknowledgement.** The authors would like to thank Filip Najman and the referee for very useful comments on the previous version of this paper.

## REFERENCES

- [1] J. Aguirre, F. Castañeda, J.C. Peral, *High rank elliptic curves with torsion group  $\mathbb{Z}/2\mathbb{Z}$* , Math. Comp. **73** (2004), 323–331.
- [2] B. J. Birch, *Elliptic curves and modular functions*, in Symposia Mathematica, Vol. IV, Academic Press, London, 1970, pp. 27–32.
- [3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265.
- [4] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, preprint.
- [5] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.
- [6] A. Dujella, *High rank elliptic curves with prescribed torsion*, <http://web.math.hr/~duje/tors/tors.html>
- [7] A. Dujella, M. Jukić Bokun, *On the rank of elliptic curves over  $\mathbb{Q}(i)$  with torsion group  $\mathbb{Z}_4 \times \mathbb{Z}_4$* , Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), 93–96.
- [8] N. D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, Lecture notes, Oberwolfach, 2007, [arXiv:0709.2908](https://arxiv.org/abs/0709.2908)
- [9] M. Jukić Bokun, *On the rank of elliptic curves over  $\mathbb{Q}(\sqrt{-3})$  with torsion group  $\mathbb{Z}_3 \times \mathbb{Z}_3$  and  $\mathbb{Z}_3 \times \mathbb{Z}_6$* , Proc. Japan Acad. Ser. A Math. Sci. **87** (2011), 61–64.
- [10] S. Kamienny, *Torsion points on elliptic curves and  $q$ -coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
- [11] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
- [12] L. Kulesz, C. Stahlke, *Elliptic curves of high rank with nontrivial torsion group over  $\mathbb{Q}$* , Experiment. Math. **10** (2001), 475–480.
- [13] J.-F. Mestre, *Rang des courbes elliptiques d’ invariant donné*, C. R. Acad. Sci. Paris **314** (1992), 919–922.
- [14] J.-F. Mestre, *Rang de certaines familles de courbes elliptiques d’ invariant donné*, C. R. Acad. Sci. Paris **327** (1998), 763–764.
- [15] K. Nagao, *An example of elliptic curve over  $Q$  with rank  $\geq 20$* , Proc. Japan Acad. Ser. A Math. Sci. **69** (1993) 291–293.
- [16] PARI/GP, version 2.4.0, Bordeaux, 2008, <http://pari.math.u-bordeaux.fr>
- [17] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144** (2010), 17–52.
- [18] K. Rubin, A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), 559–569.
- [19] K. Rubin, A. Silverberg, *Twists of elliptic curves of rank at least four*, in: Ranks of Elliptic Curves and Random Matrix Theory, Cambridge University Press, 2007, pp. 177–188.
- [20] U. Schneiders, H. G. Zimmer, *The rank of elliptic curves upon quadratic extension*, in Computational Number Theory, Eds.: A. Pethő, M.E. Pohst, H.C. Williams and H.G. Zimmer, W. de Gruyter, 1991, pp. 239–260.
- [21] J. Silverman, *The Arithmetic of Elliptic curves*, Springer, New York, 2009.
- [22] C.L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.
- [23] T. Womack, *Curves with moderate rank and interesting torsion group*, <http://tom.womack.net/math/torsion.htm>

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL PAÍS VASCO, APTDO. 644, 48080 BILBAO, SPAIN

*E-mail address*, J. Aguirre: [julian.aguirre@ehu.es](mailto:julian.aguirre@ehu.es)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

*E-mail address*, A. Dujella: [duje@math.hr](mailto:duje@math.hr)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OSIJEK, TRG LJUDEVITA GAJA 6, 31000 OSIJEK, CROATIA

*E-mail address*, M. Jukić Bokun: [mirela@mathos.hr](mailto:mirela@mathos.hr)

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL PAÍS VASCO, APTDO. 644, 48080 BILBAO, SPAIN

*E-mail address*, J. C. Peral: [juancarlos.peral@ehu.es](mailto:juancarlos.peral@ehu.es)