CONSTRUCTION OF HIGH RANK ELLIPTIC CURVES

ANDREJ DUJELLA AND JUAN CARLOS PERAL

TO THE MEMORY OF ELIAS M. STEIN WITH ADMIRATION AND GRATITUDE

Abstract. We list a number of strategies for construction of elliptic curves having high rank with special emphasis on those curves induced by Diophantine triples, in which we have contributed more. These strategies have been developed by many authors.

In particular we present a new example of a curve, induced by a Diophantine triple, with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and with rank 9 over $\mathbb{Q}$. This is the present record for this kind of curves.

1. Introduction

An elliptic curve E/K over a field K is a smooth projective variety of genus 1 with a specified K-rational base point O. When the characteristic of K is not equal to 2 or 3, an elliptic curve can be represented by a Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in K \text{ with } -4A^3 - 27B^2 \neq 0.$$

With these conditions, a group operation, called the chord and tangent process, with a neutral point O can be defined on the set $E(K)$ of K-rational points. The following theorem was proved by Mordell [Mo] in 1922 for $K = \mathbb{Q}$ and generalized by Weil [We] in 1928 not only to elliptic curves over number fields but also to abelian varieties.

Theorem 1. *(**Mordell-Weil**) Let K be a number field and E/K an elliptic curve defined over K. The set of K-rational points $E(K)$ forms a group and $E(K)$ is finitely generated. It has the form*

$$E(K) = E_{tors}(K) \times \mathbb{Z}^r$$

where the torsion subgroup $E_{tors}(K)$ is finite and the non-negative integer r is called the rank of E/K.

So determining the structure of $E(K)$ involves two problems: the structure of $E_{tors}(K)$ and the value of the rank r. These two problems are far from being solved and only partial results are known.

When $K = \mathbb{Q}$ the possible $E_{tors}(K)$ are described in the following theorem. See [K] for a description of the models.

Theorem 2. *(**Mazur** [Ma]) There are 15 possibilities for the torsion group of an elliptic curve over $\mathbb{Q}$ given as follows:*

- *$\mathbb{Z}/m\mathbb{Z}$ with $1 \leq m \leq 10$ and $m = 12$*
- *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$*

2010 *Mathematics Subject Classification.* 11G05.

A. D. acknowledges support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). A. D. was also supported by the Croatian Science Foundation under the project no. IP-2018-01-1313. J. C. P. was supported by the grant: MTM2014-52347-C2-1-R.

For quadratic fields the next theorem gives all the possibilities.

Theorem 3. *(***Kenku and Momose** [KM]**, Kamienny** [Ka]*)*
Let $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ and square-free, be a quadratic number field and E an elliptic curve defined over K. Then the torsion subgroup for $E(K)$ is one of the following 26 groups:

- $\mathbb{Z}/m\mathbb{Z}$ *with* $1 \le m \le 16$ *and* $m = 18$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ *with* $1 \le m \le 6$
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}$ *with* $1 \le m \le 2$*; only possible for* $K = \mathbb{Q}(\sqrt{-3})$
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*; only possible for* $K = \mathbb{Q}(\sqrt{-1})$.

See [Ra] for models.

For other number fields K there are partial results describing the possible torsion subgroups $E_{tors}(K)$. Even in the case of quadratic fields given a fixed quadratic field determining which of the 26 possibilities given in the Kamienny, Kenku, Momose theorem appear in this field is not completely solved.

The problem of determining the rank is a difficult one, and no general algorithm is known to solve it. For the current rank records of elliptic curves over $\mathbb{Q}$, with prescribed torsion group, see [Du1] for a detailed information. Here follows a resume.

Torsion	Rank	Author(s)
0	28	Elkies(2006)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	14	Elkies (2018)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies(2006), Dujella & Peral (2014)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (2009), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	8	Dujella, Elkies, Eroshkin (2008) Dujella & Peral (2012), Dujella & Peral & Tadić (2014) Gandhikumar & Voznyy (2019)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006) Eroshkin (2009, 2011), Dujella & Lecacheux (2009) Dujella & Eroshkin (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006), Dujella & MacLeod & Peral (2013)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009), van Beek (2015)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella & Peral (2012, 2019)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006), Dujella & Peral & Tadić (2015)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000, 2001, 2006, 2008), Campbel & Goins (2003), Rathbun (2003, 2006, 2013) Dujella & Rathbun (2006)

In the search of high rank curves it is useful to have high rank families of elliptic curves (or high rank curves over $\mathbb{Q}(u)$) and then look for particular examples within these families. The current rank records of elliptic curves over $\mathbb{Q}(u)$ with prescribed torsion subgroup can be seen also in [Du1]. The next table gives a summary.

0	18	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/4\mathbb{Z}$	5	Kihara (2004), Elkies (2007), Dujella & Peral & Tadić (2014), Khoshnam & Moody (2016)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009), MacLeod (2014)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008), Dujella & Peral (2012)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009), MacLeod (2014)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella & Peral (2012), MacLeod (2014)
$\mathbb{Z}/9\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/10\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/12\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	7	Elkies (2007).
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	4	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	2	Dujella & Peral (2012, 2015, 2017), MacLeod (2013)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

It is an open question whether the rank of an elliptic curve over a fixed number field can be arbitrarily large. It was a widely accepted conjecture that there is no upper bound for the rank of elliptic curves, although no curve over $\mathbb{Q}$ of rank greater than 28 is known. In fact the elliptic curve with the largest known rank over $\mathbb{Q}$ was found by Elkies in 2006 and has rank at least 28 (the rank is exactly equal to 28 assuming GRH, see [KSW]).

However there are also heuristic arguments that suggest the boundedness of the rank of elliptic curves. In the following table the second column gives the rank of known infinite families for each torsion group, over $\mathbb{Q}$, and the third column gives the predicted maximum, for such kind of infinite families, according to the heuristic in [PPVW]. So, if this heuristic is true, only a finite number of curves would have rank higher that 21 and consequently the rank of elliptic curves over $\mathbb{Q}$ would be bounded by an absolute constant.

It can be observed that the known estimates and the prediction in the heuristic fit very well. In fact for the torsion groups $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ those two values are equal. In all the other cases the predicted value is greater than the known lower value but only in one or two units.

Torsion	Known Lower Bound	Heuristic Prediction
0	19	21
$\mathbb{Z}/2\mathbb{Z}$	11	13
$\mathbb{Z}/3\mathbb{Z}$	7	9
$\mathbb{Z}/4\mathbb{Z}$	6	7
$\mathbb{Z}/5\mathbb{Z}$	4	5
$\mathbb{Z}/6\mathbb{Z}$	5	5
$\mathbb{Z}/7\mathbb{Z}$	2	3
$\mathbb{Z}/8\mathbb{Z}$	3	3
$\mathbb{Z}/9\mathbb{Z}$	1	2
$\mathbb{Z}/10\mathbb{Z}$	1	2
$\mathbb{Z}/12\mathbb{Z}$	1	2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8	9
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	5	5
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	3	3
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1	2

2. Strategies

The construction of families of elliptic curves having high rank often is based on two basic strategies described by Elkies in [El1].

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 [Me1].

There are other strategies such as the following.

c) Restricting to a particular kind of curves.

d) Using the general equation of the curves with a particular torsion group.

e) Looking for good quadratic sections.

f) Also an 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, see [DP1]. This is the current record for this torsion group.

3. Elliptic curves with j invariant equal to 1728.

3.1. **Mestre construction.** In order to illustrate some of the strategies mentioned above we present here the construction of a family of curves having $j = 1728$. A model over $\mathbb{Q}$ for these curves is

$$Y^2 = X^3 - B\,X.$$

In particular when $B = d^2$ the curves are the d-twist of the curve $Y^2 = X^3 - X$ and they are a model for the congruent number problem curve.

In 1991 Mestre [Me2] constructed a family of curves with $j = 1728$ and having rank 4. For the construction Mestre takes the polynomial

$$P(X) = (X - a)(X - b)(X - c)(X + a + b + c).$$

So $P(x) = X^4 + a_2X^2 + a_1X + a_0$ where

$$\begin{aligned} a_2 =& -(a^2 + ab + b^2 + ac + bc + c^2),\\ a_1 =& (a + b)(a + c)(b + c),\\ a_0 =& -abc(a + b + c). \end{aligned}$$

Then the curve E with equation $x^4 + a_2y^2 + a_1y + a_0 = 0$ has the points (a, a), (b, b), (c, c) and $(-(a + b + c), -(a + b + c))$.

If $a_0 = -u^4$ then the curve has an additional independent point with coordinates $O = (-u, 0)$. The condition $a_0 = -u^4$ is equivalent to $u^4 = abc(a + b + c)$. Euler, see [Di] page 660, gave the following solution

$$u = 1, \quad a = \frac{t(2t^2 - 1)}{2t^2 + 1}, \quad b = \frac{2t^2 - 1}{2t(2t^2 + 1)}, \quad c = \frac{4t}{2t^2 - 1}.$$

The curve E, defined over $\mathbb{Q}(t)$, has genus 1 and it is equivalent to the elliptic curve with equation

$$Y^2 = X^3 + a_2(a_1^2 - 4a_0a_2)X.$$

By taking O as base point, the independence of the other points can be proved by showing a particular value of t for which the specialized points are independents. See Silverman [Si, Theorem 11.4] for this kind of result.

For example, for $t = 1$ the determinant of the matrix of heights is equal to 603.6123....

So the rank is ≥ 4 and the elliptic curve, avoiding denominators, is $Y^2 = X^3 + BX$ where

$$\begin{aligned} B = -4(-1 + 2t^2)^2(1 + 2t^2)^2(3 + 2t^2)(1 + 6t^2)(1 + 12t^2 + 4t^4)(3 + 4t^2 + 12t^4)\\ \times (1 + 2t^2 + 76t^4 + 176t^6 + 304t^8 + 32t^{10} + 64t^{12}). \end{aligned}$$

3.2. **Another construction.** In [ACP] the following variant of the method of Fermigier [Fe] is used in order to get a curve with j-invariant 1728 and rank 4.

The resulting curve has simpler coefficients than the ones in Mestre construction.

Begin with the monic, even polynomial of degree 8

$$p(x) = \prod_{i=1}^{i=4}(x^2 - a_i^2) = x^8 - s_1x^6 + s_2x^4 - s_3x^2 + s_4$$

where s_i is the i-th elementary symmetric polynomial in 4 variables, evaluated at $(a_1^2, a_2^2, a_3^2, a_4^4)$. Then $p(x) = q(x)^2 - r(x)$ with

$$q(x) = x^4 - \frac{s_1}{2}x^2 + \frac{s_3}{s_1} \text{ and } r(x) = (\frac{s_1^2}{4} + \frac{2s_3}{s_1} - s_2)x^4 + (\frac{s_3^2}{s_1^2} - s_4)$$

The associated cubic model for the quartic $y^2 = r(x)$ is the curve $y^2 = x^3 - Bx$ with

$$B = -(\frac{s_1^2}{4} + \frac{2s_3}{s_1} - s_2)(\frac{s_3^2}{s_1^2} - s_4).$$

It has at least the eight rational points $(r_4a_i^2, \pm r_4a_iq(a_i))$ where r_4 is the coefficient of x^4 in r. Observe that B has degree 14 in each a_i. Avoiding denominators, the curve can be written as

$$Y^2 = X^3 - bX,$$

where

$$b = 4(a_1a_2 + a_3a_4)(a_1a_2 - a_3a_4)(a_1a_3 + a_2a_4)(a_1a_3 - a_2a_4)(a_1a_4 + a_2a_3)(a_1a_4 - a_2a_3)$$
$$\times (a_1^2 + a_2^2 - a_3^3 - a_4^2)(a_1^2 - a_2^2 + a_3^3 - a_4^2)(a_1^2 - a_2^2 - a_3^3 + a_4^2)(a_1^2 + a_2^2 + a_3^3 + a_4^2).$$

In [ACP] there are several examples leading to curves with rank 13. Watkins has found that for $(a_1, a_2, a_3, a_4) = (304, 722, 1136, 1433)$ the corresponding curve in this family has rank 14. The curve for these values, once the fourth powers of b are reduced, is

$$Y^2 = X^3 - 16103990975507628040676417090899932X.$$

A basis for a subgroup of the full Mordell-Weil group (modulo torsion) can be found in [Du1].

Observe that, when considered over the quadratic field $\mathbb{Q}(i)$, this curve has rank equal to 28 due to the fact that it is isomorphic its twist by -1.

4. General equation of curves having torsion group $\mathbb{Z}/4\mathbb{Z}$.

Now we explain the construction of Elkies [El1] for curves with torsion group $\mathbb{Z}/4\mathbb{Z}$. He starts with the general surface having torsion $\mathbb{Z}/4\mathbb{Z}$. This surface is given by

$$Y^2 + aXY + abY = X^3 + bX^2.$$

A torsion point of order 4 is $(0, 0)$. Elkies notices that this torsion can be obtained for some elliptic $K3$ surfaces. In this case the maximum rank is obtain with the following type of reducible fibers for such a surface: four of the type I_4, two of the type I_2 and four of the type I_1, so giving a contribution to the Néron-Severi group of $4(4 - 1) + 2(2 - 1)) = 14$, hence the rank over this surface is at most $20 - 2 - 14 = 4$.

Later on Elkies shows that the discriminant -163 surface does have an elliptic model that attains rank 4 with torsion group $\mathbb{Z}/4\mathbb{Z}$, with

$$\begin{aligned} a =& (8t - 1)(32t + 7) \\ b =& 8(t + 1)(15t - 8)(31t - 7). \end{aligned}$$

With a simple change of variables the surface can be written as

$$Y^2 = X^3 + (a^2 - 8b)X^2 + 16b^2X.$$

Inserting the values of a and b mentioned above results that the following $K3$ elliptic surface

$$\begin{aligned} Y^2 =& X^3 + (65536t^4 - 17472t^3 - 10176t^2 + 18672t - 3535)X^2 \\ &+ 1024(t + 1)^2(15t - 8)^2(31t - 7)^2X \end{aligned}$$

has torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 4. A torsion point of order 4 in this model is

$$(32(t + 1)(15t - 8)(31t - 7), 2^5(1 + t)(-1 + 8t)(-8 + 15t)(-7 + 31t)(7 + 32t))$$

and the X-coordinates of four independent points of infinite order are:

$$\begin{aligned} X_1 =& -361(t + 1)(31t - 7), \\ X_2 =& -4(t + 1)(15t - 8)(16t - 7)^2, \\ X_3 =& -16(t + 1)(8t + 7)^2(15t - 8), \\ X_4 =& 4(15t - 8)(16t + 1)^2(31t - 7). \end{aligned}$$

Elkies mentions, without explicitly writing such examples, that there are several quadratic sections giving families of rank 5 for this torsion and several combinations of pairs of quadratic section leading to infinite families of curves with rank 6 parametrized by the points of elliptic curves of positive rank.

Previous to Ekies construction, in 2007, for rank 5 families Kihara [Ki1] and [Ki2] found in 2004 a family of rank 5. The coefficients in the Kihara construction are much bigger than those in Elkies examples and so are less suited for finding good particular examples of high rank curves. In fact the family in Elkies article is $y^2 = x^3 + A(t)x^2 + B(t)x$ with $A(t)$ depends on a polynomial of degree 4 and $B(t)$ depends on a polynomial of degree 6, and the examples with rank 5 have polynomial coefficients of degree 8 and 16 while the corresponding coefficients in the Kihara family have degrees 52 and 102 respectively. In 2016 Khoshnam and Moody [KhMo] have given an example of rank 5 over $\mathbb{Q}(u)$ with a simpler version of Kihara method. In fact the coefficients A and B in this family depend of polynomials of degree 19 and 38 respectively.

The value $t = \frac{18745}{6321}$, in the Elkies family, yields a curve with rank 12. This is the current record for torsion $\mathbb{Z}/4\mathbb{Z}$. See [Du1] for details of this curve.

We have made explicit the ideas of Elkies and we have found 26 families of rank 5 and several infinite families of rank 6 parametrized by elliptic curves with positive rank.

Now we list the 26 substitutions of t leading to subfamilies of rank 5 inside the rank 4 family of Elkies.

$$\begin{array}{ccc}
t = \dfrac{3\left(u^2 - 14u + 1519\right)}{7\left(u^2 - 287\right)}, & t = \dfrac{2\left(u^2 - u + 538\right)}{3\left(u^2 + 1604\right)}, & t = \dfrac{u^2 - 38u + 1216}{3\left(u^2 - 316\right)}, \\
t = -\dfrac{u^2 - 212u + 596}{4\left(u^2 - 11076\right)}, & t = -\dfrac{3(6u + 251)}{u^2 - 2065}, & t = -\dfrac{u^2 - 250u - 16352}{u^2 + 32060}, \\
t = -\dfrac{u^2 - 350u + 21924}{u^2 - 22276}, & t = \dfrac{4\left(u^2 - 1\right)}{7u^2 + 17}, & t = -\dfrac{u^2 - 42u - 3640}{u^2 + 6656}, \\
t = -\dfrac{u^2 - 54u - 272}{u^2 + 960}, & t = -\dfrac{u^2 - 135}{2(4u + 75)}, & t = \dfrac{u^2 - 3562u + 2457568}{(u - 1120)(u + 1120)}, \\
t = \dfrac{u^2 - 1196u - 202816}{2(u - 672)(u + 672)}, & t = -\dfrac{u^2 + 770u + 138960}{u^2 - 79936}, & t = -\dfrac{u^2 + 42u + 328}{(u - 28)(u + 28)}, \\
t = -\dfrac{u^2 - 1017}{8(4u + 237)}, & t = \dfrac{u^2 - 4u - 3552}{2\left(u^2 - 7696\right)}, & t = \dfrac{u^2 - 22u - 40}{u^2 - 512}, \\
t = -\dfrac{2\left(119u^2 + 569\right)}{5\left(723u^2 - 1027\right)}, & t = -\dfrac{u^2 - 4977}{8(7u + 1083)}, & t = -\dfrac{u^2 - 1017}{8(4u + 237)}, \\
t = -\dfrac{u^2 - 113}{8(7u - 57)}, & t = -\dfrac{u^2 - 31}{2(u^2 + 24)}, & t = -\dfrac{u^2 + 406u + 11878}{(u - 196)(u + 196)}, \\
t = -\dfrac{u^2 + 4418u - 132540}{u^2 + 17097660}, & t = \dfrac{7u^2 - 1534u + 82880}{u^2 - 13809}. &
\end{array}$$

We have also found, in 2014, a second example for a curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 12. It correspond to the value $u = \frac{263}{619}$ in one of the subfamilies given above: the one obtained by the substitution $t = \frac{4(u^2-1)}{7u^2+17}$. So the value of t in the initial Elkies family of rank 4 is $t = -\frac{13083}{72895}$. This subfamily of rank 5 is given by the following equation:

$$\begin{aligned}
y^2 = x^3 &+ 3(-224485317 - 211193548u^2 + 40986498u^4 - 2284428u^6 + 6034075u^8)x^2 \\
&+ 147456(-7 + u)^2(7 + u)^2(-9 + 5u)^2(9 + 5u)^2(17 + 7u^2)^2(13 + 11u^2)^2x.
\end{aligned}$$

The rank 12 curve ($u = \frac{263}{619}$), once fourth powers are reduced, is

$$\begin{aligned} y^2 = x^3 &- 19891640677357186552063 9x^2 \\ &+ 99182666553709982296167379815851637739110400 00x \end{aligned}$$

and 12 independent points of infinite order (on the corresponding reduced minimal Weierstrass equation) are given in [Du1].

5. Looking for quadratic sections. $\mathbb{Z}/8\mathbb{Z}$ torsion group case.

5.1. **Tate normal form for $\mathbb{Z}/8\mathbb{Z}$ group.** Tate's normal form for an elliptic curve with torsion group $\mathbb{Z}/8\mathbb{Z}$ is given by

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

(see [Kn, Section V.5]). 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, Section V.5]. 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 using quadratic sections. In fact their x-coordinates should be either divisors of B or rational squares times divisors of B.

5.2. **Quadratic sections leading to rank 1 subfamilies.** In the case of torsion group $\mathbb{Z}/8\mathbb{Z}$ families having rank at least 1 over $\mathbb{Q}(u)$ have been previously found by several authors, see [Ku], [Le]. We have improved these results, in [DP2], by showing the existence of two elliptic curves having this torsion group and rank at least 2 over $\mathbb{Q}(u)$ and the existence of infinitely many elliptic curves over $\mathbb{Q}$ with this torsion group and rank at least 3, parametrized by an elliptic curve with positive rank. All these improvements use the parametrization of appropriate quadratic sections. Let us mention that the heuristic from [PPVW, Section 8.3] predicts that there are only finitely many elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/8\mathbb{Z}$ and rank greater than 3.

For this torsion group we show nine conditions on v leading to rank 1 families. Some of them were already known due to the authors quoted before. In fact Lecacheux found in [Le] two values leading to rank 1 families by using adequate fibrations of the general model for torsion group $\mathbb{Z}/8\mathbb{Z}$. They are $v_{L_1} = \frac{-2w}{w^2+2}$ and $v_{L_2} = \frac{w(w+2)}{w^2+4w+2}$ which are included in the first and the fourth places in our list.

$$\begin{aligned}
x_1 &= -2v^2(-1+2v^2), & v_1 &= \frac{-2w}{2+w^2},\\
x_2 &= \frac{-(-1+v)^4(-5+8v)(-5+18v)}{4(-2+3v)^2}, & v_2 &= \frac{5(1+w^2)}{2(9+4w^2)},\\
x_3 &= \frac{-4(-3+v)(-1+v)^2v^4(-1+3v)}{(1-4v+2v^2)^2}, & v_3 &= \frac{(1+3w^2)}{3+w^2},\\
x_4 &= 16(-1+v)^2v^2(1-2v+2v^2), & v_4 &= \frac{w(w+2)}{2+4w+w^2},\\
x_5 &= \frac{-64(-1+v)^2v^2(-1-v+v^2)}{(-1-4v+4v^2)^2}, & v_5 &= \frac{(-2+w)w}{1+w^2},\\
x_6 &= -(-1+v)^2(1-6v+4v^2), & v_6 &= \frac{2-2w+w^2}{4+w^2},\\
x_7 &= 4v^4, & v_7 &= \frac{5-w^2}{4(1+w)},\\
x_8 &= \frac{-(-1+v)^2(-5+2v)^2(25-70v+36v^2)}{(-7+6v)^2}, & v_8 &= \frac{34-6w+w^2}{36+w^2},\\
x_9 &= -\frac{4(v-1)^4(4v-1)}{4v-3}, & v_9 &= \frac{1+3w^2}{4(1+w^2)}.
\end{aligned}$$

5.3. **Details for one of the families 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 rank 1 families above. The fact is that to force the value

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

to become the x-coordinate of a point in the curve is equivalent to solving

$$-(v-3)(3v-1) = \text{Square},$$

whose solution is given by $v_3 = \frac{1+3w^2}{w^2+3}$.

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

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

5.4. **A family with rank 2 and torsion group $\mathbb{Z}/8\mathbb{Z}$.** By searching on several homogeneous spaces of the associate curve we have found the possibility of imposing two new conditions which lead to new points. The values xx_1 and xx_2 jointly with the specialization of the parameter are

$$\begin{aligned}
X_1 &= \frac{(-1+w)^2(1+w)^2(5+7w^2)^2(11+25w^2)}{16}, & W_1 &= \frac{11-u^2}{10u},\\
X_2 &= \frac{(-1+w)^2(1+w)^2(1+11w^2)^2(7+29w^2)}{16w^2}, & W_2 &= \frac{29-12u+u^2}{-29+u^2}.
\end{aligned}$$

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

Let us give details in the first case. First we see that forcing

$$x = \frac{(w-1)^2(w+1)^2(7w^2+5)^2(25w^2+11)}{16}$$

to be the x-coordinate of a new point into the curve

$$Y^2 = X^3+(-31-148w^2+214w^4-116w^6+337w^8)X^2+256(-1+w)^4(1+w)^4(1+3w^2)^4X$$

we get the condition that $25w^2+11$ has to be a square. This is achieved with $W_1 = \frac{11-u^2}{10u}$.

Once we insert W_1 into the coefficients AA_8, BB_8 we get as new coefficients AAA_8, BBB_8 given by

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

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 a torsion point of order 8 is:

$$T_1 = -8(-11+u)(-1+u)(1+u)(11+u)(363+34u^2+3u^4)^3.$$

That the rank of this curve is at least 2 over $\mathbb{Q}(u)$ can be proved using a specialization argument, since the specialization map is a homomorphism, see [DP2].

After our preprint presenting the preceding two curves of rank two appeared on the arXiv, by using similar methods, MacLeod found another two curves of rank 2 [McL].

5.5. **Existence of infinitely many curves with rank 3.** Finally it can be proved that there exist infinitely many elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ 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.:

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

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 solution, $(r,t)=(1,60)$ for example, hence it is birationally equivalent to the cubic $y^2 = x^3-463x^2+45936x$ whose rank is 2 as proved with `mwrank` [Cr]. 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 [Le] or [Ra] for this kind or argument.

6. Elliptic curves induced by Diophantine triples

6.1. Definitions and first results.

Definition. A set $\{c_1, c_2, \ldots, c_m\}$ of non-zero integers (rationals) is called a (rational) $D(n)$-m-tuple if $c_i \cdot c_j + n$ is a perfect square for all $1 \le i < j \le m$. A $D(1)$-m-tuple is also called a Diophantine m-tuple.

Let $\{c_1, c_2, c_3, c_4\}$ be a rational Diophantine quadruple. Consider a subtriple $\{c_1, c_2, c_3\}$ and define an elliptic curve by the equation

$$y^2 = (c_1\,x + 1)(c_2\,x + 1)(c_3\,x + 1). \tag{E}$$

We say that E is the elliptic curve induced by the Diophantine triple $\{c_1, c_2, c_3\}$. Let

$$c_i c_j + 1 = t_{i,j}^2, \quad 1 \le i < j \le 4.$$

Then the curve E has at least the following three rational points of order 2:

$$T_1 = [\,-1/c_1, 0\,], \qquad T_2 = [\,-1/c_2, 0\,], \qquad T_3 = [\,-1/c_3, 0\,],$$

and at least three other rational points:

$$\begin{cases} P_1 = [\,0, 1\,], \\ P_2 = [\,c_4, t_{1,4}\,t_{2,4}\,t_{3,4}\,], \\ P_3 = \Big[\,\dfrac{t_{1,2}\,t_{1,3} + t_{1,2}\,t_{2,3} + t_{1,3}\,t_{2,3} + 1}{c_1c_2c_3}, \\ \qquad \dfrac{(t_{1,2} + t_{1,3})(t_{1,2} + t_{2,3})(t_{1,3} + t_{2,3})}{c_1c_2c_3}\,\Big]. \end{cases} \tag{1}$$

Our goal is to show that Diophantine triples and quadruples are good tools in the search for high rank elliptic curves having as torsion group one of the non-cyclic groups in Mazur's theorem.

In the case of torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ we show that adequate specialization of the parameters induce subfamilies of curves with rank 4, rank 5 and rank 6 and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We use a set of quadruples presented in [Du2]. In [ADP] a family of rank 5 over $\mathbb{Q}(t)$ was constructed, later several families of rank 6 over $\mathbb{Q}(t)$ were found [DP3]. In the general case (not required to be induced by Diophantine triples) Elkies constructed a family with rank 7.

In our paper [DP1] we constructed a curve over $\mathbb{Q}(t)$ induced by Diophantine triples having rank 4 and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We also show an example of a curve with rank 9. These are the best results known for that torsion.

In the case of torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ we present three curves over $\mathbb{Q}(t)$ with rank 2 induced by Diophantine triples. This ties the results for the general case, see [DP3]. We also show that the curve with rank 6 over $\mathbb{Q}$, (which is the record for this torsion group and was found by Elkies, see [Du1]), is induced by a Diophantine triple.

Finally, in the case of torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ it is known that all such curves are induced by Diophantine triples (see [CG, Du4]).

6.2. **Rank 3 over $\mathbb{Q}(t)$.**

In [Du2] several families of $D(n)$-quadruples are described. We will use for our construction the one given by

$$\{a, a(k+1)^2 - 2\,k, a(2\,k+1)^2 - 8\,k - 4, a\,k^2 - 2\,k - 2\}.$$

For each a and k this quadruple is a $D(2\,a(2\,k+1)+1)$-quadruple. Now we specialize to the following value of k:

$$k = \frac{-1 - 2\,a + n^2}{4\,a}.$$

The resulting quadruple is a $D(n^2)$-quadruple and once divided by n we get the following rational $D(1)$-quadruple:

$$\begin{cases} c_1(a,n) = \dfrac{a}{n}, \\ c_2(a,n) = \dfrac{((n-3)(n-1)+2\,a)((n+1)(n+3)+2\,a)}{16\,a\,n}, \\ c_3(a,n) = \dfrac{(n-3)(n-1)(n+1)(n+3)}{4\,a\,n}, \\ c_4(a,n) = \dfrac{((n-3)(n-1)-2\,a)((n+1)(n+3)-2\,a)}{16\,a\,n}. \end{cases} \tag{2}$$

In the terminology of Gibbs this is an irregular and twice semi-regular Diophantine quadruple. A Diophantine triple $\{a_1,a_2,a_3\}$ is regular if $(a_3-a_2-a_1)^2 = 4(a_1a_2+1)$, while a Diophantine quadruple $\{a_1,a_2,a_3,a_4\}$ is regular if $(a_4+a_3-a_1-a_2)^2 = 4(a_1a_2+1)(a_3a_4+1)$. It can be checked that (2) is irregular, but it contains two regular triples: $\{c_1,c_2,c_4\}$ and $\{c_2,c_3,c_4\}$.

Now we define the elliptic curve associated to the triple $\{c_1,c_2,c_3\}$ as explained above, i.e.:

$$y^2 = (c_1(a,n)x+1)(c_2(a,n)x+1)(c_3(a,n)x+1).$$

Note that we choose an irregular triple which is a subtriple of an irregular quadruple. Otherwise, by [Du3], the points P_1, P_2, P_3 would not be independent.

Besides the 2-torsion points, this curve has the points with x-coordinate given by

$$0, \quad c_4(a,n) \quad \text{and} \quad \frac{t_{1,2}\,t_{1,3}+t_{1,2}\,t_{2,3}+t_{1,3}\,t_{2,3}+1}{c_1(a,n)c_2(a,n)c_3(a,n)},$$

where as before $t_{i,j} = t_{i,j}(a,n) = \sqrt{c_i(a,n)c_j(a,n)+1}$, $1 \le i < j \le 3$. In terms of a and n, the three rational points (1) are:

$$\begin{aligned} P_1 &= [\,0,1\,], \\ P_2 &= \Big[\frac{(n^2+4\,n-2\,a+3)(n^2-4\,n-2\,a+3)}{16\,a\,n}, \\ &\qquad -\frac{(n^2-2\,a+3)(n^4-10\,n^2-4\,a^2+9)(n^4-2\,a\,n^2-10\,n^2-6\,a+9)}{512\,a^2\,n^3}\Big], \\ P_3 &= \Big[\frac{6\,n}{(n-3)(n+3)}, \frac{(n^2+6\,a-9)(3\,n^2+2\,a-3)}{4\,a(n-3)(n+3)}\Big]. \end{aligned}$$

Theorem 4. *The curve $y^2 = (c_1(a,n)x+1)(c_2(a,n)x+1)(c_3(a,n)x+1)$ has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank ≥ 3 over $\mathbb{Q}(n,a)$. The points P_1, P_2 and P_3 are of infinite order and independent.*

6.3. Construction of a curve of rank 4 over $\mathbb{Q}(t)$.

Now we look for conditions on a and n such that there are new rational points on the curve. The coordinate transformation

$$x \mapsto c_1(a,n)c_2(a,n)c_3(a,n)\,x, \quad y \mapsto c_1(a,n)c_2(a,n)c_3(a,n)\,y$$

applied to the curve leads to

$$y^2 = (x+c_1(a,n)c_2(a,n))(x+c_1(a,n)c_3(a,n))(x+c_2(a,n)c_3(a,n)).$$

Next, the change $x \mapsto x - c_1(a,n)c_2(a,n)$ transforms it into

$$\begin{aligned} y^2 = x(x &+ c_1(a,n)c_3(a,n) - c_1(a,n)c_2(a,n)) \\ &\times (x + c_2(a,n)c_3(a,n) - c_1(a,n)c_2(a,n)). \end{aligned}$$

From this point on, in order to avoid denominators, we will make, when necessary, the appropriate change of variables to write the curve as

$$y^2 = x^3 + A\,x^2 + B\,x \tag{3}$$

where $A(a,n)$ and $B(a,n)$ have are polynomials with integer coefficients. This leads to the following values of the coefficients A and B:

$$\begin{aligned} A(a,n) &= 81 + 108\,a + 108\,a^2 - 96\,a^3 - 32\,a^4 - 180\,n^2 - 84\,a\,n^2 - 120\,a^2\,n^2 \\ &\quad - 32\,a^3\,n^2 + 118\,n^4 - 28\,a\,n^4 + 12\,a^2\,n^4 - 20\,n^6 + 4\,a\,n^6 + n^8, \\ B(a,n) &= 4\,a^2(9 + 2\,a - n^2)(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2) \\ &\quad \times (-3 + 2\,a + 3\,n^2)(-9 + 4\,a^2 + 10\,n^2 - n^4). \end{aligned}$$

The x-coordinates of the three infinite order points are

$$\begin{aligned} x_1 &= 4\,a^2(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2), \\ x_2 &= \frac{(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2)(9 - 6\,a - 10\,n^2 - 2\,a\,n^2 + n^4)^2}{16\,n^2}, \\ x_3 &= 2\,a(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2)(-3 + 2\,a + 3\,n^2). \end{aligned}$$

Now we look for those polynomial factors of B that can be conditioned in a simple way to yield a new point in the curve.

The condition for $(3 + 2a - 4n + n^2)(-3 + 2a + 3n^2)(-9 + 4a^2 + 10n^2 - n^4)$ to become the X coordinate of a new point is that $2(9 + 6a + 8a^2 - 18n - 4an + 8n^2 - 2an^2 + 2n^3 - n^4)$ converts into a square. This can be achieved with the value $n = 7/3$. The coefficients of the curve are

$$\begin{aligned} A(a) &= -2(-51200 + 109440a + 38880a^2 + 55404a^3 + 6561a^4) \\ B(a) &= 243a^2(20 + 3a)(-4 + 9a)(16 + 9a)(80 + 9a)(320 + 81a^2), \end{aligned}$$

and the x-coordinates of the preceding points jointly with the new one are

$$\begin{cases} x_1 = 81a^2(-4 + 9a)(80 + 9a) \\ x_2 = 27a(20 + 3a)(-4 + 9a)(80 + 9a) \\ x_3 = \dfrac{1}{441}(-4 + 9a)(80 + 9a)(160 + 171a)^2 \\ x_4 = 3(20 + 3a)(-4 + 9a)(320 + 81a^2). \end{cases} \tag{4}$$

This is a rank 4 curve over $\mathbb{Q}(a)$ since it can be proved that the four points quoted above are independent. The quadruple is

$$\begin{cases} q_1 = -\dfrac{3a}{7}, \\ q_2 = -\dfrac{(80 + 9a)(-4 + 9a)}{756\,a}, \\ q_3 = \dfrac{320}{189\,a}, \\ q_4 = -\dfrac{(4 + 9a)(-80 + 9a)}{756\,a}. \end{cases} \tag{5}$$

Theorem 5. *The elliptic curve induced by the first three components of the Diophantine quadruple* (5) *has torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *and rank* ≥ 4 *over* $\mathbb{Q}(a)$*. The points with* x*-coordinate given in* (4) *are of infinite order and independent.*

6.4. **Construction of curves of rank 5 over $\mathbb{Q}(t)$.** We have found 30 specializations of the parameter in the above rank 4 curve leading to curves having rank 5. In four cases with a further specialization we get rank 6 over $\mathbb{Q}(t)$.

We present the details in one of the cases and in the other three we just quote the specialization of the parameter a leading to rank 6 curves.

In order to force $9a(-20+9a)(16+9a)(80+9a)$ as X coordinate of a new point in the rank 4 curve we have to parametrize $10(-20+9a)(-2+9a) = \text{square}$. We get

$$a = \frac{2(-1+10w)(1+10w)}{9(-1+10w^2)}.$$

Now the rank 5 curve is $Y^2 = X^3 + A(w)X^2 + B(w)X$ where

$$\begin{aligned}
A(w) &= -2(-169 - 12020w^2 + 678000w^4 - 12680000w^6 + 80000000w^8),\\
B(w) &= (-1+10w)^2(1+10w)^2(-1+20w^2)(1+80w^2)(-31+400w^2)\\
&\quad (-41+500w^2)(9-200w^2+2000w^4).
\end{aligned}$$

Five independent points have the X-coordinates as follows

$$(6)\qquad \begin{cases}
x_1 = \frac{1}{9}(-1+10w)^2(1+10w)^2(1+80w^2)(-41+500w^2),\\
x_2 = \frac{1}{9}(-1+10w)(1+10w)(1+80w^2)(-31+400w^2)(-41+500w^2),\\
x_3 = \frac{1}{49}(1+80w^2)(-11+300w^2)^2(-41+500w^2),\\
x_4 = (1+80w^2)(-31+400w^2)(9-200w^2+2000w^4),\\
x_5 = 9(-1+10w)(1+10w)(-1+20w^2)(-41+500w^2).
\end{cases}$$

6.5. **Construction of curves of rank 6 over $\mathbb{Q}(t)$.** Now we can force $-9(-1+10w)^2(1+10w)^2(-1+20w^2)(-41+500w^2)$ as X coordinate of a new point in the previous rank 5 curve by solving $-(-2+7w)(2+7w) = \text{square}$, so we have

$$w = \frac{2(-1+v)(1+v)}{7(1+v^2)}$$

With this choice of w the curve transforms into the rank 6 curve given by $Y^2 = X^3 + A(v)X^2 + B(v)X$ where

$$\begin{aligned}
A(v) &= -2(130752711 - 35202346632v^2 + 260292593988v^4 - 1337869740984v^6\\
&\quad + 1975889131370v^8 - 1337869740984v^{10} + 260292593988v^{12} - 35202346632v^{14}\\
&\quad + 130752711v^{16}),\\
B(v) &= -(9-80v+9v^2)(9+80v+9v^2)(-27+13v^2)^2(-13+27v^2)^2\\
&\quad (9+8018v^2+9v^4)(31-258v^2+31v^4)(369-542v^2+369v^4)\\
&\quad (14409-41564v^2+400054v^4-41564v^6+14409v^8).
\end{aligned}$$

The X-coordinates of six independent points are as follows

$$(7)\qquad \begin{cases} x_1 = -\dfrac{1}{9}(-27+13v^2)^2(-13+27v^2)^2(9+8018v^2+9v^4) \\ \quad (369-542v^2+369v^4), \\ x_2 = -\dfrac{1}{9}(9-80v+9v^2)(9+80v+9v^2)(-27+13v^2) \\ \quad (-13+27v^2)(9+8018v^2+9v^4)(369-542v^2+369v^4), \\ x_3 = -\dfrac{1}{49}(9+8018v^2+9v^4)(369-542v^2+369v^4) \\ \quad (661-3478v^2+661v^4)^2, \\ x_4 = (9-80v+9v^2)(9+80v+9v^2)(369-542v^2+369v^4) \\ \quad (14409-41564v^2+400054v^4-41564v^6+14409v^8), \\ x_5 = -441(1+v^2)^2(-27+13v^2)(-13+27v^2)(9+8018v^2+9v^4) \\ \quad (31-258v^2+31v^4), \\ x_6 = -9(-27+13v^2)^2(-13+27v^2)^2(9+8018v^2+9v^4) \\ \quad (31-258v^2+31v^4), \end{cases}$$

and the quadruple becomes:

$$(8)\qquad \begin{cases} q_1 = \dfrac{2(-27+13v^2)(-13+27v^2)}{21(9+178v^2+9v^4)}, \\ q_2 = -\dfrac{(9+8018v^2+9v^4)(369-542v^2+369v^4)}{42(-27+13v^2)(-13+27v^2)(9+178v^2+9v^4)}, \\ q_3 = -\dfrac{160(9+178v^2+9v^4)}{21(-27+13v^2)(-13+27v^2)}, \\ q_4 = \dfrac{3(111-418v^2+111v^4)(237+2074v^2+237v^4)}{14(-27+13v^2)(-13+27v^2)(9+178v^2+9v^4)}. \end{cases}$$

By taking the specialization $v=5$ and applying [GT2, Theorem 1.1], we see that these six points are independent and the rank over $\mathbb{Q}(v)$ is exactly equal to 6 and the torsion group is equal to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Theorem 6. *The elliptic curve induced by the first three components of the Diophantine quadruple* (8) *has torsion* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *and rank* $=6$ *over* $\mathbb{Q}(v)$. *The points with* x*-coordinate given in* (7) *are of infinite order and independent.*

Details of the proofs can be seen in [DP3].

6.6. **Other curves of rank** 6 **over** $\mathbb{Q}(t)$**.** The following specializations of the parameter a in the rank 4 curve also produce rank 6 curves

$$(9)\qquad \begin{cases} a_1 = -\dfrac{64(831744-40128v+4288v^2-44v^3+v^4)}{9(-1520+88v+v^2)(-2736-264v+5v^2)}, \\ a_2 = -\dfrac{10732176-628992v+19192v^2-576v^3+9v^4}{36(-27+v)v(-364+9v)}, \\ a_3 = -\dfrac{5(-10+6v+v^2)(-18-18v+5v^2)}{9(12-2v+v^2)(3-v+v^2)}. \end{cases}$$

6.7. **Torsion** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ **and rank** 4**.** We consider elliptic curves with the torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Such curves have an equation of the form

$$(10)\qquad y^2 = x(x+x_1^2)(x+x_2^2), \quad x_1, x_2 \in \mathbb{Q}.$$

The point $[x_1x_2, x_1x_2(x_1+x_2)]$ is a rational point on the curve of order 4. The coordinate transformation $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ applied to the curve leads to the elliptic curve $y^2 = (x+ab)(x+ac)(x+bc)$ in the Weierstrass form, and by translation we obtain the equation

$$y^2 = x(x+ac-ab)(x+bc-ab). \tag{11}$$

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 the torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We may expect that this curve will have positive rank, since it also contains the point $[ab, abc]$. A convenient 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. We get the system

$$ac+1 = \square, \quad -\frac{c}{a}+1 = \square. \tag{12}$$

Inserting $ac+1 = s^2$ into $-\frac{c}{a}+1 = t^2$, we obtain

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

which has the parametric solution of the form

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

Inserting this in (11), after some simplifications, we get

$$y^2 = x^3 + 2(\alpha^2+\tau^2+4\alpha^2\tau^2+\alpha^4\tau^2+\alpha^2\tau^4)x^2 + (\tau+\alpha)^2(\alpha\tau-1)^2(\tau-\alpha)^2(\alpha\tau+1)^2x. \tag{13}$$

Now we force $x = (\tau+\alpha)^2(\alpha\tau-1)(\alpha\tau+1)$ to satisfy the equation (13), and we get the condition

$$\tau^2 + \alpha^2 + 2 = \square. \tag{14}$$

By [Ca, §10], the solution of (14) is given by

$$\tau = \frac{r^2 - s^2 - 2t^2 + 2v^2}{2(rt+sv)}, \quad \alpha = \frac{rs - 2tv}{rt+sv}. \tag{15}$$

On the other hand, by forcing $x = (\tau+\alpha)(\alpha\tau-1)^2(\tau-\alpha)$ to satisfy (13), we get the condition

$$\alpha^2\tau^2 + 2\alpha^2 + 1 = \square. \tag{16}$$

We seek for a parametric solution of the system (14) and (16). By our construction, this should give a family of elliptic curves with rank at least 3. However, we will show that the resulting family has rank 4. Motivated by some experimental data, we take $v = 0$, $r = s+t+1$ and insert (15) in (16). We get the quartic in s:

$$\begin{aligned}(12t^2+8t+4)s^4 &+ (12t^3+20t^2+12t+4)s^3 \\ + (13t^4+12t^3+10t^2+4t+1)s^2 &+ (8t^5+8t^4)s + 4t^6+8t^5+4t^4 = G^2.\end{aligned} \tag{17}$$

Since it contains the point $[0, 2t^3+2t^2]$, it can be transformed into the cubic:

$$\begin{aligned}&w^3 + (13t^4+12t^3+10t^2+4t+1)w^2 \\ &+(-96t^8 - 256t^6 - 256t^7 - 128t^5 - 32t^4)w \\ &-1152t^{12} - 3840t^{11} - 5504t^{10} - 4608t^9 - 2432t^8 - 768t^7 - 128t^6 = H^2.\end{aligned} \tag{18}$$

Note that the point $[4t^2(3t^2+2t+1), 4t^2(t-1)(3t+1)(3t^2+2t+1)]$ lies on (18). By transforming it back to the quartic (17), we get

$$s = -\frac{7t^3+9t^2+3t+1}{t^2+6t+3}.$$

Then we can easily compute:

$$\begin{aligned}
\tau =&\frac{(3t^2+6t+1)(5t^2+2t-1)}{4t(t-1)(3t+1)(t+1)},\\
\alpha =&-\frac{(t+1)(7t^2+2t+1)}{t(t^2+6t+3)},\\
a =&-\frac{(t+1)(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)}{t(11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)},\\
b =&\frac{t(11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)}{(t+1)(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)},\\
c =&\big(16(t-1)(3t+1)(t+1)t(t^2+6t+3)(3t^2+6t+1)\\
&(5t^2+2t-1)(7t^2+2t+1)\big)/\\
&((11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)\\
&(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)).
\end{aligned}$$

Now we claim that the induced elliptic curve

$$E: \quad y^2 = x^3 + A(t)x^2 + B(t)x,$$

where

$$\begin{aligned}
&A(t) =\\
&\quad 2(87671889t^{24}+854321688t^{23}+3766024692t^{22}+9923033928t^{21}\\
&\quad +17428851514t^{20}+21621621928t^{19}+19950275060t^{18}\\
&\quad +15200715960t^{17}+11789354375t^{16}+10470452464t^{15}+8925222696t^{14}\\
&\quad +5984900048t^{13}+2829340620t^{12}+820299856t^{11}+59930952t^{10}\\
&\quad -66320528t^{9}-35768977t^{8}-9381000t^{7}-1017244t^{6}+262760t^{5}\\
&\quad +159130t^{4}+41096t^{3}+6468t^{2}+600t+25),\\
&B(t) =\\
&\quad (t^2-2t-1)^2(69t^4+148t^3+78t^2+4t+1)^2(13t^2-2t-1)^2\\
&\quad \times(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\quad \times(9t^2+14t+7)^2(31t^4+52t^3+22t^2-4t-1)^2(3t^2+2t+1)^2,
\end{aligned}$$

has rank ≥ 4 over $\mathbb{Q}(t)$. Indeed, it contains the points whose x-coordinates are

$$\begin{aligned}
X_1 &= (9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\quad \times(69t^4+148t^3+78t^2+4t+1)^2,\\
X_2 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1)\\
&\quad \times(9t^4+28t^3+18t^2+4t+1)(11t^4+12t^3+2t^2-4t-1)^2\\
&\quad \times(31t^4+52t^3+22t^2-4t-1),\\
X_3 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1)\\
&\quad \times(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)\\
&\quad \times(69t^4+148t^3+78t^2+4t+1),\\
X_4 &= -(3t^2+2t+1)^2(9t^2+14t+7)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\quad \times(31t^4+52t^3+22t^2-4t-1)^2.
\end{aligned}$$

and a specialization, e.g. $t = 2$, shows that the four points P_1, P_2, P_3, P_4, having these x-coordinates, are independent points of infinite order. Thus we obtained an elliptic curve over the field of rational functions with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank ≥ 4.

This improves previous records (with rank ≥ 3) for curves with this torsion group, obtained by Lecacheux, Elkies and Eroshkin ([**?**, El2, Er]).

Moreover, since our curve has full 2-torsion, we can get more precise information by applying the algorithm by Gusić and Tadić [GT1, Theorem 3.1 and Corollary 3.2]. Using this algorithm we can show that $\operatorname{rank}(E(\mathbb{Q}(t))) = 4$ and that the four points P_1, P_2, P_3, P_4 are free generators of $E(\mathbb{Q}(t))$.

Details of the proofs can be seen in [DP1].

7. Examples of curves with high rank

7.1. **Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank 9 over $\mathbb{Q}$. The first example.** In this section, we are searching for particular elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and high rank. In [Du3], several such curves, induced by Diophantine triples, with rank 7 were presented. In the above notation, they correspond to $\alpha = 2$. Here we search for such curves with τ and α of the form (15).

We not only improve the result of [Du3], but by finding a curve of rank 9, we give the current record for all known elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Previous records with rank 8, due to Elkies, Eroshkin and Dujella ([El2, Er, Du4]), were found by different methods.

In our search in [DP1], we covered the range $|r| + |s| + |t| + |v| \leq 420$, while in [DP2] we searched also for parameters of special form outside this range. We use sieving methods, which include computing Mestre-Nagao sums Selmer rank and Mestre's conditional upper bound to locate good candidates for high rank, and then we compute the rank with `mwrank`. In that way, we found five curves with rank 8 in [DP1] and additional five curves with rank 8 in [DP3], corresponding to the parameters

$$
\begin{aligned}
&(r,s,t,v) = \\
&(20,-11,25,68),(82,9,73,30),(55,31,142,15),(91,55,33,104),(157,127,43,12)\\
&(131,-29,49,96),(186,-57,62,199),(107,107,149,430),(103,103,168,725),\\
&(749,749,138,245)
\end{aligned}
$$

(the details about these curves can be found on [Du1]). Finally, we find a curve with rank equal to 9, corresponding to the parameters $(r,s,t,v) = (155,54,96,106)$. The curve is induced by the Diophantine triple

$$\left\{ \frac{301273}{556614}, -\frac{556614}{301273}, -\frac{535707232}{290125899} \right\}.$$

The minimal Weierstrass form of the curve is

$$
\begin{aligned}
y^2 = x^3 + x^2 - 6141005737705911671519806644217969840x\\
+ 5857433177348803158586285785929631477808095171159063188.
\end{aligned}
$$

The torsion points and 9 independent points of infinite order can be found in [Du1].

7.2. **Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank 9 over $\mathbb{Q}$. The second example.** Here we give a different example with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank equal to 9. We follow the approach from Subsection 6.7, until the condition (14):

$$\tau^2 + \alpha^2 + 2 = \square.$$

By taking

$$\tau^2 + \alpha^2 + 2 = \Big(\frac{\tau^2+1}{\tau} + \Big(\alpha - \frac{1}{\tau}\Big)t\Big)^2,$$

we get

$$\alpha = \frac{-2\tau^2 t + 1 - 2t + t^2}{\tau(t^2-1)}.$$

Motivated by some experiments, we now take $\tau = 1/7$ as a possible good choice for obtaining curves with higher rank. An additional motivation for this choice comes when we write our curve in the form $y^2 = x^3 + Ax^2 + Bx$. Here B factorize as

$$B = 16(\tau^2t^2 - \tau^2 - 2\tau^2t + 1 - 2t + t^2)^2(\tau^2t - 1 + t)^2(\tau^2t^2 - \tau^2 + 2\tau^2t - 1 + 2t - t^2)^2t^2(\tau^2 + 1 - t)^2.$$

So we have 5 irreducible factors in B. But if we want more factors, we may choose τ in such a way that some of the factors factorizes, and this means that the discriminant is a square. The discriminant of $\tau^2t^2 - \tau^2 - 2\tau^2t + 1 - 2t + t^2$ and $\tau^2t^2 - \tau^2 + 2\tau^2t - 1 + 2t - t^2$ with the respect to t is $8\tau^2(\tau^2 + 1)$, which is a square e.g. for $\tau = 1/7$. For $\tau = 1/7$, B factorizes as

$$256/33232930569601(5t-4)^2(5t-6)^2(50t-49)^2(6t-5)^2(4t-5)^2t^2(-50+49t)^2,$$

so we have 7 factors instead of 5.

Now we perform a search for high rank curves by using similar sieving methods as in the previous subsection. We searched for $t = t_1/t_2$ in the range $\max(|t_1|, |t_2|) < 3000$. We found 7 examples with rank equal to 8, for $t = 201/170$, $245/138$, $-800/459$, $1610/1417$, $1955/1754$, $2254/2215$, $2301/1670$, and one example with rank equal to 9, for $t = 900/781$. The last curve is induced by the Diophantine triple

$$\left\{\frac{181800}{127673}, -\frac{127673}{181800}, -\frac{996869751703}{2072406375000}\right\}.$$

The minimal Weierstrass form of the curve is

$$y^2 + xy = x^3 - 144370584236849299130167544556987839128626 0x$$
$$+ 518524534126954116322153225511662398609137586525877978241619600.$$

The torsion points are

$$\mathcal{O}, [4052667835584573661 20, -2026333917792286830 60],$$
$$[9465075778048471261 20, -473253788902423563060],$$
$$[-5407097445453217968961/4, 5407097445453217968961/8],$$
$$[-16880580513176195868 0, -27521269452973351848551320510260],$$
$$[-168805805131761958680, 27521269453142157653683082468940],$$
$$[206182096074145621092 0, -79415869652391657291324304635060],$$
$$[2061820960741456210920, 79415869650329836330582848424140],$$

while independent points of infinite order are:

$$[1282231740033536797 20, 183170993684701177611994211729 40],$$
$$[956390935331148119400, 35457689142935553215501462724 60],$$
$$[10163771110240599961 20, 10055611157530821697614783806940],$$
$$[169782735399656768337 0, 54420111049349435946331048024440],$$
$$[5649594628848460496106 6, 1342543337846301929226360968940886 2],$$
$$[289704950331957158160, 11162008755000776928955192667940],$$
$$[10366818430963801401263229 6/625, 1055496671159222837902206275138714086956/15625],$$
$$[-1198812138771230215367 0/9, -238796691154542884537206928300120/27],$$
$$[-2653745756105826823863552 0/29929, -171844066225434189468646360371177721020/5177717].$$

Acknowledgements. The authors want to deeply thank to the anonymous referees for a careful reading of our paper and for valuable suggestions which improved the presentation.

References

[ACP] J. Aguirre, F. Castaneda, J. C, Peral, *High rank elliptic curves with torsion group* $\mathbb{Z}/(2\mathbb{Z})$, Math. of Computation, vol 73, number 245, (2003), 323–331.

[ADP] J. Aguirre, A. Dujella, J. C. Peral, *On the rank of elliptic curves coming from rational Diophantine triples*, Rocky Mountain J. Math., **42** (2012), 1759–1776.

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

[Ca] R. D. Carmichael, Diophantine Analysis, Dover, New York, 1959.

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

[Di] L. Dickson, History of the theory of numbers, Vol 2, Chelsea 1971.

[Du1] A. Dujella, *High rank elliptic curves with prescribed torsion,* `http://web.math.hr/~duje/tors/tors.html`.

[Du2] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328** (1996), 25–30.

[Du3] A. Dujella, *Diophantine m-tuples and elliptic curves*, J. Théor. Nombres Bordeaux **13** (2001), 111–124.

[Du4] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.

[DP1] 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,* LMS J. Comput. Math. **17** (2014), 282-288.

[DP2] A. Dujella and J. C. Peral, *Elliptic curves with torsion group* $\mathbb{Z}/8\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$*,* in: Trends in Number Theory, Contemp. Math. **649** (2015), 47–62.

[DP3] A. Dujella and J. C. Peral, *Elliptic curves induced by Diophantine triples,* Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **113** (2019), 791-806.

[El1] N. Elkies, *Three lectures on elliptic surfaces and curves of high rank,* `arXiv: 0709.2908v1` (2007)

[El2] N. D. Elkies, $E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}^8$, Number Theory Listserver, Jun 2005.

[Er] Y. G. Eroshkin, Personal communication, 2008.

[Fe] S. Fermigier, *Construction of high rank elliptic curves over* $\mathbb{Q}$ *and over* $\mathbb{Q}(t)$ *with non trivial* 2*-torsion,* in: Algorithmic Number Theory (Talence 1996), Springer, Berlin (1996)

[GT1] I. Gusić, P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III **47** (2012), 265-275.

[GT2] I. Gusić, P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137-152.

[K] S. Kubert *Universal bounds on the torsion of elliptic curves,* Proc. London Math, Soc., 3 (33) (1976), 193-237.

[Ka] S. Kamienny, *Torsion on elliptic curves and q-coefficients of modular forms,* Invent, Math., 109(2) (1992), 221-229.

[KSW] Z. Klagsbrun, T. Sherman, J. Weigandt, *The Elkies curve has rank* 28 *subject only to GRH*, Math. Comp. **88** (2019), 837-846.

[Ki1] S. Kihara, *On the rank of elliptic curves with a rational point of order* 4*,* Proc. Japan Acad. Ser A Math. Sci. **80** (2004), 26-27.

[Ki2] S. Kihara ,*On the rank of elliptic curves with a rational point of order* 4*, II,* Proc. Japan Acad. Ser A Math. Sci. **80** (2004), 158-159

[KM] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J. **109** , (1988), 125-149.

[Kn] A. Knapp, Elliptic curves, Princeton University Press, 1992.

[KhMo] F. Khoshnam, D. Moody, *High rank elliptic curves with torsion* $\mathbb{Z}/4\mathbb{Z}$) *induced by Kiharaś Elliptic curves,* Integers, **16** , *A*70, (2016), 1, 12.

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

[Le] O. Lecacheux, *Rang de courbes elliptiques dont le groupe de torsion est non trivial,* Ann. Sci. Math. Quebec **28** (2004), 145-151

[McL] A. MacLeod, *A simple method for Hihg-Rank Families of Elliptic Curves with specified torsion,* ArXiv: 1410.1662v1 [math. NT] (2014).

[Me1] J.F. Mestre, *Courbes elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(t)$*,* C. R. Acad. Sci. Paris. Sér. I Math. **313** (1991), 139-142.

[Me2] J.F. Mestre, *Rang de courbes elliptiques d´invariant donné,* C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), 919–922.

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

[Mo] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degree*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[PPVW] J. Park, B. Poonen, J. Voight and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), 2859-2903.

[Ra] P. Rabarison, *Structure de torsion des courbes elliptiques definies sur les corps de nombres quadratiques,* Acta Arithmetica **144** (2010), 17–52.

[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.

[Si] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

[We] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Mathematica **52** (1929), 281–315.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address, A. Dujella: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
Email address, J. C. Peral: juancarlos.peral@ehu.es