ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 43, Number 2, 2013

VARIATIONS ON TWISTS 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 the j-invariants of the curves E_2, E_3 are equal to 0, there exist rational functions $D_{2,3,3}$, $D_{2,6,6} \in \mathcal{Q}(u,v,w)$ with the following properties:

- 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 $\mathcal{Q}(u,v,w)$,
- 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 $\mathcal{Q}(u,v,w)$.

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

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 a polynomial D such that the quadratic twist $E_{i,D}$ of the curve E_i by D has positive rank for $i = 1, 2$. Their method cannot be used in the case when $j(E_1) = j(E_2) = j$, for $j = 0, 1728$. Unfortunately, we are unable to show that in these cases it is also possible to 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, that elliptic curves with the j-invariant equal to 0 or, in other words, curves of the form $E : y^2 = x^3 + p$, also have 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 $y^2 = x^3 + pD$.

2010 AMS *Mathematics subject classification.* Primary 11G05.
Keywords 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).
Received by the editors on May 29, 2010, and in revised form on July 25, 2010.
DOI:10.1216/RMJ-2013-43-2-645

In a recent paper [**6**] we proved that for any quadruple of pairwise distinct elliptic curves E_i, $i = 1, 2, 3, 4$, with the j-invariant 0 there exists a polynomial $D \in \mathbf{Z}[u]$ 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 them E_1, E_2 with $j = 0$ there exists 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 $m, a, b, c \in \mathbf{Z}$ and consider the elliptic curves

$$\begin{aligned} E_1 &: \ y_1^2 = x_1^3 + mx_1 + a, \\ E_2 &: \ y_2^2 = x_2^3 + b, \\ E_3 &: \ y_3^2 = x_3^3 + c, \end{aligned} \tag{1}$$

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

- 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 $\mathcal{Q}(u, v, w)$,
- 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 $\mathcal{Q}(u, v, w)$.

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

Let us define $f(x) = x^3 + mx + a$ and note that, in order to find the required 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 the case of a quadratic twist and two cubic twists, then

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

in the 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 the case of two cubic twists and a sextic twist.

In order to prove our results, we will construct a 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-known classification of possible torsion subgroups of the rational elliptic curve $E : y^2 = x^3 + q$, where $q \in \mathcal{Q}$ 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 curve E by $D \in \mathcal{Q}(t_1, \ldots, t_m) \setminus \mathcal{Q}$ and on the curve E' we have a $\mathcal{Q}(t_1, \ldots, t_m)$-rational point $P = (x, y)$ with $xy \neq 0$ for some $m \in \mathbf{Z}_+$, then the order of the point P in the group $E'(\mathcal{Q}(t_1, \ldots, t_m))$ is not finite, provided that E' is not isomorphic to an elliptic curve defined over $\mathcal{Q}$. Thus, the curve E' defined over $\mathcal{Q}(t_1, \ldots, t_m)$ has positive rank. It is clear that exactly the same argument works for the cubic twists of the curve E.

2. Quadratic twist and two cubic twists. The aim of this section is to prove the following result.

Theorem 2.1. *Let $m, a, b, c \in \mathbf{Z}$, and consider the elliptic curves given by* (1). *Then there exists a rational function $D_{2,3,3} \in \mathcal{Q}(u, v, w)$ 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 $\mathcal{Q}(u, v, w)$.*

Proof. It is clear that for our purposes we need solutions x_i, y_i of system (2) which satisfy the conditions $x_i y_i \neq 0$ 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 system (2), we make the following substitutions:

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

where u, v are rational parameters and p, q, T have to be determined. After this substitution, 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 one:

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

The first equation is just solved, the second can be interpreted as a quadratic equation with coefficients in the field $\mathcal{Q}(v)$. So this equation defines a genus zero curve, say C_1, over the field $\mathcal{Q}(v)$. It is easy to see that curve C_1 has a $\mathcal{Q}(v)$-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:

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

where w is a rational parameter. Using the computed value of p we find that the T from the system (2) takes the form

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

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

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

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

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

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

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

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 $m, a, b, c \in \mathbf{Z}$. Moreover, it is easy to see that the rational function $D_{2,3,3}^j$ for $j = 2, 3$ is not of the form $AF(u,v,w)^6$, where $A \in \mathcal{Q}$ and $F \in \mathcal{Q}(u,v,w)$, which implies that the curve E_i' is not isomorphic to the one defined over $\mathcal{Q}$. 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 $E_i'(\mathcal{Q}(u,v,w))$ for $i = 2, 3$. □

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

Corollary 2.2. *Let $m, a, b, c \in \mathbf{Z}$, and consider the elliptic curves given by* (1). *Then the set, say $\mathcal{D}_{2,3,3}$, of all $d \in \mathcal{Q}$ 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 $m, a, b, c \in \mathbf{Z}$, there exist infinitely many integers u_0, v_0, w_0 for which 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 nor a cube in $\mathcal{Q}$. This proves that the set $\mathcal{D}_{2,3,3}$ is infinite. □

Example 2.3. Let us consider the following elliptic curves:

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

One can easily check using the 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 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

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

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 $m, a, b \in \mathbf{Z}$, 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 $D_{2,3} \in \mathcal{Q}(u, v, w)$ for which 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 $\mathcal{Q}(u, v, w)$.*

Proof. In order to define the required function, we make the substitution $c = b$ in the function $D_{2,3,3}$. As $D_{2,3}$ we take the result of this substitution. Now let us note that on the curve E_1' which is the quadratic twist of E_1 by $D_{2,3}(u, v, w)$, we have a point P coming 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 come from points P_2, P_3 lying 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 now show that the points Q_1, Q_2 are independent in the group $E_2'(\mathcal{Q}(u, v, w))$. In order to do this, let us consider the automorphism ϕ of the field $\mathcal{Q}(u, v, w)$ given by $\phi(u, v, w) = (u, -v, -w)$. Note that

$D_{2,3}$ is fixed under the action of ϕ, and thus we have a natural action of ϕ on the group $E_2'(\mathcal{Q}(u,v,w))$. It is easy to see that $\phi(Q_1) = -Q_1$ and $\phi(Q_2) = Q_2$. 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 $E_2'(\mathcal{Q}(u,v,w))$. Now acting 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 $m, a, b \in \mathbf{Z}$, 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 $d \in \mathcal{Q}$ 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 $m, a, b, c \in \mathbf{Z}$, and consider the elliptic curves given by* (1). *Then there exists a rational function $D_{2,6,6} \in \mathcal{Q}(u,v,w)$ 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 $\mathcal{Q}(u,v,w)$.*

Proof. It is clear that for our purposes we need solutions x_i, y_i of system (3) satisfying the conditions $x_iy_i \neq 0$ 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 system (3) we make the following substitutions

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

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

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

Now solving 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 system (8), we need to solve the equation

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

which defines a curve, say C_2, of genus 0 with the 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

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

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

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

Now using 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

$$\begin{aligned} P_2 &= (T(u, v, w),\ pT(u, v, w)), \\ P_3 &= \left(v^2T(u, v, w),\ qT(u, v, w)\right), \end{aligned}$$

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

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

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 point P_i is of infinite order in the group $E_i'(\mathcal{Q}(u, v, w))$ for $i = 1, 2, 3$. □

Corollary 3.2. *Let $m, a, b, c \in \mathbf{Z}$, and consider the elliptic curves given by* (1). *Then the set, say $\mathcal{D}_{2,6,6}$, of all $d \in \mathcal{Q}$ 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 $\mathbf{R}$.*

Proof. From the shape of the function $D_{2,6,6}$ we see that it can be seen as a polynomial in the variable u with coefficients in $\mathcal{Q}(v, w)$. 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 $m, a, b, c \in \mathbf{Z}$ are given, then we can find 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 numbers in such a way that the polynomial $D_{2,6,6}(u, v_0, w_0)$ is nonzero and is neither a square nor a sixth power as an element of $\mathcal{Q}[u]$. Now putting $u = U^3$, 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 the Faltings theorem [**3**] we deduce that for all but finitely many $U \in \mathcal{Q}$ 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 $\{D_{2,6,6}(U^3, v_0, w_0) : U \in \mathcal{Q}\} \subset \mathcal{D}_{2,6,6}$ is dense in $\mathcal{Q}$ follows from the fact that the 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. Now taking $u = 1$, $v = 2$, $w = 2$ we find that $d = D_{2,6,6}(1, 2, 2) = 576$. Then from the construction presented in 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

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

lie on the sextic twists of 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 Corollary 2.2 with the same automorphism ϕ of field $\mathcal{Q}(u, v, w)$ given by $\phi(u, v, w) = (u, -v, -w)$, we get the following.

Corollary 3.4. *Let $m, a, b \in \mathbf{Z}$, 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 $D_{2,6} \in \mathcal{Q}(u, v, w)$ for which 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 $\mathcal{Q}(u, v, w)$.*

Corollary 3.5. *Let $m, a, b \in \mathbf{Z}$, 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 $d \in \mathcal{Q}$ 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 $\mathbf{R}$.*

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 admits cubic twists. We prove the following.

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

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

Then there exists a polynomial $D_{3,3,6} \in \mathbf{Z}[u, v, w]$ 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 $\mathcal{Q}(u, v, w)$.

Proof. It is clear that, for our purposes, we need solutions x_i, y_i of 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 system (4), we make the following substitutions

$$\begin{aligned} x_1 &= \frac{1}{T}, \qquad x_2 = \frac{1}{u^2 T}, \qquad x_3 = vT \\ y_1 &= p, \qquad y_2 = q, \qquad y_3 = T, \end{aligned}$$

where u, v are rational parameters and p, q, T have to been determined. After this substitution, 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 one:

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

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

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

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

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

Now using 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

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

which are cubic twists of curves 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 curve E_3.

Using the same argument as at the end of the proof of Theorem 3.1, we deduce that point P_i is of infinite order in the group $E_i'(\mathcal{Q}(u,v,w))$ for $i = 1,2,3$. □

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

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

Example 4.3. Let us consider the following curves:

$$E_1 : \mathbf{Y}^2 = x^3 + 1, \qquad E_2 : y^2 = x^3 + 6, \qquad E_3 : y^2 = x^3 + 7.$$

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

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

lie 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 curve E_3 by d. It is clear that this point is of infinite order.

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

Corollary 4.4. *Let $a, b \in \mathbf{Z} \setminus \{0\}$, 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 $D_{3,6} \in \mathcal{Q}(u, v, w)$ with the 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 $\mathcal{Q}(u, v, w)$.*

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

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

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

It is clear that this conjecture would be proved if we were able to find the 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 checked the validity of this conjecture for all $m, a, b, c \in \mathbf{Z} \setminus \{0\}$ which satisfies the condition $\max\{|m|, |a|, |b|, |c|\} \leq 5$. Moreover, it is possible to find a 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:

$$E^2 : D(u,v)u^2 = x^3 + mx + a,$$
$$E^3 : y^2 = x^3 + D(u,v)^2,$$
$$E^6 : y^2 = x^3 + D(u,v),$$

$$P = \left(u, \frac{1}{p(u,v)^2}\right),$$
$$Q = (f(u)p(u,v)^2, f(u)p(u,v)^3 q(u,v)),$$
$$R = (q(u,v)^2, p(u,v)^2 q(u,v)),$$

where

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

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 Corollary 3.2 leads to the conclusion that the set $\mathcal{D}(a,1,1)$ is in fact dense in $\mathbf{R}$ (note that $D(u,v)$ is a polynomial in the variable u and that $\deg_u D(u,v)$ is odd).

After having obtained the example above, we hoped that Conjecture 5.1 could be proved in the case when $m = 0, a = b = c$. Although we were 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 $a \in \mathbf{Z} \setminus \{0\}$, and consider the elliptic curve $E : y^2 = x^3 + a$. Then the set of $d \in \mathcal{Q}$ with the property that the quadratic, cubic and sextic twists of curve E by d have 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 a general result. However, we believe that the following is true.

Conjecture 5.4. *Let $a, b, c \in \mathbf{Z}\setminus\{0\}$, and consider the elliptic curves (10). Then the set of those $d \in \mathcal{Q}$ with the property that the cubic twist of 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 a rational parametric solution in the cases where a,b,c are squares, say a^2,b^2,c^2, in $\mathbf{Z}$. In order to get the result, we put

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

Then our system is equivalent to the following:

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

From the geometric point of view the above system is an intersection of two quadratic surfaces defined over the field $\mathcal{Q}(u)$ 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 long and tiresome we omit them and give only the final form of y_i for $i=1,2,3$. We have

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

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

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

From our computations we deduce that, on each of the curves

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

we have the point

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

respectively, where y_1, y_2, y_3 are given above. From the form of 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. *Conjecture* 5.4 *is true if curve* E_i *is the cubic twist of the curve* $E : y^2 = x^3 + 1$ *for* $i = 1, 2, 3$.

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.

REFERENCES

1. J.W.S. Cassels, *Lectures on elliptic curves*, London Math. Soc. Student Texts **24**, Cambridge University Press, Cambridge, 1991.

2. I. Connell, APECS: *Arithmetic of plane elliptic curves*, available 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 and 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** (2010), 371–381.

7. ———, *Variations on higher twists of elliptic curves*, Int. J. Number Theory **6** (2010), 1183–1189.

Jagiellonian University, Faculty of Mathematics and Computer Science, Institute of Mathematics, Łojasiewicza 6, 30-348 Kraków, Poland
Email address: maciej.ulas@uj.edu.pl