

On quadratic twists of elliptic curves

$$y^2 = x(x - 1)(x - \lambda)$$

ANDREJ DUJELLA, IVICA GUSIĆ and LUKA LASIĆ

University of Zagreb, Croatia

Abstract

Let E be an elliptic curve over \mathbb{Q} given by $y^2 = f(x)$ where $f(x) = x(x - 1)(x - \lambda)$. In this paper, we describe a construction of twists $E_{g(u)}$ of rank 2 over $\mathbb{Q}(u)$, where $g(u)$ are polynomials over \mathbb{Q} . The construction leads to two sets of twists: the first consists of five twists obtained by Rubin and Silverberg with a different method, while the second consists of five new twists.

1 Introduction

Let $f(x) = x^3 + ax^2 + bx + c$ be a cubic polynomial over \mathbb{Q} and let E be an elliptic curve defined by $y^2 = f(x)$. For each polynomial g over \mathbb{Q} let E_g denote the quadratic twist of E by g defined by

$$g(t)y^2 = f(x),$$

and let \tilde{E}_g be E_g written in the form

$$y^2 = x^3 + ag(t)x^2 + bg^2(t)x + cg^3(t).$$

There is a $\mathbb{Q}(t)$ -isomorphism $E_g \rightarrow \tilde{E}_g$, given by $(x, y) \mapsto (g(t)x, g^2(t)y)$. The twist $E_{f(t)} : f(t)y^2 = f(x)$ has rank 1 over $\mathbb{Q}(t)$, with a point of infinite order $(t, 1)$ (see arguments given after Lemma 1). In [6] and [7] a general method for finding quadratic extensions $\mathbb{Q}(u)/\mathbb{Q}(t)$ such that the curve E_f has a new point over $\mathbb{Q}(u)$ independent from $(t(u), 1)$ has been described. It is based on the assumption that the x -coordinate is of the form $h(t(u))$

⁰2010 *Mathematics Subject Classification.* 11G05, 14H52.

Key words and phrases. Elliptic curve, quadratic twist.

where $h(t)$ is a linear fractional transformation in $\mathbb{Q}(t)$ that permutes roots of f . By varying h 's (i.e. by composing the quadratic extensions), families of quadratic twists of rank 3 and 4 were obtained in the case when E is defined by $y^2 = x(x-1)(x-\lambda)$. Similar results were obtained independently by Kuwata in [5]. On the other hand, several authors successfully used another method for constructing points on elliptic curves over $\mathbb{Q}(t)$ (see, for example [1] and [2]). For elliptic curves $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Q}[t]$, they searched for (as simple as possible) integral points. In the case of elliptic curves E_f it means that we are seeking integral points on the curve \tilde{E}_f . In this paper we make a detailed analysis of the later method for a class of possible integral points, for quadratic twists of $E : y^2 = x(x-1)(x-\lambda)$. We find that, for this class, the method rediscovers five twists coming from [6, Propositions 2.7 and 2.9]. Further, we find that the method discovers five new twists (see Theorem 2). In other words the method leads to new five quadratic extensions of $\mathbb{Q}(t)$ over which E_f has rank two.

In Section 2 we get four sets of five quadratic twists (it is only a part of quadratic twists that can be obtained by the approach from Section 2). We prove that these four sets reduce to two sets of five twists (Lemma 4). In Section 3 we prove that one of these two sets corresponds to the set of five twists coming from [6, Propositions 2.7 and 2.9] (these five twists correspond to five nontrivial fractional linear transformations permuting $\{0, 1, \lambda\}$).

2 Description and application of the method

Lemma 1 *Let E be an elliptic curve over \mathbb{Q} , let g be a polynomial over \mathbb{Q} , and let C be the curve $s^2 = g(u)$. Then $\text{rank}(E_g(\mathbb{Q}(u))) \leq \text{genus}(C)$.*

PROOF. See [8, Section 4, Corollary 1] and [6, Remark 2.12]. ■

By Lemma 1, E_f has rank 1 over $\mathbb{Q}(t)$, with a point of infinite order $T_1(t, 1)$ (see e.g. [4, Corollary 1(1)]). Note that $\tilde{T}_1(tf(t), f^2(t))$ is the corresponding point on \tilde{E}_f .

In the rest of the paper, we assume that

$$E = E^\lambda : y^2 = x(x-1)(x-\lambda) = x^3 - (\lambda+1)x^2 + \lambda x.$$

Then,

$$E_g : g(t)y^2 = x(x-1)(x-\lambda),$$

and

$$\tilde{E}_g : y^2 = x(x-g(t))(x-\lambda g(t)) = x^3 - (\lambda+1)g(t)x^2 + \lambda g^2(t)x.$$

For each g , the curve E_g has three points of second order: $(0, 0)$, $(1, 0)$, $(\lambda, 0)$.

Lemma 2 *Let $T(r, s)$ be a point on E_g . Then*

$$\begin{aligned} T + (0, 0) &= \left(\frac{\lambda}{r}, -\frac{\lambda s}{r^2} \right), & T + (1, 0) &= \left(\frac{r - \lambda}{r - 1}, \frac{(\lambda - 1)s}{(r - 1)^2} \right), \\ T + (\lambda, 0) &= \left(\frac{\lambda(r - 1)}{r - \lambda}, \frac{\lambda(1 - \lambda)s}{(r - \lambda)^2} \right). \end{aligned}$$

PROOF. By direct calculation. ■

We try to find a new point \tilde{T}_2 on \tilde{E}_f under the assumption that it is $\mathbb{Q}[t]$ -integral, especially that $\tilde{x} := x(\tilde{T}_2)$ satisfies $\tilde{x}|f^2(t)$. Generally, for $y^2 = x^3 + ax^2 + bx$, we search for a point (\tilde{x}, \tilde{y}) such that $\tilde{x}|b$ and

$$\tilde{J} := \tilde{x} + a + \frac{b}{\tilde{x}} \tag{1}$$

is a complete square in $\mathbb{Q}[t]$. We will see that this is possible after a suitable quadratic substitution $t = t(u)$. In other words, the new point is defined over a quadratic extension $\mathbb{Q}(u)$ of $\mathbb{Q}(t)$. Let us sketch the procedure. Although we have a variety of possibilities for \tilde{x} , in this Section we restrict our consideration to $\tilde{x} = A(t - \alpha)(t - \beta)^2$, where α, β, γ are the roots of $x^3 - (\lambda + 1)x^2 + \lambda x$ and A is a rational constant. Then the expression \tilde{J} from (1) becomes

$$\tilde{J}_{A,\alpha,\beta}(t) = \frac{t - \alpha}{A} (A^2(t - \beta)^2 - (\lambda + 1)A(t - \beta)(t - \gamma) + \lambda(t - \gamma)^2). \tag{2}$$

Note that the corresponding point T_2 on E_f has first coordinate $x = x(T_2) = A \frac{t - \beta}{t - \gamma}$, i.e. that it is of the form $h(t)$ where h is a special fractional linear transformation over \mathbb{Q} .

Generally, $\tilde{J}_{A,\alpha,\beta}$ is a cubic polynomial in t . We search for a substitution $t = t(u)$ under which it becomes a square. In the following lemma we will describe conditions under which $\tilde{J}_{A,\alpha,\beta}$ has a double root, or reduces to a quadratic polynomial.

Lemma 3 *Let $\tilde{J}_{A,\alpha,\beta}$ be as in (2). Then:*

- (a) $\tilde{J}_{A,\alpha,\beta}(t) = \frac{1}{A}(t - \alpha)((A - 1)t - (\beta A - \gamma))((A - \lambda)t - (\beta A - \lambda\gamma))$.
- (b) *If $\tilde{J}_{A,\alpha,\beta}$ has a double root, then $A = \frac{\alpha - \gamma}{\alpha - \beta}$ or $A = \lambda \frac{\alpha - \gamma}{\alpha - \beta}$; in both cases α is the unique double root.*

(c) If $\tilde{J}_{A,\alpha,\beta}$ reduces to a quadratic polynomial, then $A = 1$ or $A = \lambda$.

PROOF.

(a) By direct calculation.

(b) It is easy to see that the polynomials $(A - 1)t - (\beta A - \gamma)$ and $(A - \lambda)t - (\beta A - \lambda\gamma)$ are not proportional. Now the statement follows from (a).

(c) Directly from (a). \blacksquare

Let us consider the case $A = \frac{\alpha - \gamma}{\alpha - \beta}$ from Lemma 3. Then

$$\frac{\tilde{J}_{A,\alpha,\beta}}{(t - \alpha)^2} = \frac{\beta - \gamma}{(\alpha - \gamma)(\alpha - \beta)} ((1 - \lambda)\alpha + \lambda\beta - \gamma)t - (\alpha\beta - (1 - \lambda)\beta\gamma - \lambda\alpha\gamma).$$

The condition that \tilde{J} has to be a square can be restated as

$$t = t(u) = \frac{u^2 - (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)(\alpha\beta + (\lambda - 1)\beta\gamma - \lambda\gamma\alpha)}{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)((\lambda - 1)\alpha - \lambda\beta + \gamma)}. \quad (3)$$

The first coordinate $x = A \frac{t - \beta}{t - \gamma}$ of the corresponding point T_2 on $E_{f(t(u))}$ becomes

$$x = x(T_2) = \frac{\alpha - \gamma}{\alpha - \beta} \cdot \frac{u^2 - \lambda(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)}{u^2 + (\alpha - \beta)(\beta - \gamma)^2(\gamma - \alpha)^2}. \quad (4)$$

Remark 1 The point from (4) is defined over $\mathbb{Q}(u)$, where $u = \sqrt{k_{\alpha,\beta}(t)}$, with

$$k_{\alpha,\beta}(t) := (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)((\lambda - 1)\alpha - \lambda\beta + \gamma)t + (\alpha\beta - (1 - \lambda)\beta\gamma - \lambda\alpha\gamma).$$

If $(\alpha, \beta, \gamma) = (0, 1, \lambda)$ then $k(t)$ degenerates and we have no new points. It is easy to see (by direct calculation) that the other five cases produce nonisomorphic twists $E_{f(t(u))}$. Furthermore, in each case a new point

$$T_2 \left(x, \sqrt{\frac{f(x)}{f(t(u))}} \right)$$

is independent from $T_1(t(u), 1)$ (see Theorem 1, below). By Lemma 1, it means that in that cases we have $\text{rank}(E_{f(t(u))}(\mathbb{Q}(u))) = 2$. In other words, E_f has rank two over five quadratic extensions $\mathbb{Q}(\sqrt{k_{\alpha,\beta}(t)})$ of $\mathbb{Q}(t)$. There are some exceptional values of λ : if $(\alpha, \beta, \gamma) = (0, \lambda, 1)$ then $\lambda \neq -1$, if $(\alpha, \beta, \gamma) = (1, 0, \lambda)$ then $\lambda \neq \frac{1}{2}$, and if $(\alpha, \beta, \gamma) = (\lambda, 1, 0)$ then $\lambda \neq 2$. Let us interpret (α, β, γ) as the permutation π of the letters $0, 1, \lambda$ defined by $\pi(0) = \alpha$, $\pi(1) = \beta$, $\pi(\lambda) = \gamma$. Then there is no exceptional value of λ if and only if π is a cyclic permutation.

In the following theorem we use arguments from [6, Lemma 2.3 and Corollary 3.3] to prove that T_1 and T_2 are independent.

Theorem 1 *Let $\tilde{J}_{A,\alpha,\beta}$ be as in (2), with $A = \frac{\alpha-\gamma}{\alpha-\beta}$. Assume that $(\alpha, \beta, \gamma) \neq (0, 1, \lambda)$. Then the points $T_1(t(u), 1)$ and $T_2\left(x, \sqrt{\frac{f(x)}{f(t(u))}}\right)$ on $E_{f(t(u))}$, where x is as in (4), are independent.*

PROOF. The points T_1, T_2 are nonconstant, which implies that they are of infinite order. Namely, if g is non-constant and E any elliptic curve over \mathbb{Q} , then in the family $E_{g(\tau)}$, $\tau \in \mathbb{Q}$ there are infinitely many \mathbb{Q} -nonisomorphic quadratic twists of E (see, for example, [8, Theorem 2]). Assume that E_g has a non-constant torsion point T over $\mathbb{Q}(u)$. Then the specialization produces torsion points of order > 2 on infinitely many different \mathbb{Q} -twists of E . It is a contradiction (see, for example [3, Proposition 1]).

Consider the second coordinate y of the point T_2 . By this procedure, up to a sign, we have

$$y = \frac{\tilde{x}(t(u) - \alpha)u}{(\alpha - \beta)(\gamma - \alpha)f(t(u))^2} = \frac{x(t(u) - \alpha)u}{(\alpha - \beta)(\gamma - \alpha)f(t(u))}.$$

Since $t(u)$ and x are even functions in u , we see that y is odd as a function in u . Therefore the automorphism $u \mapsto -u$ of $\mathbb{Q}(u)$ over $\mathbb{Q}(t)$ fixes T_1 and sends T_2 to $-T_2$. This implies that T_1 and T_2 are independent. ■

Lemma 4 *Let the notation be as in Lemma 3. Then:*

- (a) *Assume that $J_{A,\alpha,\beta}$ has a double root (reduces to a quadratic polynomial). Then $J_{\frac{\lambda}{A},\alpha,\gamma}$ has a double root (reduces to a quadratic polynomial).*
- (b) *Let T (respectively T') be the points on E_f corresponding to the choice $\tilde{x} = A(t - \alpha)(t - \beta)^2$ (respectively to the choice $\tilde{x} = \frac{\lambda}{A}(t - \alpha)(t - \gamma)^2$). Then, after a choice of the sign, we have $T' = T + (0, 0)$.*

PROOF.

- (a) Follows from Lemma 3.
- (b) Follows from (a) and Lemma 2. ■

Remark 2 By permuting α, β, γ , the expression $A = \frac{\alpha-\gamma}{\alpha-\beta}$ takes six different values $\lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}$. Then the expression $\frac{\lambda}{A}$ takes the

corresponding values $1, \lambda^2, \frac{\lambda}{1-\lambda}, \lambda(1-\lambda), \frac{\lambda^2}{\lambda-1}, \lambda-1$. Note that (1) is invariant under the transformation $\tilde{x} \mapsto \frac{b}{\tilde{x}}$. Therefore $\tilde{x} = A(t-\alpha)(t-\beta)^2$ leads to the same substitution $t = t(u)$ as $\tilde{x} = \frac{\lambda}{A}(t-\alpha)(t-\gamma)^2$. Therefore, in both cases we get the same twist $E_{f(t(u))}$. By Lemma 4, the corresponding points on $E_{f(t(u))}$ differ by the point $(0, 0)$. Therefore, without loss of generality, we may assume that, in the case when \tilde{J} has a double point, we have $A = \frac{\alpha-\gamma}{\alpha-\beta}$.

In the following theorem we will describe the case when \tilde{J} reduces to a quadratic polynomial. By Lemma 3, we have $A = 1$ or $A = \lambda$. By Lemma 4, we may assume that $A = 1$. We will see that this case leads to five new quadratic twists of rank two. In other words, we find new five different quadratic extensions $\mathbb{Q}(z)$ of $\mathbb{Q}(t)$ over which E_f has rank two.

Theorem 2 *Assume that $\tilde{J}_{A,\alpha,\beta}$ reduces to a quadratic polynomial with $A = 1$. For $(\alpha, \beta, \gamma) \neq (0, \lambda, 1)$ it leads to five twists over*

$$\mathbb{Q}(z) = \mathbb{Q}(t)(\sqrt{(\beta-\gamma)(t-\alpha)((\lambda-1)t+(\beta-\lambda\gamma))}),$$

with $t = t(z) = \frac{\alpha z^2 + (\beta-\gamma)(\beta-\lambda\gamma)}{z^2 - (\lambda-1)(\beta-\gamma)}$, and the point on $E_{f(t(z))}$ with first coordinate $x = \frac{(\alpha-\beta)z^2 + \lambda(\beta-\gamma)^2}{(\alpha-\gamma)z^2 + (\beta-\gamma)^2}$. These five twists are different from those described by (3), (4) and Remark 1.

PROOF. By Lemma 3 (a), we get $\tilde{J}_{A,\alpha,\beta} = (\beta-\gamma)(t-\alpha)((\lambda-1)t+(\beta-\lambda\gamma))$. Now we apply the transformation $\tilde{J}_{A,\alpha,\beta} = ((t-\alpha)z)^2$, and put into $x = \frac{t-\beta}{t-\gamma}$. Note that these five twists are defined over five different quadratic extensions of $\mathbb{Q}(t)$, which are different from the extensions $\mathbb{Q}(t)(\sqrt{k_{\alpha,\beta}(t)})$ from Remark 1. Analogously as in Theorem 1, we see that the rank over $\mathbb{Q}(z)$ of each of five curves is two. ■

3 A connection with formulas from [6] and [7]

In [6] a method of finding points on

$$E_{f(t(u))} : f(t(u))y^2 = f(x)$$

with x -coordinate equal to $h(t(u))$ has been described, where $h(t)$ is a linear fractional transformation in $\mathbb{Q}(t)$ that permutes roots of f and $\mathbb{Q}(u)$ is a suitable quadratic extension of $\mathbb{Q}(t)$. By [6, Proposition 2.9], given such h , there exist a linear polynomial k and a rational function j over \mathbb{Q} such that

$$f(h(t)) = k(t)f(t)j^2(t).$$

Therefore, we may make the substitution $k(t) = u^2$. Then

$$(h(t(u)), \sqrt{\frac{f(h(t(u)))}{f(t(u))}})$$

is a point on $E_{f(t(u))}$. This method works for f having at least one rational root; here we concentrate on f of the form $x(x-1)(x-\lambda)$ for $\lambda \in \mathbb{Q}$, $\lambda \neq 0, 1$. We will see that this method is equivalent to the method from Section 2 in the case when \tilde{J} has a double point. As we have already seen (see Remark 2), it is sufficient to consider the case $A = \frac{\alpha-\gamma}{\alpha-\beta}$. Recall that this case leads to the point on E_f with first coordinate $x = \frac{\alpha-\gamma}{\alpha-\beta} \cdot \frac{t-\beta}{t-\gamma}$.

Theorem 3 *Assume that a point T on E_f has first coordinate $\frac{\alpha-\gamma}{\alpha-\beta} \cdot \frac{t-\beta}{t-\gamma}$. Let $h(t) = h_{\alpha,\beta}(t)$ be the first coordinate of $T + (\lambda, 0)$. Then h permutes letters $0, 1, \lambda$. Explicitly, $h(\alpha) = 0$, $h(\beta) = 1$, $h(\gamma) = \lambda$.*

PROOF. By Lemma 2, we get

$$h(t) = h_{\alpha,\beta}(t) = \lambda \frac{(\alpha - \gamma)(t - \beta) - (\alpha - \beta)(t - \gamma)}{(\alpha - \gamma)(t - \beta) - \lambda(\alpha - \beta)(t - \gamma)}.$$

Now the statement follows by direct calculation. ■

Remark 3 Theorem 3 says that formula (4) from Section 2 in this context leads to formulas from [6, Propositions 2.7 and 2.9]

Following [7, Definition 3.1], we fix linear fractional transformations h_i ; $i = 1, 2, 3, 4, 5, 6$ that permute roots

$$\begin{aligned} h_1(t) &= t, & k_1(t) &= 1, \\ h_2(t) &= \frac{t - \lambda}{(2 - \lambda)t - 1}, & k_2(t) &= (1 - \lambda)((\lambda - 2)t + 1), \\ h_3(t) &= \frac{\lambda^2 t - \lambda^2}{(\lambda^2 - \lambda + 1)t - \lambda}, & k_3(t) &= \lambda(1 - \lambda)((\lambda^2 - \lambda + 1)t - \lambda), \\ h_4(t) &= \frac{\lambda t}{(\lambda + 1)t - \lambda}, & k_4(t) &= \lambda((\lambda + 1)t - \lambda), \\ h_5(t) &= \frac{\lambda^2 t - \lambda^2}{((2\lambda - 1)t - \lambda^2)}, & k_5(t) &= \lambda(\lambda - 1)((1 - 2\lambda)t + \lambda^2), \end{aligned}$$

$$h_6(t) = \frac{\lambda t - \lambda^2}{(\lambda^2 - \lambda + 1)t - \lambda^2}, \quad k_6(t) = \lambda(\lambda - 1)((\lambda^2 - \lambda + 1)t - \lambda^2).$$

Using cycle notation we have:

$$h_2 = (0\lambda), \quad h_3 = (0\lambda 1), \quad h_4 = (1\lambda), \quad h_5 = (01), \quad h_6 = (01\lambda).$$

Remark 4 It is easy to check that h_i , $i = 1, 2, \dots, 6$ coincide with $h_{\alpha,\beta}$ as α, β, γ permute. Also, k_i are square-free parts of

$$k_{\alpha,\beta}(t) := (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)((\lambda - 1)\alpha - \lambda\beta + \gamma)t + (\alpha\beta - (1 - \lambda)\beta\gamma - \lambda\alpha\gamma)$$

(see Remark 1). Explicitly:

$$\begin{aligned} h_{0,1} &= h_1, & k_{0,1}(t) &= \lambda^2(\lambda - 1)^2 = \lambda^2(\lambda - 1)^2 \cdot k_1(t), \\ h_{0,\lambda} &= h_4, & k_{0,\lambda}(t) &= (\lambda - 1)^2 \cdot k_4(t), \\ h_{1,0} &= h_5, & k_{1,0} &= k_5, \\ h_{1,\lambda} &= h_3, & k_{1,\lambda} &= k_3, \\ h_{\lambda,0} &= h_6, & k_{\lambda,0}(t) &= k_6, \\ h_{\lambda,1} &= h_2, & k_{\lambda,1}(t) &= \lambda^2 \cdot k_2(t). \end{aligned}$$

We see that, for corresponding $k_{\alpha,\beta}$ and k_i , there exists $d_{\alpha,\beta} \in \mathbb{Z}[\lambda]$ such that $k_{\alpha,\beta}(t) = d_{\alpha,\beta}^2 k_i(t)$.

Acknowledgements. This work has been supported by Croatian Science Foundation under the project no. 6422.

References

- [1] J. Aguirre, A. Dujella and J. C. Peral, *On the rank of elliptic curves coming from rational Diophantine triples*, Rocky Mountain J. Math. **42** (2012), 1759–1776.
- [2] A. Dujella and M. Jukić Bokun, *On the rank of elliptic curves over $\mathbb{Q}(i)$ with torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$* , Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), 93–96.
- [3] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
- [4] I. Gusić and L. Lasić, *Explicit canonical height on isotrivial elliptic curves*, J. Algebra Number Theory, Adv. Appl. **7** (2012), 95–107.

- [5] M. Kuwata, *Quadratic twists of an elliptic curve and maps from a hyperelliptic curve*, Math. J. Okayama Univ. **47** (2005), 85–97.
- [6] K. Rubin and A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experimental Mathematics **10** (2001), 559–569.
- [7] K. Rubin and 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.
- [8] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

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

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

Luka Lasić
Faculty of Chemical Engin. and Techn.
University of Zagreb
Marulićev trg 19, 10000 Zagreb
Croatia
E-mail address: `llasic@fkit.hr`