THE RANK AND GENERATORS OF KIHARA’S ELLIPTIC CURVE WITH TORSION $\mathbb{Z}/4\mathbb{Z}$ OVER $\mathbb{Q}(t)$

ANDREJ DUJELLA, IVICA GUSIĆ AND PETRA TADIĆ

ABSTRACT. For the elliptic curve $E$ over $\mathbb{Q}(t)$ found by Kihara, with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank $\geq 5$, which is the current record for the rank of such curves, by using a suitable injective specialization, we determine exactly the rank and generators of $E(\mathbb{Q}(t))$.

1. Introduction

By Mazur’s theorem, we know that the torsion group of an elliptic curve over $\mathbb{Q}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. The same 15 groups appear as possible torsion groups for elliptic curves over the field of rational functions $\mathbb{Q}(t)$. The current records for the rank of elliptic curves over $\mathbb{Q}(t)$ with prescribed torsion group can be found in the table [3]. Note that in this table for the most of torsion groups only the lower bounds for the rank of record curves are given. Indeed, it seems that only for the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ the exact rank over $\mathbb{Q}(t)$ of the record curve can be found in literature. In fact, in [5], Dujella and Peral proved that the corresponding curve, obtained from the so-called Diophantine triples, has rank equal to 4 and they provide the generators for the group. The proof uses the method introduced by Gusić and Tadić in [6] for an efficient search for injective specializations. In this paper, we will prove an analogous result for the curve with record rank over $\mathbb{Q}(t)$ with torsion group $\mathbb{Z}/4\mathbb{Z}$ found by Kihara [9] (see Theorem 2.1). Here we will use results from the recent paper [7], where the authors generalize and extend their method from [6]. In particular, by results of [7], now the method can be applied to curves with only one rational 2-torsion point.

Our main tool is [7, Theorem 1.3]. It deals with elliptic curves $E$ given by $y^2 = x^3 + A(t)x^2 + B(t)x$, where $A, B \in \mathbb{Z}[t]$, with exactly one nontrivial 2-torsion point over $\mathbb{Q}(t)$. If $t_0 \in \mathbb{Q}$ satisfies the condition that for every
nonconstant square-free divisor \( h \) of \( B(t) \) or \( A(t)^2 - 4B(t) \) in \( \mathbb{Z}[t] \) the rational number \( h(t_0) \) is not a square in \( \mathbb{Q} \), then the specialized curve \( E_{t_0} \) is elliptic and the specialization homomorphism at \( t_0 \) is injective. If additionally there exist \( P_1, \ldots, P_r \in E(\mathbb{Q}(t)) \) such that \( P_1(t_0), \ldots, P_r(t_0) \) are the free generators of \( E(t_0)(\mathbb{Q}) \), then \( E(\mathbb{Q}(t)) \) and \( E(t_0)(\mathbb{Q}) \) have the same rank \( r \), and \( P_1, \ldots, P_r \) are the free generators of \( E(\mathbb{Q}(t)) \).

We can mention here that by the methods from [7], it is easy to show that the general families of curves with torsion \( \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) given in Kubert’s paper [10] all have rank 0 over \( \mathbb{Q} \), as expected from the corresponding entries in the above table (see Remark 3.1).

2. Kihara’s curve with rank \( \geq 5 \)

In 2004, Kihara [9] constructed a curve over \( \mathbb{Q}(t) \) with torsion group \( \mathbb{Z}/4\mathbb{Z} \) and rank \( \geq 5 \). This improved his previous result [8] with rank \( \geq 4 \). We briefly describe Kihara’s construction. The quartic curve \( H \) given by the equation

\[
(x^2 - y^2)^2 + 2a(x^2 + y^2) + b = 0
\]

is considered. Forcing five points with coordinates of the form \((r, s), (r, u), (s, p), (u, q), (p, m)\) to satisfy (2.1) leads to a system of certain quadratic Diophantine equations, for which a parametric solution is found. By the transformation \( X = (a^2 - b)y^2/x^2 \) and \( Y = (a^2 - b)y(b + ax^2 + ay^2)/x^3 \), we get from \( H \) the elliptic curve \( E \) with equation

\[
Y^2 = X(X^2 + (2a^2 + 2b)X + (a^2 - b)^2).
\]

We can write (2.2) in the form

\[
Y^2 = X^3 + A(t)X^2 + B(t)X,
\]
where

\[ A(t) = 4 \cdot (6561t^{52} - 363636t^{51} + 9938430t^{50} - 17337920t^{49} + 2093381633t^{48} - 17874840696t^{47} + 104874633374t^{46} - 354077727932t^{45} - 225490507368t^{44} + 1142693538256t^{43} - 77979654468618t^{42} + 278213963503072t^{41} - 11125386611731t^{40} - 601867684563976t^{39} + 5043730228698390t^{38} - 272612407880904180t^{37} + 1164419469986139655t^{36} - 4197430502686137512t^{35} + 13172874796371804t^{34} - 36632311181492128960t^{33} + 9127072648658186066t^{32} - 205234200473064086512t^{31} + 41856594958882731196t^{30} - 776853016569799513688 * t^{29} + 131519360741156944924t^{28} - 2034605787348730781688t^{27} + 2881061692467531957312t^{26} - 3743290609966430672640t^{25} + 4481632889126213095506t^{24} - 4982866114496291088464t^{23} + 5212858449376876320156t^{22} - 5228984497845291579880t^{21} + 51336832788660716535t^{20} - 499373054378193438052t^{19} + 47844994223644389062t^{18} - 440888972356409443776t^{17} + 378417447854465465655t^{16} - 2930449238068167436056t^{15} + 1987364904374352466086t^{14} - 1143489371242947035052t^{13} + 534571453903095183576t^{12} - 18722208177806813708t^{11} + 38190501318649624878t^{10} + 3640463051927237920t^{9} - 66122105306224758398 + 2873353737226558120t^{7} - 748108460242930642t^{6} + 127972510817241756t^{5} - 14371540294374703t^{4} + 1013310571582176t^{3} - 40376902667904t^{2} + 671143753728t + 2176782336),

\[ B(t) = 256t^2(t - 1)^4(t + 1)^4(t - 3)^2(t - 5)^2(3t - 1)^2(t - 2)^4(t^2 + 2t - 2t + 3)^2 \times (t^2 + 2t + 1)^2(7t^2 - 18t + 23)^2(3t^2 - 2t + 7)^2(3t^2 + 4t^2 - 5t + 16)^2 \times (3t^4 - 17t^3 + 27t^2 - 43t + 6)^2(2t^4 - 7t^3 + 9t^2 - 11t - 5)^2(2t^4 - 17t^3 + 27t^2 - 25t + 1)^2 \times (t^4 - 4t^3 + 6t^2 - 12t + 1)^2(5t^4 - 17t^3 + 27t^2 - 79t + 16)^2(t^4 - 28t^3 + 54t^2 - 92t + 41)^2 \times (t^4 - 9t^3 + 15t^2 - 19t + 4)^2.\]
Here we give also the factorization of $A(t)^2 - 4B(t)$ because it is essential for the proof of Theorem 2.1.

$$A(t)^2 - 4B(t) = 16(6561t^{52} - 393876t^{51} + 12044286t^{50} - 233179992t^{49} + 3037888017t^{48} - 27010254024t^{47} + 156557186174t^{46} - 431368937388t^{45} - 1778897440520t^{44} + 29118669267908t^{43} - 185554409423562t^{42} + 692712486737480t^{41} - 814770507947971t^{40} - 9637269870935344t^{39} + 91712999355372182t^{38} - 511726240316396532t^{37} + 220921056425660999t^{36} - 7976932199520997736t^{35} + 2493402585224375740t^{34} - 68753516109041894560t^{33} + 168954992642195397618t^{32} - 372775248087820281744t^{31} + 740995668471372699516t^{30} - 1328945941188034678776t^{29} + 214926880379326882800t^{28} - 3126651933116879854968t^{27} + 4072542345072750657372t^{26} - 4716734217685402094832t^{25} + 481438309685780538790t^{24} - 42966099977077762663152t^{23} + 3376161521034367049052t^{22} - 2507937390234783793960t^{21} + 21753897461766376920t^{20} - 2602425451380388744228t^{19} + 3581059482295238331078t^{18} - 456063505415834637368t^{17} + 496691184338971545574t^{16} - 4539431424438631575336t^{15} + 3452812241784521490182t^{14} - 21550049860560689396t^{13} + 107100328670667643616t^{12} - 395973787910697589516t^{11} + 87894481825369263726t^{10} + 4136860927499429288t^{9} - 12949727214730449839t^{8} + 587322103481598669t^{7} - 1551776386124274418t^{6} + 266291310738984156t^{5} - 2971860649281967t^{4} + 2058088618943172t^{3} - 79201521880704t^{2} + 1255157987328t + 2176782336)$$

\[\times (81t^{20} - 2058t^{25} + 22205t^{24} - 13691t^{23} + 569600t^{22} - 1941994t^{21} + 7144777t^{20} - 31865642t^{19} + 143465455t^{18} - 557913380t^{17} + 1796620282t^{16} - 4792045284t^{15} + 10672893440t^{14} - 19973820452t^{13} + 31471575770t^{12} - 41625786276t^{11} + 45790269127t^{10} - 41147326466t^{9} + 29240715721t^{8} - 15417678410t^{7} + 5182080208t^{6} - 45922934t^{5} - 434078947t^{4} + 182700750t^{3} - 25979095t^{2} + 933744t + 46656).\]

Kihara in [9] found five independent points $P_1, \ldots, P_5$ on this curve, corresponding to the five points on $H$ mentioned above, showing that the rank of $E$ over $\mathbb{Q}(t)$ is $\geq 5$. The torsion subgroup is $\mathbb{Z}/4\mathbb{Z}$. Indeed, the point $T_1 = (a^2 - b, 2a(a^2 - b))$ on (2.2) is of order 4 since $2T_1 = (0, 0)$ and $4T_1 = \mathcal{O}$. Furthermore, from the factorizations of $B(t)$ and $A(t)^2 - 4B(t)$ we see that $T_1 \not\in 2E(\mathbb{Q}(t))$ and that $E(\mathbb{Q}(t))$ has exactly one point of order 2. An alternative proof of this fact will be given in Section 3.

Our goal is to prove that the rank of $E$ over $\mathbb{Q}(t)$ is exactly equal to 5 and to find the generators of $E(\mathbb{Q}(t))$. Computations with several specializations indicate that $P_1, P_2, P_3, P_4, P_5$ are not generators of $E(\mathbb{Q}(t))$. Indeed, from our results it will follow that they generate a subgroup of index 64 in $E(\mathbb{Q}(t))$.

In fact, it holds that $P_i + P_i \in 2E(\mathbb{Q}(t))$ for $i = 2, 3, 4, 5$, i.e. there exist points $W_2, W_3, W_4, W_5$ of $E(\mathbb{Q}(t))$ such that $P_i + P_i = 2W_i$, $i = 2, 3, 4, 5$. Since the torsion subgroup is $\mathbb{Z}/4\mathbb{Z}$, there are two choices for each $W_i$. We choose
one of them. The $x$-coordinates of these points are

\[
x(W_2) = 4(t - 3)(3t - 1)(t^2 + 2)(t^4 - 4t^3 + 6t^2 - 12t + 1)(3t^4 - 17t^3 + 27t^2 - 43t + 6)
\]
\[
\times (t^4 - 9t^3 + 15t^2 - 19t + 4)(7t^2 - 18t + 23)(t^4 - 28t^3 + 54t^2 - 92t + 41)(t - 2)^2
\]
\[
\times (9t^{12} - 110t^{11} + 576t^{10} - 2333t^9 + 7802t^8 - 19832t^7 + 39488t^6 - 57374t^5
\]
\[
+ 61421t^4 - 42914t^3 + 16488t^2 - 701t - 216)(t + 1)^4,
\]
\[
x(W_3) = -16(t - 1)^3(t + 1)^3(t^2 + 2)(t^2 + 6t - 1)(t^3 + 4t^2 - 5t + 16)
\]
\[
\times (t^4 - 9t^3 + 15t^2 - 19t + 4)(2t^4 - 17t^3 + 27t^2 - 25t + 1)(3t^4 - 17t^3 + 27t^2 - 43t + 6)
\]
\[
\times (3t^2 - 2t + 7)(t - 2)^2(t^2 - 5)^2(t^4 - 28t^3 + 54t^2 - 92t + 41)^2
\]
\[
\times (2t^4 - 7t^3 + 9t^2 - 11t - 5)^2,
\]
\[
x(W_4) = 16(t - 1)^3(t - 1)(3t - 1)(t^2 + 2)(t^2 + 6t - 1)(t^3 + 4t^2 - 5t + 16)
\]
\[
\times (3t^4 - 17t^3 + 43t^2 + 19t + 4)(t^4 - 9t^3 + 15t^2 - 19t + 4)(2t^4 - 17t^3 + 27t^2 - 25t + 1)
\]
\[
\times (3t^2 - 2t + 7)(t - 2)^2(t - 5)^2(7t^2 - 18t + 23)^2(t^4 - 4t^3 + 6t^2 - 12t + 1)^2
\]
\[
\times (2t^4 - 7t^3 + 9t^2 - 11t - 5)^2(3t^2 - 2t + 7)^2(t^4 - 28t^3 + 54t^2 - 92t + 41)^2
\]
\[
\times (8 - 55t - 29t^2 + 103t^3 - 120t^4 + 69t^5 - 27t^6 + 3t^7)^2,
\]
\[
x(W_5) = 16(t - 1)^3(t - 2)^3(t - 3)^2(t^2 + 2)(t^2 - 2t + 7)^2(3t^2 - 2t + 7)^2(t^3 + 4t^2 - 5t + 16)^2
\]
\[
\times (t^4 - 28t^3 + 54t^2 - 92t + 41)(t^4 - 4t^3 + 6t^2 - 12t + 1)(3t^4 - 17t^3 + 27t^2 - 43t + 6)
\]
\[
\times (t^4 - 9t^3 + 15t^2 - 19t + 4)(5t^4 - 17t^3 + 27t^2 - 79t + 16)(t^4 - 17t^3 + 27t^2 - 25t + 1)
\]
\[
\times (t^2 + 6t - 1)(t - 5)(3t - 1)(t + 1)t.
\]

We also give the $x$-coordinate of $P_1$:

\[
x(P_1) = 16(t - 2)^2(t - 3)(t - 5)(3t - 1)(t^2 + 2)(3t^2 - 2t + 7)(7t^2 - 18t + 23)
\]
\[
\times (t^2 + 6t - 1)(t^3 + 4t^2 - 5t + 16)(2t^4 - 17t^3 + 27t^2 - 25t + 1)
\]
\[
\times (2t^4 - 7t^3 + 9t^2 - 11t - 5)(3t^4 - 17t^3 + 27t^2 - 43t + 6)(t^4 - 4t^3 + 6t^2 - 12t + 1)
\]
\[
\times (t^2 - 2t + 3)(5t^4 - 17t^3 + 27t^2 - 79t + 16)(t^4 - 9t^3 + 15t^2 - 19t + 4)
\]
\[
\times (t^4 - 28t^3 + 54t^2 - 92t + 41)(3t^{13} - 128t^{12} + 1185t^{11} - 5018t^{10} + 136289 - 27704t^8
\]
\[
+ 44162t^7 - 63956t^6 + 84827t^5 - 100976t^4 + 92061t^3 - 52802t^2 + 10662t - 552)^2/
\]
\[
(12t^{11} - 219t^{10} + 1699t^9 - 7248t^8 + 21004t^7 - 45434t^6 + 72862t^5 - 90128t^4
\]
\[
+ 77496t^3 - 46283t^2 + 10095t - 768)^2.
\]

The points $P_1, W_2, \ldots, W_5$ are a natural guess for the generators, and we will show that this is indeed true by proving the following theorem in the next section.

**Theorem 2.1.** The elliptic curve $E$ over $\mathbb{Q}(t)$ has rank equal to 5 with free generators the points $P_1, W_2, W_3, W_4, W_5$ and the torsion group is $\mathbb{Z}/4\mathbb{Z}$. 
3. An injective specialization

As described in the introduction, we use [7, Theorem 1.3] to find rational numbers $t_0$ for which the specialization map at $t_0$ is injective. The condition is that for each nonconstant square-free divisor $h$ of $B(t)$ or $A(t)^2 - 4B(t)$ in $\mathbb{Z}[t]$ the rational number $h(t_0)$ is not a square in $\mathbb{Q}$. The condition is easy to check, and we can find many rationals $t_0$ satisfying it. However, the coefficients of the curve $E$ are polynomials with large degrees and coefficients. Thus, for the success of our approach, it is crucial to find suitable specialization $t_0$ of reasonably small height. Furthermore, we need a specialization for which the rank of $E_{t_0}$ over $\mathbb{Q}$ is equal to 5, so it is reasonable to consider only specializations for which the the root number of $E_{t_0}$ is $-1$ (conjecturally implying that the rank is odd).

We find that the specialization at $t_0 = -\frac{11}{4}$ satisfies all requirements, see preceding section for the factorization of $B(t)$ and $A(t)^2 - 4B(t)$. It remains to compute the rank and generators of $E_{-11/4}$. For that purpose, we use the excellent program [2] of Cremona, which is included in the program package Sage [13]. By extending significantly the default precision (we use options $\text{p 800 -b 11}$), we get the elliptic curve $E_{-11/4}$ over $\mathbb{Q}$, given by the equation

$$
y^2 = x^3 + 484371205173916954475505177386303655600428018856419825361x^2 + 199107945503532544541442922607063711556495848199368164800^2 x,
$$

which is of rank 5 with five free generators $G_1, \ldots, G_5$ and the generator of the torsion group $T_0$, given by their $x$-coordinates

$$
\begin{align*}
x(T_0) &= -199107945503532544541442922607063711556495848199368164800, \\
x(G_1) &= 35128929795293330966584382924686967322464932483259844000000, \\
x(G_2) &= -\frac{1331589544443896979015060618015468433326765676888020035648633838098791000259350993560000}{76159758997263590677307690401}, \\
x(G_3) &= -\frac{5369366852482550282341688034606137477987482678373004839681994240}{1416844881}, \\
x(G_4) &= \frac{47761687809406977974534416082366648044181684476555895981133946800}{9223369}, \\
x(G_5) &= \frac{72794607048562741902495446990852196447100359265007972065657045989202204731022849600}{13386309077372650899951050449}.
\end{align*}
$$

The rank 5 and generators are also confirmed in the most recent version V2.20-10 of Magma [1] (by the function \texttt{MordellWeilShaInformation} with option \texttt{SetClassGroupBounds("GRH")}). Now denote by $P^*_1, W^*_2, \ldots, W^*_5$ the points
obtained from $P_1, W_2, \ldots, W_5$ after specialization $t \mapsto -\frac{11}{4}$. We easily get that
\begin{align*}
P_1^* &= T_0 + G_5, \\
W_2^* &= T_0 - G_3 + G_4, \\
W_3^* &= T_0 + G_1 + G_2 - G_3 + G_4 - G_5, \\
W_4^* &= T_0 - G_2 + G_3 - G_4 + G_5, \\
W_5^* &= T_0 + G_4.
\end{align*}
Here all points are chosen up to sign of $y$-coordinates. It is easy to check that
the matrix of this base change (modulo torsion) is of determinant $\pm 1$ (the signs
of the determinant depends on the choice of the signs of $y$-coordinates), so we
see that $P_1^*, W_2^*, \ldots, W_5^*$ are free generators of the elliptic curve $E_{-11/4}$ over $\mathbb{Q}$.

From the comments at the end of the introduction, we see that [7, Theorem 1.3] now implies that $E$ has rank 5 over $\mathbb{Q}(t)$ and that $P_1, W_2, W_3, W_4, W_5$ are its free generators. Since $E$ has a point of fourth order and the torsion group of $E_{-11/4}(\mathbb{Q})$ is $\mathbb{Z}/4\mathbb{Z}$, we conclude that the torsion group of $E(\mathbb{Q}(t))$ is also $\mathbb{Z}/4\mathbb{Z}$.

Remark 3.1. Here we prove that the elliptic curves with torsion $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and with rank $\geq 0$ listed in Kubert’s paper [10] have rank equal to 0 over $\mathbb{Q}(t)$.

For torsion group $\mathbb{Z}/10\mathbb{Z}$, the curve is given by the equation
\[
y^2 = x(x^2 - (2t^2 - 2t + 1)(4t^4 - 12t^3 + 6t^2 + 2t - 1)x + 16t^5(t - 1)^5(t^2 - 3t + 1)).
\]
The specialization for $t_0 = 6$ satisfies the condition of [7, Theorem 1.3], and the specialized elliptic curve has rank 0, which proves our claim for that torsion group.

For torsion group $\mathbb{Z}/12\mathbb{Z}$, the curve is
\[
y^2 = x(x^2 + (t^8 - 12t^6 - 48t^5 - 162t^4 - 480t^3 - 540t^2 - 624t - 183)x + 1024(t^2 + 3)^2(t + 1)^6),
\]
and the specialization which satisfies the condition of [7, Theorem 1.3] and has rank 0 is $t_0 = 11$.

Finally, for torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, we have the curve
\[
y^2 = x(x + (t^2 - 1)^4)(x + 16t^4).
\]
The specialization for $t_0 = 6$ satisfies the condition of [7, Theorem 1.1], and the specialized elliptic curve has rank 0, which proves our claim in that case.

Remark 3.2. An alternative method for computing the rank of an elliptic curves over $\mathbb{Q}(t)$ (and over $\mathbb{C}(t)$) is to use theory of Mordell-Weil lattices, in particular the Shioda-Tate formula [12]. This method does not require that the curve has nontrivial 2-torsion and it is very efficient if the corresponding surface is rational or K3 surface (see e.g. [4, 11, 14]).
References


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

(Ivica Gusić) Faculty of Chemical Engin. and Techn., University of Zagreb, Marulićev trg 19, 10000 Zagreb, Croatia
E-mail address, Ivica Gusić: igusic@fkit.hr

(Petra Tadić) Department of Economics and Tourism, Juraj Dobrila University of Pula, 52100 Pula, Croatia
E-mail address, Petra Tadić: ptadic@unipu.hr