Iranian Journal of Mathematical Sciences and Informatics
Vol. 12, No. 1 (2017), pp 27-34
DOI: 10.7508/ijmsi.2017.01.003

A Note on Twists of $y^2 = x^3 + 1$

Farzali Izadi[a], Arman Shamsi Zargar[b,*]

[a]Department of Mathematics, Faculty of Science, Urmia University, Urmia 165-57153, Iran.
[b]Department of Pure Mathematics, Faculty of Basic Science, Azarbaijan Shahid Madani University, Tabriz 53751-71379, Iran.

E-mail: f.izadi@urmia.ac.ir
E-mail: shzargar.arman@azaruniv.edu

Abstract. In the category of Mordell curves $E_D : y^2 = x^3 + D$ with nontrivial torsion groups we find curves of the generic rank two as quadratic twists of E_1, and of the generic rank at least two and at least three as cubic twists of E_1. Previous work, in the category of Mordell curves with trivial torsion groups, has found infinitely many elliptic curves with rank at least seven as sextic twists of E_1 [4].

Keywords: Elliptic curve, Mordell curve, (Mordell-Weil) rank, Twist.

2000 Mathematics subject classification: 14H52.

1. Introduction

Let us consider the elliptic curve E_k defined over $\mathbb{Q}$ by the equation

$$y^2 = x^3 + k. \tag{1.1}$$

The elliptic curve (1.1) with an integer k is known as Mordell curve in the literature. (Throughout the paper, all curves and their points are assumed to be $\mathbb{Q}$-rational.)

[*]Corresponding Author

Received 23 June 2014; Accepted 06 May 2015

It is known that each elliptic curve has a quadratic twist. However, it is also well known that elliptic curves with j-invariant equal to 0, or in other words, curves of the form (1.1) also have higher twists. By [12, Definition 7.29], the quadratic, cubic, and sextic twists of the curve (1.1) by D are respectively of the forms $E_{kD^3} : y^2 = x^3+kD^3$, $E_{kD^2} : y^2 = x^3+kD^2$, and $E_{kD} : y^2 = x^3+kD$. We note that $E_k \simeq E_{kD^6}$, $E_{kD} \simeq E_{kD^5}$, $E_{kD^2} \simeq E_{kD^4}$, and that the constants of our curves are sixth-power free [15]. It would be interesting to have any information concerning the rank behavior of twists of E_k as $k \in \mathbb{Z}$ varies. In this work, however, we are interested in the $k = 1$ case.

By [5, Theorem 5.3], one can easily classify twists of E_1 into two categories: twists with trivial torsion groups, and twists with nontrivial torsion groups. The first class includes sextic twists while the other includes quadratic and cubic twists. In the first category, previous work has found infinitely many elliptic curves with rank at least seven [4] and particular members with ranks up to fifteen [6, 30 December, 2009]. Nevertheless, there is no more information on quadratic and cubic twists of E_1 (see also [10]). We recall that there are several infinite families of not Mordell curves over $\mathbb{Q}$ with nonconstant quadratic twists over the rational field $\mathbb{Q}(a)$, with the variable a, of rank at least two, three, and four [9, 2].

In Section 2 it is given parametric families of cubic and quadratic twists of E_1 whose (generic) ranks are, respectively, at least two and two, while in Section 3, we show the existence of infinitely many curves of rank ≥ 3, parametrised by an elliptic curve of rank at least two, and also construct a curve whose rank is at least three as cubic twists by the elliptic curve E_1. We do so by showing the independence of certain points.

2. Twists with Rank Two

Let us first recall how a torsion part of the Mordell curve E_k, with (nonzero) integer k assumed sixth-power free, looks like ([5, Theorem 5.3]. If $k = 1$, then $\mathcal{T} \simeq \mathbb{Z}/6\mathbb{Z}$. If $k \neq 1$ and k is a square in $\mathbb{Z}$, then $\mathcal{T} = \{\mathcal{O}, (0, \sqrt{k}), (0, -\sqrt{k})\}$. In case when $k = -432$, we have $\mathcal{T} = \{\mathcal{O}, (12, 36), (12, -36)\}$. If $k \neq 1$ and k is cubic in $\mathbb{Z}$, then $\mathcal{T} = \{\mathcal{O}, (-\sqrt[3]{k}, 0)\}$. In the remaining cases, $\mathcal{T} = \{\mathcal{O}\}$. As an immediate consequence we obtain that for any $k \neq -432$ if on the twisted curve E_k defined over $\mathbb{Q}$ we have a rational point $P = (x, y)$ with $xy \neq 0$, then the order of P in the group $E_k(\mathbb{Q})$ is infinite. Thus, the curve E_k over $\mathbb{Q}$ has positive rank.

For our next results, we need the following theorem of Gusić and Tadić:

Theorem 2.1. [3, Theorem 1.3] *Let*

$$E(t) : y^2 = x^3 + Ax^2 + Bx + C; \;\; A, B, C \in \mathbb{Z}[t]$$

be an nonconstant elliptic curve over $\mathbb{Q}$. Assume that $E(t)$ has exactly one nontrivial 2-torsion point over $\mathbb{Q}(t)$, i.e.,

$$x^3 + Ax^2 + Bx + C = (x - e_1)(x - e)(x - \bar{e}),$$

where $e_1 \in \mathbb{Z}[t]$, and e and $\bar{e}$ are conjugate. Let $t_0 \in \mathbb{Q}$ satisfy the following condition:

($\mathcal{A}$) *For every nonconstant square-free divisor h of $e_1^2 - (e + \bar{e})e_1 + e\bar{e}$ or $(e - \bar{e})^2$ in $\mathbb{Z}[t]$, the rational number $h(t_0)$ is not a square in $\mathbb{Q}$.*

Then, the specialised curve $E(t_0)$ is elliptic and the specialisation homomorphism at t_0 is injective.

Now we are ready to prove the following.

Theorem 2.2. *Let E_k be an elliptic curve defined by $y^2 = x^3 + k$, where*

(i) $k = (16a^6 + 27)^2$;

(ii) $k = \{3(27a^6 - 1)\}^3$,

with a variable a. Then, E_k has rank (i) at least two and (ii) two over $\mathbb{Q}(a)$, whose independent points are as follows

(i) $P_1 = (-12a^2, 16a^6 - 27)$, $P_2 = ((16a^6 - 81)/9, 4a^3(16a^6 + 243)/27)$;

(ii) $P_1 = (-(27a^6 - 1)/a^2, (27a^6 - 1)^2/a^3)$,
$P_2 = ((27a^6 - 1)(27a^6 - 4)/(9a^4), (27a^6 - 1)^2(27a^6 + 8)/(27a^6))$.

Proof. (i) By the specialisation theorem of Silverman ([13, Theorem 20.3] or [14]), in order to prove that the curve has rank at least two over $\mathbb{Q}(a)$, it suffices to find a specialisation $a = a_0$ such that the points P_1 and P_2 are (linearly) independent on the specialised curve over $\mathbb{Q}$. If we take $a = 1$, then the points

$$P_1 = (-12, 11), \quad P_2 = (-65/9, 1036/27)$$

are independent of infinite order on the rank-two specialised elliptic curve

$$E_{1849} : y^2 = x^3 + 1849.$$

Indeed, the elliptic regulator, i.e., the determinant of the Néron-Tate height pairing matrix, of the two points is the nonzero value 10.6633620537268 according to `SAGE` [11].

(ii) Take $a = 1$, then the points

$$P_1 = (-26, 676), \quad P_2 = (598/9, 23660/27)$$

are independent of infinite order on the rank-two elliptic curve

$$E_{474552} : y^2 = x^3 + 474552,$$

since the regulator of points P_1 and P_2 is the nonzero value 5.32235114744438. This shows that the curve has rank at least two over $\mathbb{Q}(a)$ with independent points P_1, P_2. Now, in order to show that the curve over $\mathbb{Q}(a)$ has rank two, it is sufficient to see that $a = 1$ satisfies the condition $(\mathcal{A})$ of Theorem 2.1. With the notation of Theorem 2.1, we have

$$e_1 = -81a^6 + 3, \quad e = \frac{3}{2}(1 + \sqrt{-3})(9a^4 + 3a^2 + 1)(3a^2 - 1),$$
$$\text{and} \quad \bar{e} = \frac{3}{2}(1 - \sqrt{-3})(9a^4 + 3a^2 + 1)(3a^2 - 1),$$

and hence

$$e_1^2 - (e + \bar{e})e_1 + e\bar{e} = 27(3a^2 - 1)^2(9a^4 + 3a^2 + 1)^2 \in \mathbb{Z}[a],$$

showing that the specialisation map at $a = 1$ is injective. This completes the proof. □

Similarly to Theorem 2.2, the following is proved.

Theorem 2.3. *Let E_k be an elliptic curve defined by $y^2 = x^3 + k$, where*

(i) $k = \{4a(a-1)(a-8)/(a^2-8)^2\}^2$;
(ii) $k = (a^6 + 1)^3$,

with a variable a. Then, E_k has rank (i) at least two and (ii) two over $\mathbb{Q}(a)$, whose independent points are as follows

(i) $P_1 = (-4a(a-1)(a-8)/(a^2-8)^2, 4a(a-1)(a-8)(a^2-2a+8)/(a^2-8)^3)$,
$P_2 = (-8a(a-1)(a-8)/(a^2-8)^2, 4a(a-1)(a-8)(a^2-16a+8)/(a^2-8)^3)$;
(ii) $P_1 = (a^2(a^6+1), (a^6+1)^2)$, $P_2 = ((a^6+1)/a^2, (a^6+1)^2/a^3)$.

Proof. (i) Specialisation at $a = 3$ shows that the points

$$P_1 = (120, 1320), \quad P_2 = (240, 3720)$$

are independent of infinite order on the rank-two elliptic curve

$$E_{14400} : y^2 = x^3 + 14400,$$

as the elliptic regulator of the two points is the nonzero value 1.38909303935706. Hence, the assertion follows immediately from the specialisation theorem of Silverman.

(ii) Choose $a = 2$. Then the specialised curve becomes

$$E_{274625} : y^2 = x^3 + 274625,$$

whose rank is two, and the two points are

$$P_1 = (260, 4225), \quad P_2 = (65/4, 4225/8).$$

These points are independent of infinite order, as the canonical height pairing matrix has nonzero determinant 1.79610378763826 showing that the curve has rank at least two over $\mathbb{Q}(a)$. Now, to prove that the curve over $\mathbb{Q}(a)$ has rank two, it suffices to see that $a = 2$ satisfies the condition $(\mathcal{A})$ of Theorem 2.1. With the notation of Theorem 2.1, for the curve we have

$$e_1 = -a^6 - 1, \quad e = \frac{1}{2}(1 + \sqrt{-3})(a^4 - a^2 + 1)(a^2 + 1),$$
$$\text{and} \quad \bar{e} = \frac{1}{2}(1 - \sqrt{-3})(a^4 - a^2 + 1)(a^2 + 1) \quad .$$

Hence

$$e_1^2 - (e + \bar{e})e_1 + e\bar{e} = 3(a^2 + 1)^2(a^4 - a^2 + 1)^2 \in \mathbb{Z}[a],$$

which shows the specialisation map at $a = 2$ is injective. This completes the proof. □

The following remark illustrates some connections between the elliptic curves $E_{\kappa^3} : y^2 = x^3 + \kappa^3$ and those of Rubin and Silverberg [9, Corollary 3.3].

Remark 2.4. In [9, Corollary 3.3], Rubin and Silverberg have proven that the elliptic curves

$$E_g^{A,B} : y^2 = x^3 + Agx^2 + Bg^2x$$

with $g = -AB(u^2 + B^2)(u^4 + 2B^2u^2 - A^2Bu^2 + B^4)$, $AB(B^2 - 4A) \neq 0$, are of rank (exactly) two. The curves $E_{\kappa^3} : y^2 = x^3 + \kappa^3$, $\kappa \neq 0$, isomorphic to $y^2 = x^3 - 3\kappa x^2 + 3\kappa^2 x$, can be thus changed into $E_g^{A,B}$, over some extension of $\mathbb{Q}$, so that $A^2 = 3B$. The quadratic $A^2 = 3B$ is equivalent to choosing $A = 3v$, $B = 3v^2$, and hence the curves E_{κ^3} with $\kappa = 9v^4u^6 + 6561v^{16}$ are of rank two over $\mathbb{Q}(u, v)$.

3. Cubic Twists with Rank Three

In this section we prove:

Theorem 3.1. *Consider the elliptic curve $E_{k^2} : y^2 = x^3 + k^2$. Then*

(i) *There are infinitely many elliptic curves E_{k^2} over $\mathbb{Q}$ whose ranks are at least three, parametrised by an elliptic curve of rank at least two.*

(ii) *There is an elliptic curve E_{k^2} over $\mathbb{Q}(m)$ whose rank is at least three, parametrised by an elliptic curve of rank at least two.*

Proof. (i) Let us set $k = a^2 - 1$. Theorem 5.3 of [5] implies that the Mordell curve

$$E_{k^2} : y^2 = x^3 + k^2, \tag{3.1}$$

is an infinite family with non-obvious point

$$P_1 = (a^2 - 1, a(a^2 - 1)).$$

A new point P_2 with x-coordinate $x_2 = 1 - a$ is on the cubic (3.1) if the expression $a^2 + a + 2$ is a rational square. This turns out to be equivalent to choosing

$$a = \frac{t^2 - 4t + 2}{t^2 - 1}.$$

Hence, the coefficient k of the subfamily E_k becomes

$$k = -\frac{(4t-3)(2t^2-4t+1)}{(t^2-1)^2},$$

and the x-coordinates of two independent points P_1 and P_2 turn out to be

$$\begin{aligned} x_1 &= -(4t-3)(2t^2-4t+1)/(t^2-1)^2, \\ x_2 &= (4t-3)/(t^2-1). \end{aligned}$$

Specialisation at, e.g., $t = 2$ shows that the points P_1 and P_2 are independent: For this value of t, which makes $a = -2/3$ and $k = -5/9$, the two points

$$P_1 = (-5/9, 10/27), \quad P_2 = (5/3, 20/9),$$

are independent of infinite order on the rank-two specialised curve

$$E_{(5/9)^2} : y^2 = x^3 + \left(\frac{5}{9}\right)^2.$$

Indeed, the determinant of the Néron-Tate height pairing matrix of the two points P_1, P_2 is the nonzero value 1.38909303935706. Now the condition for $x_3 = -1$ to be the x-coordinate of third point P_3 on the resulting cubic, gives the quartic equation

$$s^2 = -t^4 - 8t^3 + 24t^2 - 16t + 2.$$

Observe that $(-1, 7)$ is a rational point on the curve, so the quartic curve is birationally equivalent to the elliptic curve

$$E : w^2 + 4zw - 24w = z^3 - 10z^2 + 4z - 40,$$

being generated by $(-5, 29)$ and $(11, 5)$. Now a rational point (z, w) gives rise to the coordinate

$$t = \frac{2z + w - 20}{w}.$$

In particular, the generator $(z, w) = (-5, 29)$ maps to $t = -1/29$, which makes $a = -257/120$. Then the points

$$\begin{aligned} P_1 &= (51649/14400, 13273793/1728000), \\ P_2 &= (377/120, 95381/14400), \\ P_3 &= (-1, 49601/14400), \end{aligned}$$

are independent points of infinite order on the elliptic curve

$$y^2 = x^3 + 2667619201/207360000,$$

since the regulator of the points is over 104. So, the points on the elliptic curve E give a parametrisation for infinity many curves with rank at least three.

(ii) If we impose $x_2 = -2(a^2 - 1)$, as x-coordinate of a rational point P_2 on the cubic (3.1), then this leads to the condition that $9 - 8a^2$ is a square, and hence $a = -6t/(t^2 + 8)$. We thus get a family of (3.1) with

$$k = -\frac{(t-4)(t-2)(t+2)(t+4)}{(t^2+8)^2},$$

and independent points P_1 and P_2 with x-coordinates:

$$x_1 = -\frac{(t-4)(t-2)(t+2)(t+4)}{(t^2+8)^2},$$
$$x_2 = 2\frac{(t-4)(t-2)(t+2)(t+4)}{(t^2+8)^2}.$$

(In light of the specialisation theorem of Silverman, the resulting family has generic rank at least two over $\mathbb{Q}(t)$.) A calculation shows that if we consider $x_3 = -(t^2 - 4)/(t^2 + 8)$, as an x-coordinate of a new point P_3 on the resulting cubic, then the expression $8 - t^2$ must be a square. Setting

$$t = 2\frac{m^2 - 2m - 1}{m^2 + 1}, \tag{3.2}$$

then $8 - t^2 = 4(m^2 + 2m - 1)^2/(m^2 + 1)^2$. Thus with this value of t, we are led to an elliptic curve E_{k^2} with generic rank at least three over $\mathbb{Q}(m)$. The independence can be easily verified, and we omit the details. □

Acknowledgments

The authors would like to thank the referee for carefully reading of the paper and offering insightful comments, which improved the presentation of the paper.

References

1. H. Daghigh, M. Bahramian, Generalized jacobian and discrete logarithm problem on elliptic curves, *Iran. J. Math. Sci. Inform.*, **4**(2), (2009), 55–64.
2. A. Dujella, I. Gusić, L. Lasić, On quadratic twists of elliptic curves $y^2 = x(x-1)(x-\lambda)$, *Rad HAZU, Mat. Znan.*, **18**, (2014), 27–34.
3. I. Gusić, P. Tadić, Injectivity of specialization homomorphism of elliptic curves, *J. Number Theory*, **148**, (2015), 137–152.
4. S. Kihara, On the rank of elliptic curve $y^2 = x^3 + k$. II, *Proc. Japan Acad. Ser. A Math. Sci.*, **72**, (1996), 228–229.
5. A. Knapp, *Elliptic Curves*, Princeton University Press, 1992.
6. NMBRTHRY Home Page, https://listserv.nodak.edu/archives/nmbrthry.html.
7. A. Rastegar, Deformation of outer representations of Galois group, *Iran. J. Math. Sci. Inform.*, **6**(1), (2011), 33–52.
8. A. Rastegar, Deformation of outer representations of Galois group II, *Iran. J. Math. Sci. Inform.*, **6**(2), (2011), 33–41.
9. K. Rubin, A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, *Exp. Math.*, **10**, (2001), 559–569.

10. K. Rubin, A. Silverberg, *Twists of elliptic curves of rank at least four, in: Ranks of Elliptic Curves and Random Matrix Theory*, Cambridge University Press, 2007, 177–188.
11. SAGE software, *Version 4.5.3*, http://www.sagemath.org.
12. S. Schmitt, H. G. Zimmer, *Elliptic curves: A Computational Approach*, De Gruyter studies in mathematics, **31**, Berlin, Germany, 2003.
13. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1986.
14. J. H. Silverman, Heights and the specialization map for families of abelian varieties, *J. Reine Angew. Math.*, **342**, (1983), 197–211.
15. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.