HIGH RANK ELLIPTIC CURVES WITH TORSION $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ INDUCED BY DIOPHANTINE TRIPLES

ANDREJ DUJELLA AND JUAN CARLOS PERAL

Abstract. We construct 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 equal to 4, and an elliptic curve over $\mathbb{Q}$ with the same torsion group and rank 9. Both results improve previous records for ranks of curves of this torsion group. They are obtained by considering elliptic curves induced by Diophantine triples.

1. Introduction

A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero integers (rationals) is called *a (rational) Diophantine m-tuple* if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. In this paper, we will consider elliptic curves of the form

$$y^2 = (ax+1)(bx+1)(cx+1), \tag{1}$$

where $\{a, b, c\}$ is a rational Diophantine triple. We say that the elliptic curve (1) is induced by the Diophantine triple $\{a, b, c\}$. By Mazur's theorem, there are at most four possibilities for the torsion group of such curves, namely, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and in [7] it was shown that all these torsion groups indeed appear. Questions about the ranks of elliptic curves induced by Diophantine triples have been considered in several papers. In [1], a parametric family of elliptic curves induced by Diophantine triples with rank 5, and an elliptic curve over $\mathbb{Q}$ with rank 11 were constructed (improving previous similar results from [6, 7]). These curves have torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Curves with larger torsion were studied in [7]. In particular, it was shown that every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by a Diophantine triple, see also [2].

In this paper, we study elliptic curves induced by Diophantine triples, with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In [7], such curves with rank $r = 0, 1, \ldots, 7$ were constructed. Our purpose is not just to improve that result, but also to obtain elliptic curves over $\mathbb{Q}$ and over the field of rational functions $\mathbb{Q}(t)$ with the largest known rank. The previous records were rank 8 over $\mathbb{Q}$, due to Elkies, Eroshkin and Dujella [10, 12], and rank ≥ 3 over $\mathbb{Q}(t)$, due to Lecacheux, Elkies and Eroshkin [16, 11, 12].

We find new examples of such curves over $\mathbb{Q}$ with rank 8 and one example with rank 9. Also, we construct a parametric family of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and with rank ≥ 4. Moreover, we prove that its generic rank is equal to 4 and find the generators of the Mordell-Weil group.

2. Rank 4 family

We consider elliptic curves with the torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. It follows from the 2-descent proposition [15, 4.2, p.85], that all such curves have

---

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.

equations of the form

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

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 (1) leads to the elliptic curve $y^2 = (x + ab)(x + ac)(x + bc)$ in the Weierstrass form, and by translation we obtain the equation

$$y^2 = x(x + ac - ab)(x + bc - ab). \tag{3}$$

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 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 we require $ac - ab = ac + 1 = p^2$ and $bc - ab = bc + 1 = q^2$. It remains to find c such that$\{a, -1/a, c\}$ is a Diophantine triple. We get the system

$$ac + 1 = \square, \quad -\frac{c}{a} + 1 = \square. \tag{4}$$

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

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

which has the parametric solution of the form

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

Inserting this in (3), after some simplifications, we get

$$y^2 = x^3 + 2(\alpha^2 + \tau^2 + 4\alpha^2\tau^2 + \alpha^4\tau^2 + \alpha^2\tau^4)x^2 + (\tau + \alpha)^2(\alpha\tau - 1)^2(\tau - \alpha)^2(\alpha\tau + 1)^2x. \tag{5}$$

Up the this point, we followed closely the approach from [7]. Now we force $x = (\tau + \alpha)^2(\alpha\tau - 1)(\alpha\tau + 1)$ to satisfy the equation (5), and we get the condition

$$\tau^2 + \alpha^2 + 2 = \square. \tag{6}$$

By [3, §10], the solution of (6) is given by

$$\tau = \frac{r^2 - s^2 - 2t^2 + 2v^2}{2(rt + sv)}, \quad \alpha = \frac{rs - 2tv}{rt + sv}. \tag{7}$$

On the other hand, by forcing $x = (\tau + \alpha)(\alpha\tau - 1)^2(\tau - \alpha)$ to satisfy (5), we get the condition

$$\alpha^2\tau^2 + 2\alpha^2 + 1 = \square. \tag{8}$$

We seek a parametric solution of the system (6) and (8). 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 (7) in (8). We get the quartic in s:

$$\begin{aligned}(12t^2 + 8t + 4)s^4 &+ (12t^3 + 20t^2 + 12t + 4)s^3 \\ + (13t^4 + 12t^3 + 10t^2 + 4t + 1)s^2 &+ (8t^5 + 8t^4)s + 4t^6 + 8t^5 + 4t^4 = g^2.\end{aligned} \tag{9}$$

Since it contains the point $[0, 2t^3 + 2t^2]$, it can be transformed into the cubic over $\mathbb{Q}(t)$ given by:

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

For explicit transformations see e.g. [4, Section 2.1]. By checking factors of $1152t^{12}+3840t^{11}+5504t^{10}+4608t^9+2432t^8+768t^7+128t^6 = 128t^6(t+1)^2(3t^2+2t+1)^2$ as possible w-coordinates of points on (10), we find that the point $[4t^2(3t^2+2t+1), 4t^2(t-1)(3t+1)(3t^2+2t+1)]$ lies on (10). By transforming it back to the quartic (9), 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 points whose x-coordinates are

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

Note that the point X_4 corresponds to the point $[-1,-c]$ on the curve (3). Other points were found by searching for points on E with x-coordinates which are divisors of the polynomial $B(t)$. A specialization, e.g. $t=2$, shows that the four points P_1,P_2,P_3,P_4, having x-coordinates X_1,X_2,X_3,X_4, are independent points of infinite order. Thus we obtain 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 [16, 11, 12]. Moreover, since our curve has full 2-torsion, we can get more precise information by applying the algorithm by Gusić and Tadić [13, Theorem 3.1 and Corollary 3.2], see also [14]. 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 $E(\mathbb{Q}(t))$. We will sketch the application of this algorithm (for a detailed example of such application see e.g. [9]). To apply the algorithm, we write E in the form

$$y^2=(x-e_1)(x-e_2)(x-e_3),$$

with $e_1,e_2,e_3\in\mathbb{Z}[t]$, and consider the factorization

$$(e_1-e_2)\cdot(e_1-e_3)\cdot(e_2-e_3)=\beta\cdot f_1^{\alpha_1}(t)\cdots f_l^{\alpha_l}(t),$$

where $\beta\in\mathbb{Z}$ and $f_i\in\mathbb{Z}[t]$ are irreducible (of positive degree) and $\alpha_i\geq 1$. Let $t_0\in\mathbb{Q}$. Assume that for each $i=1,\dots,l$ the square-free part of each of $f_i(t_0)$ has at least one prime factor that does not appear in the square-free part of any of $f_j(t_0)$ for $j\neq i$ and does not appear in the factorization of β. Then the specialization homomorphism $E(\mathbb{Q}(t))\to E(t_0)(\mathbb{Q})$ is injective [13, Theorem 3.1]. Furthermore, if $|E(t_0)(\mathbb{Q})_{\text{tors}}|=8$ and there exist points $Q_1,\dots,Q_r\in E(\mathbb{Q}(t))$ such that $Q_1(t_0),\dots,Q_r(t_0)$ are the free generators of $E(t_0)(\mathbb{Q})$, then the specialization homomorphism $E(\mathbb{Q}(t))\to E(t_0)(\mathbb{Q})$ is an isomorphism. Thus $E(\mathbb{Q}(t))$ and $E(t_0)(\mathbb{Q})$ have the same rank r, and $Q_1,\dots,Q_r$ are the free generators of $E(\mathbb{Q}(t))$ [13, Corollary 3.2]. In our case,

$$
\begin{aligned}
&(e_1-e_2)(e_1-e_3)(e_2-e_3)=\\
&-16(13t^2-2t-1)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\times (9t^4+28t^3+18t^2+4t+1)^2(9t^2+14t+7)^2(t^2-2t-1)^2\\
&\times (69t^4+148t^3+78t^2+4t+1)^2(31t^4+52t^3+22t^2-4t-1)^2\\
&\times (3t^2+2t+1)^2(t-1)(3t+1)(2t^2+2t+1)\\
&\times (t^2+6t+3)(3t^2+6t+1)(5t^2+2t-1)\\
&\times (41t^4+76t^3+50t^2+12t+1)(9t^4+12t^3+2t^2-4t+1)\\
&\times (7t^2+2t+1)(25t^4+44t^3+26t^2+4t+1),
\end{aligned}
$$

thus we have $\beta = -16$ and $l = 18$. If we take $t_0 = 15$, then it is easy to check that the conditions of [13, Theorem 3.1], given above, are satisfied. Using `mwrank` [5], we compute that $\operatorname{rank}(E(15)(\mathbb{Q})) = 4$. Hence, we have proved that

$$\operatorname{rank}(E(\mathbb{Q}(t))) = 4.$$

Moreover, `mwrank` is able to find free generators, R_1, R_2, R_3, R_4, of $E(15)(\mathbb{Q})$. If we express $P_1(15), P_2(15), P_3(15), P_4(15)$ in the basis R_1, R_2, R_3, R_4 (modulo torsion), we get that the transformation matrix has determinant equal to -1. Thus we get that $P_1(15), P_2(15), P_3(15), P_4(15)$ also represent a full basis for $E(15)(\mathbb{Q})$. Finally, by [13, Corollary 3.2], we conclude that P_1, P_2, P_3, P_4 are free generators of $E(\mathbb{Q}(t))$.

3. Examples of curves with high rank

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 [7], several such curves, induced by Diophantine triples, with rank 7 were presented. In the above notation, they correspond to $\alpha = 2$. Here we will search for such curves with τ and α of the form (7).

We will not only improve the result of [7], but by finding a curve of rank 9, we will 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 [10, 12], were found by different methods. In our search, we cover the range $|r|+|s|+|t|+|v| \leq 420$. We use sieving methods, which include computing Mestre-Nagao sums [18], Selmer rank (as implemented in `mwrank` [5]) and Mestre's conditional upper bound [17], to locate good candidates for high rank, and then we compute the rank with `mwrank`. In that way, we find five curves with rank 8, corresponding to the parameters

$$\begin{aligned}&(r, s, t, v) = \\ &(20, -11, 25, 68), (82, 9, 73, 30), (55, 31, 142, 15), (91, 55, 33, 104), (157, 127, 43, 12).\end{aligned}$$

Details about these curves can be found on [8]. 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

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

The torsion points are:

$$\begin{gathered} \mathcal{O}, [-2861469472720778854, 0], \\ [1431017969855150171, 0], [1430451502865628682, 0], \\ [1381707195787460036, -1009900105916671297534506 30], \\ [1381707195787460036, 1009900105916671297534506 30], \\ [1480328743922840306, -1033372593557069729400637 20], \\ [1480328743922840306, 1033372593557069729400637 20], \end{gathered}$$

while independent points of infinite order are:

$$[-612695149795875652, 30643098243490773810273083 58],$$
$$[-431590874944672564, 290300576808387310415885943 0],$$
$$[187501554154394546, 217084707389741539483235100 0],$$
$$[-1383500708967173302, 342131494316383377456791740 8],$$
$$[142851904723904 9546, 455154912002177913754800 0],$$
$$[1430248713837731282, 818226000869154831593640],$$
$$[1429305792931194266, 290121252299275548355776 0],$$
$$[103900694057898826, 228484136512456207908720624 0],$$
$$[1429854291102331316, 172693650476720317571991 0].$$

The same curve can be obtained by the parameters $(r, s, t, v) = (82, -19, 87, 14)$, i.e. it is induced also the by the Diophantine triple

$$\left\{-\frac{126555}{2686}, \frac{2686}{126555}, -\frac{9107022944}{249946125}\right\}.$$

Acknowledgement. The authors would like to thank Filip Najman, Petra Tadić and the anonymous referee for useful comments on the previous version of this paper.

References

[1] 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.
[2] G. Campbell, E. H. Goins, *Heron triangles, Diophantine problems and elliptic curves*, preprint, `http://www.swarthmore.edu/NatSci/gcampbe1/papers/heron-Campbell-Goins.pdf`
[3] R. D. Carmichael, Diophantine Analysis, Dover, New York, 1959.
[4] I. Connell, Elliptic Curve Handbook, McGill University, 1999.
[5] J. Cremona, Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge, 1997.
[6] A. Dujella, *Diophantine triples and construction of high-rank elliptic curves over $\mathbb{Q}$ with three non-trivial 2-torsion points*, Rocky Mountain J. Math. **30** (2000), 157–164.
[7] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.
[8] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.pmf.unizg.hr/~duje/tors/tors.html`
[9] A. Dujella, J. C. Peral, *Elliptic curves coming from Heron tringles*, Rocky Mountain J. Math., to appear.
[10] 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.
[11] N. D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, Lecture notes, Oberwolfach, 2007, `arXiv:0709.2908`.
[12] Y. G. Eroshkin, Personal communication, 2008.
[13] I. Gusić, P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III **47** (2012), 265–275.
[14] I. Gusić, P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, preprint, `arXiv:1211.3851`.
[15] A. Knapp, Elliptic Curves, Princeton Univ. Press, 1992.
[16] O. Lecacheux, *Rang de courbes elliptiques avec groupe de torsion non trivial*, J. Théor. Nombres Bordeaux **15** (2003), 231–247.
[17] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.
[18] K. Nagao, *An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 291–293.
[19] PARI/GP, version 2.4.0, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr`.
[20] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1994.

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