VARIATIONS ON TWISTS OF TRIPLES OF ELLIPTIC CURVES

MACIEJ ULAS

Abstract. In this note we show that for any triple E_1, E_2, E_3 of elliptic curves, where j-invariants of the curves E_2, E_3 are equal to 0 there exist rational functions $D_{2,3,3}, D_{2,6,6} \in \mathbb{Q}(u, v, w)$ with such a property that:

- the quadratic twist of the curve E_1 and the cubic twists of the curves E_2, E_3 by the $D_{2,3,3}$ have positive rank over $\mathbb{Q}(u, v, w)$,
- the quadratic twist of the curve E_1 and the sextic twists of the curves E_2, E_3 by the $D_{2,6,6}$ have positive rank over $\mathbb{Q}(u, v, w)$.

Moreover, we also prove that if j-invariant of E_1 is equal to 0 then there exist a rational function $D_{3,3,6} \in \mathbb{Q}(u, v, w)$ with such a property that the cubic twists of the curves E_1, E_2 and the sextic twists of the curve E_3 by the $D_{3,3,6}$ have positive rank over $\mathbb{Q}(u, v, w)$.

1. Introduction

Let E_1, E_2 be elliptic curves with the property that their j-invariants are not equal to 0 or 1728 simultaneously. Kuwata and Wang in the paper [4] proved the existence of the polynomial D such that the quadratic twist $E_{i,\ D}$ of the curve E_i by D have positive rank for $i = 1, 2$. Their method cannot be used in the case when $j(E_1) = j(E_2) = j$, where $j = 0, 1728$. Unfortunately, we are unable to show that also in these cases one can construct quadratic twists of pairs of elliptic curves with positive rank. It is known that each elliptic curve has a quadratic twist. However, it is well known too that elliptic curves with j-invariant equal to 0, or in other words, curves of the form $E : y^2 = x^3 + p$ have also higher twists. The cubic twist of the curve E by D has the equation $y^2 = x^3 + pD^2$. However, for our purposes it will be more convenient to work with the isomorphic model of the cubic twist given by the equation $y^2 = Dx^3 + p$. The sextic twist of the curve E by D is given by the equation $y^2 = x^3 + pD$.

In a recent paper [6] we proved that for any quadruple of pairwise distinct elliptic curves E_i, $i = 1, 2, 3, 4$, with j-invariant 0 there exists a polynomial $D \in \mathbb{Z}[u]$ such that the sextic twist of the curve E_i by $D(u)$ has positive rank for $i = 1, 2, 3, 4$. Moreover, in [7] we proved that for any pair of elliptic curves E_1, E_2 with $j = 0$ there exist a polynomial D such that the sextic twist of the curve E_i by D has rank ≥ 2 for $i = 1, 2$.

The aim of this note is to give results concerning the existence of various twists of triples of elliptic curves, where two or three of elliptic curves have j-invariant 0, with positive rank. More precisely, let $m, a, b, c \in \mathbb{Z}$ and consider the elliptic curves

$$(1) \qquad E_1:\ y_1^2 = x_1^3 + mx_1 + a, \quad E_2:\ y_2^2 = x_2^3 + b, \quad E_3:\ y_3^2 = x_3^3 + c,$$

2000 *Mathematics Subject Classification.* 11G05.

Key words and phrases. higher twists of elliptic curves, elliptic curves, rank, j-invariant .
The author is holder of START scholarship funded by the Foundation for Polish Science (FNP).

(we thus assume that $bc \neq 0$ and $4m^3 + 27a^2 \neq 0$). We prove that for any choice of the integers m, a, b, c there exist a rational function $D_A \in \mathbb{Q}(u, v, w)$, where $A \in \{(2, 3, 3),\ (2, 6, 6)\}$, with such a property that:

- the quadratic twist of the curve E_1 and the cubic twists of the curves E_2, E_3 by the rational function $D_{2,3,3}$ have positive rank over $\mathbb{Q}(u, v, w)$,
- the quadratic twist of the curve E_1 and the sextic twists of the curves E_2, E_3 by the rational function $D_{2,6,6}$ have positive rank over $\mathbb{Q}(u, v, w)$.

If additionally $m = 0$, i.e. E_1 is given by the equation $y^2 = x^3 + a$, then there exist a rational function $D_{3,3,6} \in \mathbb{Q}(u, v, w)$ with such a property that the cubic twists of the curves E_1, E_2 and the sextic twists of the curve E_3 by the $D_{3,3,6}$ have positive rank over $\mathbb{Q}(u, v, w)$.

Let us define $f(x) = x^3+mx+a$ and note that in order to find demanded rational functions the following systems of equations must have parametric solutions:

$$D_{2,3,3} = \frac{f(x_1)}{y_1^2} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - c}{x_3^3} \tag{2}$$

in case of quadratic twist and two cubic twists,

$$D_{2,6,6} = \frac{f(x_1)}{y_1^2} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c} \tag{3}$$

in case of quadratic twist and two sextic twists, and finally

$$D_{3,3,6} = \frac{y_1^2 - a}{x_1^3} = \frac{y_2^2 - b}{x_3^3} = \frac{y_3^2 - x_3^3}{c}. \tag{4}$$

in case of two cubic twists and sextic twist.

In order to prove our results we will construct rational parametric solution of each of the systems given above. In order to prove that the corresponding points which lie on appropriate twists have infinite order we use the well know classification of the possible torsion subgroups of the rational elliptic curve $E:\ y^2 = x^3 + q$, where $q \in \mathbb{Q}$ and q is sixth-power free (see, for example, Cassels [1], Chapter 12). More precisely we have $q = 1, -432$, or a torsion point (x, y) has $xy = 0$. As an immediate consequence of this property we obtain that if $E':\ y^2 = x^3 + qD$ is the sextic twist of the curve E by $D \in \mathbb{Q}(t_1, \ldots, t_m) \setminus \mathbb{Q}$ and on the curve E' we have a $\mathbb{Q}(t_1, \ldots, t_m)$ rational point $P = (x, y)$ with $xy \neq 0$ for some $m \in \mathbb{Z}_+$, then the order of the point P in the group $E'(\mathbb{Q}(t_1, \ldots, t_m))$ is not finite provided that E' is not isomorphic to an elliptic curve defined over $\mathbb{Q}$. Thus, the curve E' defined over $\mathbb{Q}(t_1, \ldots, t_m)$ has positive rank. It is clear that exactly the same argument works for cubic twists of the curve E.

Acknowledgments: This project was initiated during the Junior Trimester Program "Algebra and Number Theory" at the Hausdorff Research Institute for Mathematics (Bonn, Spring 2010). The author is grateful for the hospitality of this institution.

2. Quadratic twist and two cubic twists

The aim of this section is to prove the following result.

Theorem 2.1. *Let $m, a, b, c \in \mathbb{Z}$ and consider the elliptic curves given by (1). Then there exists a rational function $D_{2,3,3} \in \mathbb{Q}(u, v, w)$ such that the quadratic twist of the curve E_1 and the cubic twists of the curves E_2, E_3 by $D_{2,3,3}(u, v, w)$ have positive rank over the field $\mathbb{Q}(u, v, w)$.*

Proof. It is clear that for our purposes we need solutions x_i, y_i of the system (2) which satisfy the condition $x_i y_i \neq 0$ for $i = 1, 2, 3$ and $f(x_1)(y_2^2 - b)(y_3^2 - c) \neq 0$.

In order to find solutions of the system (2) we make the following substitutions

$$x_1 = u, \quad x_2 = \frac{1}{v^2 T}, \quad x_3 = \frac{1}{T} \quad y_1 = \frac{1}{T}, \quad y_2 = p, \quad y_3 = q,$$

where u, v are rational parameters and p, q, T have to be determined. After this substitution the system (2) takes the form

$$T^2 f(u) = v^6 T^3 (p^2 - b) = T^3 (q^2 - c).$$

It is easy to see that the above system is equivalent to the following

$$T = \frac{f(u)}{v^6 (p^2 - b)}, \quad v^6 (p^2 - b) = q^2 - c. \tag{5}$$

The first equation is just solved, the second can be interpreted as a quadratic equation with coefficients in the field $\mathbb{Q}(v)$. So this equation defines the genus zero curve, say C_1, over the field $\mathbb{Q}(v)$. It is easy to see that the curve C_1 has $\mathbb{Q}(v)$-rational point at infinity $[p : q : r] = [1 : v^3 : 0]$. Using this point and the standard method we can parameterize the set of rational points on C_1 as follows:

$$p = \frac{(b + w^2)v^6 - c}{2wv^6}, \quad q = \frac{(b - w^2)v^6 - c}{2wv^3}, \tag{6}$$

where w is a rational parameter. Using the computed value of p we find that the T from the system (5) takes the form

$$T = T(u, v, w) = \frac{4w^2 v^6 f(u)}{v^{12} w^4 - 2v^6 (bv^6 + c) w^2 + (bv^6 - c)^2}. \tag{7}$$

From the presented construction of the solutions of the system (5), and thus the system (2), we get the value of $D_{2,3,3}$ we are looking for in the form

$$D_{2,3,3}(u, v, w) = f(u) T(u, v, w)^2.$$

Using now the computed values of p, q, T we get that the point

$$P_1 = (u f(u) T(u, v, w)^2,\ f(u)^2 T(u, v, w)^3)$$

lies on the curve $E_1' :\ y_1^2 = x_1^3 + m D_{2,3,3}(u, v, w) x_1 + a D_{2,3,3}(u, v, w)^3$ which is the quadratic twist of the curve E_1 by $D_{2,3,3}(u, v, w)$. Moreover, the points

$$P_2 = \left(\frac{1}{v^2} f(u) T(u, v, w),\ f(u) p T(u, v, w)^2) \right),$$
$$P_3 = \left(f(u) T(u, v, w),\ f(u) q T(u, v, w)^2) \right),$$

where $p, q,$ are given by (6), lie on the curves

$$E_2' :\ y_2^2 = x_2^3 + b D_{2,3,3}(u, v, w)^2, \quad E_2' :\ y_2^2 = x_2^3 + c D_{2,3,3}(u, v, w)^2$$

which are cubic twists of the curves E_2, E_3 respectively.

Because the twist by $D_{2,3,3}$ is non-constant it is clear that the point P_1 is of infinite order on the curve E_1'. Now let us note that the coordinates of the point $P_i = (x_i, y_i)$ satisfy the condition $x_i y_i \neq 0$ for $i = 2, 3$ and any given $m, a, b, c \in \mathbb{Z}$.

Moreover it is easy to see that the rational function $D^j_{2,3,3}$ for $j=2,3$ is not of the form $AF(u,v,w)^6$, where $A\in\mathbb{Q}$ and $F\in\mathbb{Q}(u,v,w)$ which implies that the curve E'_i is not isomorphic to the one defined over $\mathbb{Q}$. Thus, from the remark given at the end of the introduction we deduce that the point P_i is of infinite order in the group $E'_i(\mathbb{Q}(u,v,w))$ for $i=2,3$. □

As an easy consequence of the theorem we have just proved we get the following.

Corollary 2.2. *Let $m,a,b,c\in\mathbb{Z}$ and consider the elliptic curves given by (1). Then the set, say $\mathcal{D}_{2,3,3}$, of all $d\in\mathbb{Q}$ such that the quadratic twist of the curve E_1 and the cubic twists of the curves E_2,E_3 by d have positive rank is infinite.*

Proof. This is an easy consequence of the fact that for any given $m,a,b,c\in\mathbb{Z}$ there exist infinitely many integers u_0,v_0,w_0 with such a property that the coordinates of the point $P_i(u_0,v_0,w_0)$ obtained by the specialization of the point P_i at $(u,v,w)=(u_0,v_0,w_0)$ are nonzero for $i=1,2,3$ and the number $D_{2,3,3}(u_0,v_0,w_0)$ is not equal to 1, -432 and is not a square neither a cube in $\mathbb{Q}$. This proves that the set $\mathcal{D}_{2,3,3}$ is infinite. □

Example 2.3. Let us consider the following elliptic curves:

$$E_1:\ y^2=x^3+x+2,\quad E_2:\ y^2=x^3+1,\quad E_3:\ y^2=x^3+6.$$

One can easily check using APECS program [2] that the rank of E_i is zero for $i=1,2,3$. In our case we have $a=2,b=1,c=6,m=1$ and taking $u=1,v=2,w=2$ we get $d=D_{2,3,3}(1,2,2)=4194304/68310225$. Then from the construction presented in the Theorem 2.1 we find that the point

$$P_1=\left(\frac{4194304}{68310225},\frac{17179869184}{564584009625}\right),$$

lies on the quadratic twist of E_1 by d and is of infinite order. Moreover, the points

$$P_2=\left(\frac{1024}{8265},\frac{5144576}{68310225}\right),\quad P_3=\left(\frac{4096}{8265},-\frac{2883584}{7590025}\right)$$

lie on the cubic twists of the curves E_2,E_3 by d respectively. It is clear that these points are of infinite order.

Corollary 2.4. *Let $m,a,b\in\mathbb{Z}$ and consider the elliptic curves $E_1:\ y^2=x^3+mx+a,\ E_2:\ y^2=x^3+b$. Then there exists a rational function $D_{2,3}\in\mathbb{Q}(u,v,w)$ with such a property that the quadratic twist of E_1 by $D_{2,3}(u,v,w)$ has positive rank and the cubic twist of E_2 by $D_{2,3}(u,v,w)$ has rank ≥ 2 over $\mathbb{Q}(u,v,w)$.*

Proof. In order to define the demanding function we make a substitution $c=b$ in the function $D_{2,3,3}$. As a $D_{2,3}$ we take the result of this substitution. Now let us note that on the curve E'_1 which is the quadratic twist of the E_1 by $D_{2,3}(u,v,w)$ we have points P which comes from the point P_1 where we substitute $c=b$. It is clear that the point P is of infinite order on E'_1. Next we see that on the curve E'_2 which is the cubic twist of the curve E_2 by $D_{2,3}(u,v,w)$ we have two points Q_1,Q_2 which comes from the points P_2,P_3 which lie on the curves $y^2=x^3+b,\ y^2=x^3+c$ where we substitute $c=b$. Clearly the points Q_1,Q_2 are of infinite order. We show now that the points Q_1,Q_2 are independent in the group $E'_2(\mathbb{Q}(u,v,w))$. In order to do this let us consider the automorphism φ of the field $\mathbb{Q}(u,v,w)$ given by $\varphi(u,v,w)=(u,-v,-w)$. Note that $D_{2,3}$ is fixed under the action of φ and thus we have a natural action of φ on the group $E'_2(\mathbb{Q}(u,v,w))$. It is easy to see that

$\varphi(Q_1) = -Q_1$ and $\varphi(Q_2) = Q_2$. Now let us suppose that Q_1, Q_2 are dependent. This implies that there exist nonzero integers n_1, n_2 such that $n_1Q_1 + n_2Q_2 = \mathcal{O}$ in $E_2'(\mathbb{Q}(u, v, w))$. Acting now with φ on this equality we get that $-mQ_1 + nQ_2 = \mathcal{O}$. So we deduce that $2n_2Q_2 = \mathcal{O}$ which implies that the point Q_2 is of finite order which is a contradiction. Our theorem is proved. □

Corollary 2.5. *Let $m, a, b \in \mathbb{Z}$ and consider the elliptic curves $E_1 :\ y^2 = x^3 + mx + a$, $E_2 :\ y^2 = x^3 + b$. Then the set of all $d \in \mathbb{Q}$ such that the quadratic twist of the curve E_1 by d is of positive rank and the cubic twist of the curve E_2 by d has rank ≥ 2 is infinite.*

3. Quadratic twist and two sextic twists

The aim of this section is to prove the following result.

Theorem 3.1. *Let $m, a, b, c \in \mathbb{Z}$ and consider the elliptic curves given by (1). Then there exists a rational function $D_{2,6,6} \in \mathbb{Q}(u, v, w)$ such that the quadratic twist of the curve E_1 and the sextic twists of the curves E_2, E_3 by $D_{2,6,6}(u, v, w)$ have positive rank over the field $\mathbb{Q}(u, v, w)$.*

Proof. It is clear that for our purposes we need solutions x_i, y_i of the system (3) which satisfy the condition $x_iy_i \neq 0$ for $i = 1, 2, 3$ and $f(x_1)(y_2^2 - x_2^3)(y_3^2 - x_3^3) \neq 0$.

In order to find solutions of the system (3) we make the following substitutions

$$x_1 = u, \quad x_2 = T, \quad x_3 = v^2T \quad y_1 = \frac{1}{T}, \quad y_2 = pT, \quad y_3 = qT,$$

where u, v are rational parameters and p, q, T have to be determined. After this substitution the system (3) takes the form

$$T^2 f(u) = \frac{T^2(p^2 - T)}{b} = \frac{T^2(q^2 - v^6T)}{c}. \tag{8}$$

Solving now the first and the second equation from the above system with respect to T we get that

$$T = p^2 - bf(u) = \frac{cp^2 - bq^2}{c - bv^6}.$$

We see that in order to find solutions of the system (8) we need to solve the equation

$$v^6p^2 - q^2 + (c - bv^6)f(u) = 0,$$

which define the curve, say C_2, of genus 0 with rational point at infinity $[p : q : r] = [1 : v^3 : 0]$. Using this point and the standard method of parameterization of rational points on quadrics we find that

$$p = \frac{v^6w^2 - f(u)(c - bv^6)}{2v^6w}, \quad q = \frac{-v^6w^2 - f(u)(c - bv^6)}{2v^3w}. \tag{9}$$

Using the computed value of p we find that the value of T we are looking for has the form

$$T = T(u, v, w) = \frac{v^{12}w^4 - 2f(u)v^6(c + bv^6)w^2 + f(u)^2(c - bv^6)^2}{4v^{12}w^2}$$

From the presented construction of the solutions of the system (8) and thus the system (3) we get the value of $D_{2,6,6}$ we are looking for in the form

$$D_{2,3,3}(u, v, w) = f(u)T(u, v, w)^2.$$

Using now the computed values of p, q, T we get that the point

$$P_1 = (uf(u)T(u,v,w)^2,\ f(u)^2T(u,v,w)^3)$$

lies on the curve $E_1' :\ y_1^2 = x_1^3 + aD_{2,6,6}(u,v,w)^3$ which is the quadratic twist of the curve E_1 by $D_{2,6,6}(u,v,w)$. Moreover the points

$$P_2 = (T(u,v,w),\ pT(u,v,w)),$$
$$P_3 = \left(v^2T(u,v,w),\ qT(u,v,w)\right),$$

where p, q are given by (9), lie on the curves

$$E_2' :\ y_2^2 = x_2^3 + bD_{2,6,6}(u,v,w), \quad E_2' :\ y_2^2 = x_2^3 + cD_{2,6,6}(u,v,w)$$

which are sextic twists of the curves E_2, E_3 respectively.

Using the same argument as at the end of the proof of Theorem 2.1 we deduce that the point P_i is of infinite order in the group $E_i'(\mathbb{Q}(u,v,w))$ for $i = 1,2,3$. □

Corollary 3.2. *Let $m, a, b, c \in \mathbb{Z}$ and consider the elliptic curves given by* (1). *Then the set, say $\mathcal{D}_{2,6,6}$, of all $d \in \mathbb{Q}$ such that the quadratic twist of the curve E_1 and the sextic twists of the curves E_2, E_3 by d have positive rank is dense in $\mathbb{R}$.*

Proof. From the shape of the function $D_{2,6,6}$ we see that it can be viewed as the polynomial in the variable u with coefficients in $\mathbb{Q}(v,w)$. Moreover the degree of $D_{2,6,6}$ with respect to u is 15. In order to prove our corollary let us note that if $m, a, b, c \in \mathbb{Z}$ are given then we can find the integers v_0, w_0 such that the coordinates of the point $P_i(v_0,w_0)$, obtained by specialization of the point P_i at $v = v_0, w = w_0$, are nonzero for $i = 1,2,3$. Moreover we can choose these number with such a way that the polynomial $D_{2,6,6}(u,v_0,w_0)$ is nonzero and is not a square neither a sixth power as an element of $\mathbb{Q}[u]$. Putting now $u = U^3$ we see that the genus of the curve $D_{2,6,6}(U^3,v_0,w_0) = V^{2i}$ is at least 2 for $i = 1,3$ and thus from Faltings theorem [3] we deduce that for all but finitely many $U \in \mathbb{Q}$ the point $P_i(v_0,w_0)$ is of infinite order on the curve $E_i'(v_0,w_0)$. The fact that the set $\{D_{2,6,6}(U^3,v_0,w_0) : U \in \mathbb{Q}\} \subset \mathcal{D}_{2,6,6}$ is dense in $\mathbb{Q}$ follows from the fact that degree of the polynomial $D_{2,6,6}(U^3,v_0,w_0)$ is odd. □

Example 3.3. We consider the same curves as in Example 2.3. Taking now $u = 1, v = 2, w = 2$ we find that $d = D_{2,6,6}(1,2,2) = 576$. Then from the construction presented in the Theorem 3.1 we find that the point

$$P_1 = \left(\frac{140625}{262144}, -\frac{52734375}{67108864}\right),$$

lies on the quadratic twist of E_1 by d and is of infinite order. Moreover, the points

$$P_2 = \left(-\frac{375}{1024}, -\frac{22875}{32768}\right), \quad P_3 = \left(-\frac{375}{256}, -\frac{1125}{4096}\right),$$

lie on the sextic twists of the curves E_2, E_3 by d respectively. It is clear that these points are of infinite order.

Using exactly the same argument as in the proof of the Corollary 2.4 with the same automorphism φ of the field $\mathbb{Q}(u,v,w)$ given by $\varphi(u,v,w) = (u,-v,-w)$ we get the following.

Corollary 3.4. *Let $m, a, b \in \mathbb{Z}$ and consider the elliptic curves $E_1 :\ y^2 = x^3 + mx + a,\ E_2 :\ y^2 = x^3 + b$. Then there exists a rational function $D_{2,6} \in \mathbb{Q}(u, v, w)$ with such a property that the quadratic twist of E_1 by $D_{2,6}(u, v, w)$ has positive rank and the cubic twist of E_2 by $D_{2,6}(u, v, w)$ has rank ≥ 2 over $\mathbb{Q}(u, v, w)$.*

Corollary 3.5. *Let $m, a, b \in \mathbb{Z}$ and consider the elliptic curves $E_1 :\ y^2 = x^3 + mx + a,\ E_2 :\ y^2 = x^3 + b$. Then the set of all $d \in \mathbb{Q}$ such that the quadratic twist of the curve E_1 by d is of positive rank and the sextic twist of the curve E_2 by d has rank ≥ 2 is dense in $\mathbb{R}$.*

4. Two cubic twists and a sextic twist

In this section we assume that $m = 0$, thus the curve E_1 has the equation $y^2 = x^3 + a$. This implies that the curve admit cubic twists. We prove the following.

Theorem 4.1. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves*

$$E_1 :\ y_1^2 = x_1^3 + a, \quad E_2 :\ y_2^2 = x_2^3 + b, \quad E_3 :\ y_3^2 = x_3^3 + c. \tag{10}$$

Then there exist a polynomial $D_{3,3,6} \in \mathbb{Z}[u, v, w]$ such that the cubic twists of the curves E_1, E_2 and the sextic twist of the curve E_3 by $D_{3,3,6}(u, v, w)$ have positive rank over the field $\mathbb{Q}(u, v, w)$.

Proof. It is clear that for our purposes we need solutions x_i, y_i of the system (4) which satisfy the condition $x_i y_i \neq 0$ for $i = 1, 2, 3$ and $(y_1^3 - a)(y_2^2 - b)(y_3^2 - x_3^3) \neq 0$.

In order to find solutions of the system (4) we make the following substitutions

$$x_1 = \frac{1}{T}, \quad x_2 = \frac{1}{u^2 T}, \quad x_3 = vT \quad y_1 = p, \quad y_2 = q, \quad y_3 = T,$$

where u, v are rational parameters and p, q, T have to been determined. After this substitution the system (4) takes the form

$$T^3(p^2 - a) = u^6 T^3 (q^2 - b) = \frac{T^2(1 - v^3 T)}{c}. \tag{11}$$

It is easy to see that the above system is equivalent to the following

$$p^2 - a = u^6(q^2 - b), \quad T = \frac{1}{cu^6(q^2 - b) + v^3} \tag{12}$$

The second equation is just solved and the first defines the genus zero curve, say C_3, over the field $\mathbb{Q}(u)$. It is easy to see that the curve C_3 has $\mathbb{Q}(u)$-rational point at infinity $[p : q : r] = [u^3 : 1 : 0]$. Using this point and the standard method we can parameterize the set of rational points on C_3 as follows:

$$p = \frac{w^2 + a - bu^6}{2w}, \quad q = \frac{-w^2 + a - bu^6}{2u^3 w}. \tag{13}$$

Using the computed value of q we find that the value of T we are looking for has the form

$$T = T(u, v, w) = \frac{4w^2}{cw^4 - 2(ac - 2v^3 + bcu^6)w^2 + c(a - bu^6)^2}$$

From the presented construction of the solutions of the system (8) and thus the system (3) we get the value of $D_{3,3,6}$ we are looking for in the form

$$D_{3,3,6}(u, v, w) = \frac{w^4 - 2(a + bu^6)w^2 + (a - bu^6)^2}{4w^2} T(u, v, w)^3.$$

Using now the computed values of p, q, T we get that the points

$$P_1 = ((p^2 - a)T(u,v,w)^2,\ p(p^2-a)T(u,v,w)^3),$$

$$P_2 = \left(\frac{1}{u^2}(p^2-a)T(u,v,w)^2,\ (p^2-a)qT(u,v,w)^3\right).$$

lie on the curves

$$E_1' :\ y_1^2 = x_1^3 + aD_{2,6,6}(u,v,w)^2,\ E_2' :\ y_2^2 = x_2^3 + bD_{2,6,6}(u,v,w)^2$$

which are the cubic twists of the curve E_1, E_2 respectively. Moreover, the point

$$P_3 = (vT(u,v,w),\ T(u,v,w)),$$

lies on the curve $E_3' :\ y_2^2 = x_2^3 + cD_{3,3,6}(u,v,w)$ which is the sextic twist of the curves E_3.

Using the same argument as at the end of the proof of Theorem 2.1 we deduce that the point P_i is of infinite order in the group $E_i'(\mathbb{Q}(u,v,w))$ for $i = 1, 2, 3$.

□

Using the same argument as in the proof of the Corollary 2.2 we get the following.

Corollary 4.2. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves given by* (10). *Then set, say $\mathcal{D}_{3,3,6}$, of all $d \in \mathbb{Q}$ such that the cubic twists of the curves E_1, E_2 and the sextic twist of the curve E_3 by d have positive rank is infinite.*

Example 4.3. Let us consider the following curves:

$$E_1 :\ y^2 = x^3 + 1, \quad E_2 :\ y^2 = x^3 + 6, \quad E_3 :\ y^2 = x^3 + 7.$$

One can easily check that the rank of the curve E_i is zero for $i = 1, 2, 3$. Taking now $u = 1, v = 2, w = 2$ we find that $d = D_{3,3,6}(1,2,2) = -3840/12167$. Then from the construction presented in the Theorem 4.1 we find that the points

$$P_1 = \left(-\frac{240}{529}, \frac{960}{12167}\right), \quad P_2 = \left(-\frac{240}{529}, \frac{8640}{12167}\right)$$

liea on the cubic twists of E_1, E_2 by d respectively. It is easy to see that these points are of infinite order. Moreover, the point

$$P_3 = \left(\frac{32}{23}, \frac{16}{23}\right)$$

lies on the sextic twist of the curve E_3 by d. It is clear that this point is of infinite order.

The same argument as in the proof of the Corollary 2.4 with the automorphism φ of the field $\mathbb{Q}(u,v,w)$ given by $\varphi(u,v,w) = (-u,v,-w)$ can be used in order to prove the following.

Corollary 4.4. *Let $a, b \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves $E_1 :\ y^2 = x^3 + a,\ E_2 :\ y^2 = x^3 + b$. Then there exists a rational function $D_{3,6} \in \mathbb{Q}(u,v,w)$ with such a property that the cubic twist of E_1 by $D_{2,6}(u,v,w)$ has rank ≥ 2 and the sextic twist of E_2 by $D_{2,6}(u,v,w)$ has positive rank over $\mathbb{Q}(u,v,w)$.*

Corollary 4.5. *Let $a, b \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves $E_1 :\ y^2 = x^3 + a,\ E_2 :\ y^2 = x^3 + b$. Then the set of all $d \in \mathbb{Q}$ such that the cubic twist of the curve E_1 by d has rank ≥ 2 and the sextic twist of the curve E_2 by d has positive rank is infinite.*

5. Open questions and conjectures

In this section we state some natural questions and conjectures which arises during the research.

During the course of our research we have been trying to get results concerning the existence of the simultaneous quadratic, cubic and sextic twist with positive rank of the curves E_1, E_2, E_3 given by (1). Unfortunately, without success. This leads us to the following.

Conjecture 5.1. *Let $m, a, b, c \in \mathbb{Z}$ and consider the elliptic curves (1). Then the set, say $\mathcal{D}(m, a, b, c)$, of $d \in \mathbb{Q}$ with such a property that the quadratic twist of E_1, the cubic twist of E_2 and the sextic twist of the curve E_3 by d have positive rank is infinite.*

It is clear that this conjecture will be proved if we were able to find solution of the following system of equations

$$\frac{f(x_1)}{y_1^2} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - x_3^3}{c}.$$

We check the validity of this conjecture for all $m, a, b, c \in \mathbb{Z} \setminus \{0\}$ which satisfy the condition $\max\{|m|, |a|, |b|, |c|\} \leq 5$. Moreover, it is possible to find demanded solution of the above system for some infinite families of quadruples m, a, b, c.

Example 5.2. We show that the set $\mathcal{D}(m, a, 1, 1)$ is infinite. Indeed, in order to prove this we take

$$D(u, v) = \frac{f(u)(f(u) - v^2)^4}{16v^4},$$

and then we have the following pairs of points and curves:

$$\begin{array}{ll} E^2 : \; y^2 = x^3 + mD(u,v)^2 + aD(u,v)^3, & P = \left(u, \; q(u,v)^2\right), \\ E^3 : \; y^2 = x^3 + D(u,v)^2, & Q = \left(q(u,v)^2, \; (u,v)\right), \\ E^6 : \; y^2 = x^3 + D(u,v), & R = \left(\frac{1}{q(u,v)^2}, \; \frac{p(u,v)}{q(u,v)^3}\right), \end{array}$$

where

$$p(u, v) = \frac{f(u) + v^2}{f(u) - v^2}, \quad q(u, v) = \frac{2v}{f(u) - v^2}.$$

It is clear that the points P, Q, R are of infinite order and the argument similar to the one used in the proof of the Corollary 3.2 leads to the conclusion that the set $\mathcal{D}(a, 1, 1)$ is in fact dense in $\mathbb{R}$ (note that $D(u, v)$ is the polynomial in variable u and that $\deg_u D(u, v)$ is odd).

After getting the above example we hoped that the Conjecture 5.1 could be proved in the case when $m = 0, a = b = c$. Although we are trying quite hard to get the result in this case we failed. We believe that this case is of independent interest and in order to emphasize this we state the following.

Conjecture 5.3. *Let $a \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curve $E : \; y^2 = x^3 + a$. Then the set of $d \in \mathbb{Q}$ with such a property that the quadratic, cubic and the sextic twist of the curve E by d has positive rank is infinite.*

The last combination of three twists which we considered was three cubic twists. Unfortunately, also in this case we are unable to get general result. However, we believe that the following is true.

Conjecture 5.4. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves* (10)*. Then the set of those $d \in \mathbb{Q}$ with such a property that the cubic cubic twist of the curve E_i by d has positive rank for $i = 1, 2, 3,$ is infinite.*

The corresponding system of equations in this case has the following form:

$$\frac{y_1^2 - a}{x_1^3} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - c}{x_3^3}. \tag{14}$$

We prove that the above system has rational parametric solution in case when a, b, c are squares, say a^2, b^2, c^2, in $\mathbb{Z}$. In order to get the result we put

$$x_1 = 1, \quad x_2 = x_3 = \frac{1}{u^2}.$$

Then our system is equivalent with the following

$$y_1^2 - u^6 y_2^2 = a^2 - u^6 b^2, \quad u^6 y_2^2 - v^6 y_3^2 = u^6 b^2 - v^6 c^2.$$

From geometric point of view the above system is an intersection of two quadratic surfaces defined over the field $\mathbb{Q}(u)$ with a rational point $P = (y_1, y_2, y_2) = (a, b, c)$ and thus defines an elliptic curve, say C. Using the chord and tangent law of addition of points on C we can compute the point $2P = (y_1, y_2, y_3)$. Because the computations are rather lengthy and tiresome we omit it and give only the final form of y_i for $i = 1, 2, 3$. We have

$$y_1 = -\frac{a(a^4(b^2 - c^2)^2 + 2a^2b^2c^2(b^2 + c^2)u^6 - 3b^4c^4u^{12})}{(a(c-b) - bcu^3)(a(b+c) - bcu^3)(a(c-b) + bcu^3)(a(b+c) + bcu^3)},$$
$$y_2 = \frac{b(a^4(b^2 - c^2)(b^2 + 3c^2) - 2a^2b^2c^2(b^2 - c^2)u^6 + b^4c^4u^{12})}{(a(c-b) - bcu^3)(a(b+c) - bcu^3)(a(c-b) + bcu^3)(a(b+c) + bcu^3)},$$
$$y_3 = \frac{c(-a^4(b^2 - c^2)(3b^2 + c^2) + 2a^2b^2c^2(b^2 - c^2)u^6 + b^4c^4u^{12})}{(a(c-b) - bcu^3)(a(b+c) - bcu^3)(a(c-b) + bcu^3)(a(b+c) + bcu^3)},$$

and the common value $D_{3,3,3} \in \mathbb{Q}(u)$ of the quantities defining the system (14) in our case has the form

$$D_{3,3,3}(u) = \frac{8a^2b^2c^2u^6(a^2(b^2 - c^2) - b^2c^2u^6)(a^2(b^2 + c^2) - b^2c^2u^6)(a^2(b^2 - c^2) + b^2c^2u^6)}{(a(c-b) - bcu^3)^2(a(b+c) - bcu^3)^2(a(c-b) + bcu^3)^2(a(b+c) + bcu^3)^2}.$$

From our computations we deduce that on each of the curves

$$E_1' : \ y^2 = x^3 + a^2 D_{3,3,3}^2, \quad E_2' : \ y^2 = x^3 + b^2 D_{3,3,3}^2, \quad E_3' : \ y^2 = x^3 + c^2 D_{3,3,3}^2,$$

we have the point

$$P_1 = (D_{3,3,3}, \ D_{3,3,3}y_1), \quad P_2 = \left(\frac{D_{3,3,3}}{u^2}, \ D_{3,3,3}y_2\right), \quad P_3 = \left(\frac{D_{3,3,3}}{u^2}, \ D_{3,3,3}y_3\right),$$

respectively, where y_1, y_2, y_3 are given above. From the shape of the point P_i we deduce that it is of infinite order on the curve E_i' for $i = 1, 2, 3$.

We have thus proved

Theorem 5.5. *The Conjecture 5.4 is true if the curve E_i is the cubic twist of the curve $E : \ y^2 = x^3 + 1$ for $i = 1, 2, 3$.*

References

[1] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts 24, Cambridge University Press, 1991.

[2] I. Connell, APECS: Arithmetic of Plane Elliptic Curves, avaliable from `ftp.math.mcgill.ca/pub/apecs/`.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349-366.

[4] M. Kuwata, L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Int. Math. Research Notices, **4** (1993), 113-123.

[5] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[6] M. Ulas, *A note on higher twists of elliptic curves*, Glasgow Math. J. **52**d (2010) 371-381.

[7] M. Ulas, *Variations on higher twists of pairs of elliptic curves*, Int. J. Number Theory 6(5) (2010), 1169-1182.

Maciej Ulas, Institute of Mathematics of the Polish Academy of Sciences, ul. Śniadeckich 8, 00-956 Warszawa, Poland

and

Jagiellonian University, Institute of Mathematics, Łojasiewicza 6, 30-348 Kraków, Poland;

E-mail adress: `maciej.ulas@uj.edu.pl, Maciej.Ulas@im.uj.edu.pl`