A NOTE ON HIGHER TWISTS OF ELLIPTIC CURVES

MACIEJ ULAS

Institute of Mathematics of the Polish Academy of Sciences, Śniadeckich 8,
00-956 Warszawa, Poland
Jagiellonian University, Institute of Mathematics, Łojasiewicza 6, 30-348 Kraków, Poland
e-mail: maciej.ulas@uj.edu.pl

Abstract. We show that for any pair of elliptic curves E_1, E_2 over $\mathbb{Q}$ with j-invariant equal to 0, we can find a polynomial $D \in \mathbb{Z}[u, v]$ such that the cubic twists of the curves E_1, E_2 by $D(u, v)$ have positive rank over $\mathbb{Q}(u, v)$. We also prove that for any quadruple of pairwise distinct elliptic curves E_i, $i = 1, 2, 3, 4$, with j-invariant $j = 0$, there exists a polynomial $D \in \mathbb{Z}[u]$ such that the sextic twists of E_i, $i = 1, 2, 3, 4$, by $D(u)$ have positive rank. A similar result is proved for quadruplets of elliptic curves with j-invariant $j = 1, 728$.

2000 *Mathematics Subject Classification.* 11G05.

1. Introduction. Kuwata and Wang [1] considered an elliptic surface $\mathcal{E}$ given by the equation

$$\mathcal{E} : \left(x_1^3 + ax_1 + b\right)y^2 = x_2^3 + cx_2 + d,$$

where $a, b, c, d \in \mathbb{Z}$ fulfill the following condition:

$$(a \neq 0 \quad \text{or} \quad c \neq 0) \quad \text{and} \quad (b \neq 0 \quad \text{or} \quad d \neq 0).$$

They proved that the set $\mathcal{E}(\mathbb{Q})$ of rational points on $\mathcal{E}$ is dense in the Euclidean topology in the set $\mathcal{E}(\mathbb{R})$ of all real points on $\mathcal{E}$. This result was deduced from the existence of a specific rational curve L on $\mathcal{E}$ (it should be noted that the curve had already been obtained by Mestre in [2]). As a corollary, from the existence of the curve L, they deduced that if E_1, E_2 are elliptic curves and their j-invariants are not equal to 0 or 1,728 simultaneously, then there exists a polynomial $D \in \mathbb{Z}[t]$ such that the quadratic twists $E_{1, D}$, $E_{2, D}$ of the curves by D have positive rank. Their method cannot be used in the case when $j(E_1) = j(E_2) = j$, where $j = 0, 1, 728$. Unfortunately, we are also unable to show that in these cases one can construct quadratic twists of pairs of elliptic curves with a positive rank. It is known that each elliptic curve has a quadratic twist. However, it is well also known that elliptic curves with 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 form $E_D : y^2 = x^3 + pD^2$. The sextic twist of the curve E by D has the form $E_D : y^2 = x^3 + pD$.

In the case of elliptic curves with $j = 1, 728$ or, in other words, curves of the form $E' : y^2 = x^3 + px$, there is one additional twist, the so-called quartic twist. The quartic twist of the curve E' by D has the form $E'_D : y^2 = x^3 + pDx$.

Therefore, in view of the results of Kuwata and Wang, it is natural to state the following.

QUESTION 1.1. *Let E_1, E_2 be elliptic curves with $j(E_1) = j(E_2) = 0$. Is it possible to find a polynomial $D \in \mathbb{Z}[t]$ such that the cubic twists of E_1, E_2 by D have positive rank?*

Similarly, we can ask the following.

QUESTION 1.2. *Let $E_1, E_2, \ldots, E_n$ be elliptic curves with $j(E_i) = 0$ for $i = 1, 2, \ldots, n$ and suppose that $E_i \neq E_j$ for $i \neq j$. What is the maximal number $n = M_6(0)$ for which there exists a polynomial $D \in \mathbb{Z}[t]$ such that the sextic twists of E_i, for $i = 1, 2, \ldots, n$, by D have positive rank?*

QUESTION 1.3. *Let $E_1, E_2, \ldots, E_n$ be elliptic curves with $j(E_i) = 1,728$ for $i = 1, 2, \ldots, n$ and suppose that $E_i \neq E_j$ for $i \neq j$. What is a maximal number $n = M_4(1,728)$ for which there exists a polynomial $D \in \mathbb{Z}[t]$ such that the quartic twists of E_i, for $i = 1, 2, \ldots, n$, by D have positive rank?*

Mestre [2] proved that for a given curve E with j-invariant $j = 0$ (resp. with j-invariant $j = 1,728$), there is a polynomial $D(t)$ such that the sextic twist (resp. quartic twist) of the curve E by $D(t)$ has $\mathbb{Q}(t)$ rank equal to 6 (resp. 4). This results may suggest that $M_6(0) \geq 6$ and $M_4(1728) \geq 4$. As we will see, this prediction is true for quartic twists (Theorem 3.1). Unfortunately, we are unable to prove that this is the case for sextic twists. However, we are able to prove that $M_6(0) \geq 4$ (Theorem 2.3). We also proved that the answer to the question (1.1) is positive (first part of Theorem 2.1) and show that in order to find simultaneous cubic twists of three elliptic curves with j-invariant $j = 0$, it is enough to find an elliptic curve with positive rank in some family of elliptic curves depending on two rational parameters (the second part of Theorem 2.1).

2. Cubic and sextic twists.

In this section we are interested in the construction of cubic and sextic twists of pairs and triples of elliptic curves with j-invariant $j = 0$. Let us recall how a torsion part of the curve $E : y^2 = x^3 + q$ looks like with a fixed $q \in \mathbb{Z}$ [4, p. 323]. If $q = 1$, then $Tors E \cong \mathbb{Z}/6\mathbb{Z}$. If $q \neq 1$ and q is a square in $\mathbb{Z}$, then $Tors E = \{\mathcal{O}, (0, \sqrt{q}), (0, -\sqrt{q})\}$. In case when $q = -432$, we have $Tors E = \{\mathcal{O}, (12, 36), (12, -36)\}$. If $q \neq 1$ and q is a cube in $\mathbb{Z}$, then $Tors E = \{\mathcal{O}, (-\sqrt[3]{q}, 0)\}$. In the remaining cases we have $Tors E = \{\mathcal{O}\}$. As an immediate consequence we obtain that if $E_D : y^2 = x^3 + qD$ is a sextic twist of the curve E by $D \in \mathbb{Z}[t] \setminus \mathbb{Z}$ and on the curve E_D we have a $\mathbb{Q}(t)$ rational point $P = (x, y)$ with $xy \neq 0$, then the order of the point P in the group $E_D(\mathbb{Q}(t))$ is not finite. Thus, the curve E_D over $\mathbb{Q}(t)$ has positive rank.

Now we are ready to prove the following theorem.

THEOREM 2.1.
(1) *Let $a, b \in \mathbb{Z} \setminus \{0\}$ and suppose $a \neq b$. Consider the elliptic curves $E_1 : y_1^2 = x_1^3 + a$, $E_2 : y_2^2 = x_2^3 + b$. Then there exists a polynomial $D \in \mathbb{Z}[u, v]$ such that the cubic twist of E_i by D has positive rank for $i = 1, 2$.*
(2) *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and suppose that these numbers are pairwise distinct. Suppose that there exists rational numbers u, v such that the set of rational points on the curve*

$$\mathcal{E}(a, b, c) : Y^2 = X(v^3 X - 1)((av^6 - bu^6)X + v^3(cu^6 - a))$$

is infinite. Then the set of those numbers D, for which the cubic twists of elliptic curves

$$E_1 : y_1^2 = x_1^3 + a, \ E_2 : y_2^2 = x_2^3 + b, \ E_3 : y_3^2 = x_3^3 + c$$

by D have positive rank is infinite.

Proof. In order to prove our theorem we will construct rational curves on hypersurface $\mathcal{U}$ given by the system of equations

$$\mathcal{U} : D^2 = \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b}.$$

Let us consider the second equation in the system defining the hypersurface $\mathcal{U}$ and let $\mathcal{U}'$ be the hypersurface defined by this equation, i.e.

$$\mathcal{U}' : \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b}.$$

Let $F(x_1, y_1, x_2, y_2) = b(y_1^2 - x_1^3) - a(y_2^2 - x_2^3)$.

We will show that the hypersurface $\mathcal{U}'$ is birationally equivalent to $\mathbb{A}^3$. In order to prove this, let us put

$$x_1 = pT, \quad y_1 = qT, \quad x_2 = rT, \quad y_2 = T. \tag{1}$$

For x_i, y_i defined in this way, we have

$$F(x_1, y_1, x_2, y_2) = T^2((ar^3 - bp^3)T - (a - bq^2)).$$

By solving this equation with respect to T, we get a double root $T = 0$ and another one given by

$$T = \frac{a - bq^2}{ar^3 - bp^3} =: \lambda(p, q, r).$$

Let $S = \{(p, \ q, \ r) \in \mathbb{A}^3 : ar^3 - bp^3 = 0\}$ be the set where the function λ is not defined. By the definition of λ, we get a rational function $\Lambda : \mathbb{A}^3 \setminus S \to \mathcal{U}'$ given by

$$\Lambda : \mathbb{A}^3 \setminus S \ni (p, \ q, \ r) \mapsto (p\lambda(p, \ q, \ r), \ q\lambda(p, \ q, \ r), \ r\lambda(p, \ q, \ r), \ \lambda(p, \ q, \ r)) \in \mathcal{U}'.$$

Now define $S' = \{(x_1, \ y_1, \ x_2, \ y_2) \in \mathcal{U}' : y_2 = 0\}$. Then for the rational function $\Theta : \mathcal{U}' \setminus S' \to \mathbb{A}^3$ given by

$$\Theta : \mathcal{U}' \setminus S' \ni (x_1, \ y_1, \ x_2, \ y_2) \mapsto \left(\frac{x_1}{y_2}, \ \frac{y_1}{y_2}, \ \frac{x_2}{y_2} \right) \in \mathbb{A}^3$$

we have $\Theta \circ \Lambda = id_{\mathbb{A}^3 \setminus S}$ and $\Lambda \circ \Theta = id_{\mathcal{U}' \setminus S'}$. These equalities imply that the hypersurface $\mathcal{U}'$ is birationally equivalent to $\mathbb{A}^3$.

For x_1, y_1, x_2, y_2 defined by (1), where $T = \lambda(p, q, r)$, we have

$$\frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b} = \frac{(a - bq^2)^2(p^3 - q^2 r^3)}{(ar^3 - bp^3)^3}.$$

Now, using the above parametrization of the set of rational points on the hypersurface $\mathcal{U}'$ and the equality above, we can see that constructing rational points on the hypersurface $\mathcal{U}$ is equivalent to constructing rational points on the threefold given by the equation

$$h^2 = (p^3 - q^2 r^3)(ar^3 - bp^3). \tag{2}$$

In order to find rational points on the above hypersurface, we put $p = u^2$ and $r = 1$, where u is an indeterminate. Then the equation (2) defines a quadratic curve, say C_3, over the field $\mathbb{Q}(u)$ with a $\mathbb{Q}(u)$-rational point $(q, h) = (u^3, 0)$. Using standard method we find a parametrization of rational points on quadric C_3 given by

$$q = -\frac{u^3(1 + (a - bu^6)v^2)}{1 - (a - bu^6)v^2}, \quad h = \frac{2u^3(a - bu^6)v}{1 - (a - bu^6)v^2}.$$

Using these expressions and performing all the necessary calculations, we can define the following polynomial $D \in \mathbb{Z}[u, v]$:

$$D(u, v) = 2v(1 - 2(a + bu^6)v^2 + (a - bu^6)^2 v^4).$$

Now, after some necessary computations and simplifications we can see that on the curves

$$E_{1, D} : y_1^2 = x_1^3 + aD(u, v)^2, \quad E_{2, D} : y_2^2 = x_2^3 + bD(u, v)^2,$$

which are cubic twists of the curves E_1 and E_2 respectively, we have $\mathbb{Q}(u, v)$-rational points given by

$$P_1 = (x_1, y_1) = \left(\frac{D(u, v)}{2v}, \ (1 + (a - bu^6)v^2)\frac{D(u, v)}{2v} \right),$$
$$P_2 = (x_2, y_2) = \left(\frac{D(u, v)}{2u^2 v}, \ (1 - (a - bu^6)v^2)\frac{D(u, v)}{2u^3 v} \right).$$

From the remark presented at the beginning of this section, the point P_i has infinite order on the curve $E_{i, D}$ for $i = 1, 2$. This conclusion finishes the proof of the first part of the theorem.

In order to prove the second part of the theorem, we consider a hypersurface

$$\mathcal{V} : D^2 = \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c}.$$

Let us consider a hypersurface $\mathcal{V}'$ defined by the equations

$$\mathcal{V}' : \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c}.$$

In order to find rational curves on $\mathcal{V}'$, let us put

$$x_1 = u^2 T, \ y_1 = pT, \quad x_2 = v^2 T, \ y_2 = qT, \quad x_3 = T, \ y_3 = rT$$

and take $F(x, y) = y^2 - x^3$. Note that if $T = (-bp^2 + aq^2)/(-bu^6 + av^6) =: f_1(p, q)$, then the first equation defining $\mathcal{V}'$ is satisfied. On the other hand, if $T = (-cq^2 + br^2)/(b - cv^6) =: f_2(q, r)$, then the second equation defining $\mathcal{V}'$ is satisfied. From this

reasoning we see that in order to find rational points on $\mathcal{V}'$ it is enough to show that the quadric

$$Q: \frac{-bp^2 + aq^2}{-bu^6 + av^6} = \frac{-cq^2 + br^2}{b - cv^6},$$

defined over the field $\mathbb{Q}(u, v)$, has infinitely many rational points. On Q we have the $\mathbb{Q}(u, v)$-rational point $[p : q : r] = [u^3 : v^3 : 1]$. Using a standard method we find a rational parametrization of $\mathbb{Q}(u, v)$-rational points on the quadric Q

$$p = u^3(-a + cu^6 + (-bu^6 X^2 + av^6)X^2),$$
$$q = (a - cu^6)v^3 + 2(bu^6 - av^6)X + (-bu^6 + av^6)v^3 X^2,$$
$$r = a - cu^6 - 2(a - cu^6)v^3 X + (-bu^6 + av^6)X^2.$$

For p, q, r defined above, we get $T = T(X) := f_1(p, q) = f_2(p, q)$ and thus

$$\frac{F(u^2 T, pT)}{a} = \frac{F(v^2 T, qT)}{b} = \frac{F(T, rT)}{c}$$
$$= X(v^3 X - 1)((av^6 - bu^6)X + v^3(cu^6 - a))(2u^3 T(X))^2.$$

Therefore, under our assumption we can find $u, v \in \mathbb{Q}$ such that the set of rational points on the curve $\mathcal{E}(a, b, c)$ is infinite, and then we can find an infinite set of rational numbers, say $\mathcal{D}$, such that for each $D \in \mathcal{D}$, the cubic twist of the elliptic curve E_i by D has positive rank for $i = 1, 2, 3$. $\qquad \square$

From the first part of our theorem, we get an interesting corollary which is as follows.

COROLLARY 2.2. *Let* $a, b \in \mathbb{Z} \setminus \{0\}$ *and consider elliptic curves* $E_1: y_1^2 = x_1^3 + a$, $E_2: y_2^2 = x_2^3 + b$ *and let us denote by* $E_{i,D}$ *the cubic twist of the curve* E_i *by* D *for* $i = 1, 2$. *Then the set*

$$\mathcal{A} := \{D \in \mathbb{Q}: \text{the curves } E_{1, D}, E_{2, D} \text{ have positive rank over } \mathbb{Q}\}$$

is dense in $\mathbb{R}$.

Proof. This is a simple consequence of the fact that degree of the polynomial $D \in \mathbb{Z}[u, v]$ (with respect to v) constructed in the first part of the previous theorem is odd. $\qquad \square$

Now, we state and prove theorem concerning the existence of twists of positive rank for four elliptic curves with j-invariant $j = 0$. More precisely, we prove the following.

THEOREM 2.3. *Let* $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ *be pairwise distinct and consider the elliptic curves*

$$E_1: y_1^2 = x_1^3 + a, \quad E_2: y_2^2 = x_2^3 + b, \quad E_3: y_3^2 = x_3^3 + c, \quad E_4: y_4^2 = x_4^3 + d.$$

Then there exists a polynomial $D \in \mathbb{Z}[u]$ *such that the sextic twist of the elliptic curve* E_i *by* $D(u)$ *has positive* $\mathbb{Q}(u)$-*rank for* $i = 1, 2, 3, 4$. *Thus, the constant defined in Question* 1.2 *satisfies* $M_6(0) \geq 4$.

Proof. We will show that the set of rational curves on the hypersurface

$$\mathcal{V}_6 : \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c} = \frac{y_4^2 - x_4^3}{d}$$

is nonempty. It is clear that we are interesting in nontrivial rational curves only, i.e. a curves $L : x_i = f_i(u)$, $y_i = g_i(u)$ which satisfy the condition $y_i^2 - x_i^3 \neq 0$ for $i = 1, 2, 3, 4$.

Let us put

$$x_1 = u^2 T, \quad x_2 = x_3 = x_4 = T, \quad y_1 = pT, \quad y_2 = qT, \quad y_3 = rT, \quad y_4 = sT. \quad (3)$$

Now, let us note that if $T = (-bp^2 + aq^2)/(a - bu^6) =: f_1(p, q)$, then the first equation defining the hypersurface $\mathcal{V}_6$ is satisfied. On the other hand, if $T = (-cq^2 + br^2)/(b - c) =: f_2(q, r)$, then the second equation defining the hypersurface $\mathcal{V}_6$ is satisfied, and finally if $T = (-dr^2 + cs^2)/(c - d) =: f_3(r, s)$, then the third equation defining the hypersurface $\mathcal{V}_6$ is satisfied. Hence, it is enough to show that the system of equations

$$\frac{-bp^2 + aq^2}{a - bu^6} = \frac{-cq^2 + br^2}{b - c} = \frac{-dr^2 + cs^2}{c - d}$$

has nontrivial $\mathbb{Q}(u)$-rational solution. The above system is equivalent to

$$(b - c)p^2 = (a - cu^6)q^2 + (bu^6 - a)r^2, \quad (b - c)s^2 = (d - c)q^2 + (b - d)r^2. \quad (4)$$

From the geometric point of view, the system (4), as an intersection of two quadric surfaces with rational point $[p : q : r : s] = [u^3 : 1 : 1 : 1]$, is birationally equivalent to an elliptic curve of the form $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{Z}[u]$ depending on a, b, c, d. Although it is possible to give precise values of A and B (this could be done using the result from [**3**, p. 77]), for our purposes, it is enough to find one non-trivial point (i.e. different from $[u^3 : 1 : 1 : 1]$) on the curve defined by (4). Now, we will construct the desired solution of the system (4).

Using standard methods we can find parametric solutions of the first equation in the system (4) in the following form:

$$p = (b - c)u^3 - 2(a - cu^6)v + (a - cu^6)u^3 v^2,$$
$$q = c - b + 2(b - c)u^3 v - (a - cu^6)v^2,$$
$$r = b - c - (a - cu^6)v^2,$$

where v is a rational parameter. We put the obtained parametrization into the second equation in the system (4). We get the curve defined over the field $\mathbb{Q}(u)$ by the equation $\mathcal{C}_6 : s^2 = \sum_{i=0}^{4} A_i(u)v^i =: f(v)$, where

$$A_0 = (b - c)^2, \qquad\qquad\qquad A_1 = 4(b - c)(c - d)u^3,$$
$$A_2 = -2(ab + ac - 2ad + (bc - 3c^2 - 2bd + 4cd)u^6), \quad A_3 = 4(c - d)u^3(a - cu^6),$$
$$A_4 = (a - cu^6)^2.$$

Let us note that the point $Q = (v, s) = (0, b - c)$, lies on the curve $\mathcal{C}_6$. Moreover, we should note that under the assumption $E_i \neq E_j$ for $i \neq j$, the polynomial f is not even (i.e. $f(v) \neq f(-v)$). We use the point Q in order to compute the value of $D(u)$ we are looking for.

Let us put $v = S$, $s = mS^2 + nS + b - c$, where m, n are indeterminates. Then we have the equality $(mS^2 + nS + b - c)^2 - f(S) = \sum_{i=1}^{4} a_i(m, n)S^i$, where $a_i \in \mathbb{Z}[m, n, u]$ and a_i is of degree $3i$ with respect to u for $i = 1, 2, 3, 4$. It is easy to check that the system of equations $a_1(m, n) = a_2(m, n) = 0$ has a unique solution with respect to m, n given by

$$m = m(u) = \frac{-a(b + c - 2d) + (-bc + c^2 + 2bd - 2d^2)u^6}{b - c}, \quad n = n(u) = 2(c - d)u^3.$$

For m, n as above, we see that the equation $a_3(m, n)S^3 + a_4(m, n)S^4 = 0$ has a triple root at $S = 0$ and a $\mathbb{Q}(u)$-rational root S given by

$$S = S(u) = -\frac{a_3(m(u), n(u))}{a_4(m(u), n(u))} = \frac{2(b - c)u^3}{a + (b - c - d)u^6}.$$

Thus, the point $P = (S(u), \ m(u)S(u)^2 + n(u)S(u) + b - c)$ lies on the curve $\mathcal{C}_6$.

Using the values of m, n and S and performing all the necessary calculations and simplifications in order to get polynomial values of p, q, r, s and

$$D(u) = \frac{y_1^2 - x_1^3}{a} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c} = \frac{y_4^2 - x_4^3}{d},$$

we get

$$p = (b - c)u^3(-3a^2 + 2a(b + c + d)u^6 + (b^2 - 2bc + c^2 - 2bd - 2cd + d^2)u^{12}),$$
$$q = (b - c)(-a^2 - 2a(b - c - d)u^6 + (3b^2 - 2bc - c^2 - 2bd + 2cd - d^2)u^{12}),$$
$$r = (b - c)(a^2 - 2a(b - c + d)u^6 + (b^2 + 2bc - 3c^2 - 2bd + 2cd + d^2)u^{12}),$$
$$s = (b - c)(a^2 - 2a(b + c - d)u^6 + (b^2 - 2bc + c^2 + 2bd + 2cd - 3d^2)u^{12})$$

and $D(u) = 8(b - c)^6 u^6(a + (b - c - d)u^6)(a + (-b + c - d)u^6)(a + (-b - c + d)u^6) F(u)^2$, where

$$F(u) = (b^2 - 2bc + c^2 - 2bd - 2cd + d^2)^2 u^{24} +$$
$$- 4a(b^3 - b^2c - bc^2 + c^3 - b^2d + 10bcd - c^2d - bd^2 - cd^2 + d^3)u^{18}$$
$$+ 2a^2(3b^2 + 2bc + 3c^2 + 2bd + 2cd + 3d^2)u^{12} - 4a^3(b + c + d)u^6 + a^4.$$

The value of $T = T(u) := f_1(p, q) = f_2(q, r) = f_3(r, s)$ is given by

$$T = T(u) = \frac{(b - c)^2 F(u)}{(a + (b - c - d)u^6)^4}.$$

From our reasoning we can see that on the curves $E_{i,D}$, which are the sextic twists of E_i by $D(u)$ for $i = 1, 2, 3, 4$, we have the points

$$P_1 = (x_1, \ y_1) = (u^2 T(u)), \ p(u)T(u)),$$
$$P_2 = (x_2, \ y_2) = (T(u), \ q(u)T(u)),$$
$$P_3 = (x_3, \ y_3) = (T(u), \ r(u)T(u)),$$
$$P_4 = (x_4, \ y_4) = (T(u), \ s(u)T(u)).$$

From the remark presented at the beginning of this section, the point P_i is of infinite order on the curve $E_{i, D}$ for $i = 1, 2, 3, 4$.   □

REMARK 2.4. It is also possible (by the same method) to find a polynomial $D \in \mathbb{Z}[u, v, w]$ such that the sextic twist of the elliptic curve E_i by $D(u, v, w)$ has positive $\mathbb{Q}(u, v, w)$-rank for $i = 1, 2, 3, 4$. Indeed, taking the substitution

$$x_1 = u^2 T, \ x_2 = v^2 T, \ x_3 = w^2 T, \ x_4 = T, \ y_1 = pT, \ y_2 = qT, \ y_3 = rT, \ y_4 = sT$$

instead of (3), leads to the intersection of two quadric surfaces defined over $\mathbb{Q}(u, v, w)$ by

$$\begin{cases} (cv^6 - bw^6)p^2 = (cu^6 - aw^6)q^2 + (-bu^6 + av^6)r^2, \\ (cv^6 - bw^6)s^2 = (c - dw^6)q^2 + (-b + dv^6)r^2, \end{cases}$$

with $\mathbb{Q}(u, v, w)$-rational point $(p, q, r, s) = (u^3, v^3, w^3, 1)$. Using standards method it is possible to find a parametric solution (with parameter t) of the first equation of our system. After that we put the obtained parametrization into the second equation of the system and the problem is reduced to finding non-trivial $\mathbb{Q}(u, v, w)$-rational point (i.e. a point (t_0, s_0) whose t-coordinate satisfies $t_0 \neq 0$) on a curve of the form $C : s^2 = \sum_{i=0}^{4} a_i(u, v, w)t^i$. This can be done using exactly the same method as in the proof of the theorem above. After necessary simplifications we get a polynomial $D \in \mathbb{Z}[u, v, w]$ and points $P_i = (x_i, y_i)$ on curves $E_{i,D}$ which are the sextic twists of the curves E_i for $i = 1, 2, 3, 4$. Moreover, it is possible to show that the set of $\mathbb{Q}(u, v, w)$-rational points on C is infinite.

REMARK 2.5. We tried to use the method employed in the theorem above to construct simultaneous sextic twists with positive rank of five elliptic curves with j-invariant $j = 0$. Unfortunately, we have been unable to do this. However, we firmly believe that our method can be used in order to prove that $M_6(0) \geq 5$.

3. Quartic twists.   In this section we are interested in the construction of quartic twists of quadruplets of elliptic curves with j-invariant $j = 1, 728$. Before we give our result, let us recall how the torsion part of the curve $E : y^2 = x^3 + px$ with a fixed $p \in \mathbb{Z} \setminus \{0\}$ [**4**, p. 311] looks like.

If $p = 4$, then $Tors E \cong \mathbb{Z}/4\mathbb{Z}$. If $-p$ is a square in $\mathbb{Z}$, then $Tors E \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and finally if p does not fulfill any of these conditions, then $Tors E \cong \mathbb{Z}/2\mathbb{Z}$. As an immediate consequence, we obtain that if $E_D : y^2 = x^3 + pDx$ is the quartic twist of the curve E by $D \in \mathbb{Z}[t] \setminus \mathbb{Z}$ and on the curve E_D we have a $\mathbb{Q}(t)$ rational point $P = (x, y)$ with $y \neq 0$, then the order of the point P in the group $E_D(\mathbb{Q}(t))$ is not finite. Thus, the curve E_D over $\mathbb{Q}(t)$ has a positive rank.

Now, we are ready to prove the following

THEOREM 3.1. *Let $a, b \in \mathbb{Z} \setminus \{0\}$ and consider the elliptic curves*

$$E_1 : y_1^2 = x_1^3 + ax_1, \quad E_2 : y_2^2 = x_2^3 + bx_2, \quad E_3 : y_3^2 = x_3^3 + cx_3, \quad E_4 : y_4^2 = x_4^3 + dx_4$$

Then there exists a polynomial $D \in \mathbb{Z}[t]$ such that the quartic twist of the elliptic curve E_i by D has positive rank for $i = 1, 2, 3, 4$. Thus, the constant defined in Question 1.3 *satisfies $M_4(1728) \geq 4$.*

Proof. In order to prove our theorem we must show that the set of rational curves on the hypersurface

$$\mathcal{W}: \frac{y_1^2 - x_1^3}{ax_1} = \frac{y_2^2 - x_2^3}{bx_2} = \frac{y_3^2 - x_3^3}{cx_3} = \frac{y_4^2 - x_4^3}{dx_4}$$

is nonempty. It is clear that we are interested in nontrivial rational curves only, i.e. curves $L: x_i = f_i(u)$, $y_i = g_i(u)$ which satisfy $y_i^2 - x_i^3 \neq 0$ for $i = 1, 2, 3, 4$.

Define a rational function $f(x, y) = (y^2 - x^3)/x$ and put

$$x_1 = x_2 = T_1, \quad x_3 = x_4 = T_2, \quad y_1 = pT_1, \quad y_2 = qT_1, \quad y_3 = rT_2, \quad y_4 = sT_2, \quad (5)$$

where p, q, r, s and T_1, T_2 are indeterminates.

Now let us note that if $T_1 = T_1(p, q) = (-bp^2 + aq^2)/(a - b)$, then the first equation defining the hypersurface $\mathcal{W}$ is satisfied. On the other hand, if $T = T_2(r, s) = (-dr^2 + cs^2)/(c - d)$, then the third equation defining the hypersurface $\mathcal{W}$ is satisfied. Moreover, we have

$$\frac{f(T_1(p, q), pT_1(p, q))}{a} = \frac{f(T_1(p, q), qT_1(p, q))}{b} = \frac{(p^2 - q^2)(-bp^2 + aq^2)}{(a - b)^2},$$

$$\frac{f(T_2(r, s), rT_2(r, s))}{c} = \frac{f(T_2(r, s), sT_2(r, s))}{d} = \frac{(r^2 - s^2)(-dr^2 + cs^2)}{(c - d)^2}.$$

Thus, it is clear that in order to find a rational curve on the hypersurface $\mathcal{W}$, it is enough to find a rational curve on the surface

$$\mathcal{S}_4: (c - d)^2(p^2 - q^2)(-bp^2 + aq^2) = (a - b)^2(r^2 - s^2)(-dr^2 + cs^2).$$

Let us denote by $F(p, q, r, s)$ the polynomial defining the surface $\mathcal{S}_4$. From the geometric point of view, $\mathcal{S}_4$ is a quartic surface containing the line $p = q, r = s$ defined over $\mathbb{Q}$. Using this fact, it is possible to show that our surface is birationally equivalent to an elliptic curve of the form $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{Z}[u]$ depending on a, b, c, d. Although it is possible to give the precise values of A and B (this could be done using the result from [**3**, p. 77]), for our purposes, it is enough to find one non-trivial rational curve (i.e. a parametric curve satisfying $(p^2 - q^2)(r^2 - s^2) \neq 0$) on the surface $\mathcal{S}_4$.

In order to find the desired curve on the surface $\mathcal{S}_4$, we put

$$p = uT + t, \quad q = vT + t, \quad r = T + 1, \quad s = 2T + 1, \quad (6)$$

where u, v, t are indeterminates. Then for p, q, r, s defined in this way, we have $F(p, q, r, s) = \sum_{i=1}^{4} a_i(u, v)T^i$, where $a_i \in \mathbb{Z}[u, v, t]$ and a_i is of degree i. It is easy to check that the system of equations $a_1(u, v) = a_2(u, v) = 0$ has a solution with respect to u, v given by

$$u = u(t) = \frac{-5a + b + (11c - 7d)t^4}{6(c - d)t^3}, \quad v = v(t) = \frac{a - 5b + (11c - 7d)t^4}{6(c - d)t^3}. \quad (7)$$

For u, v as above, we see that the equation $a_3(u, v)T^3 + a_4(u, v)T^4 = 0$ has a triple root at $T = 0$ and a $\mathbb{Q}(t)$-rational root T given by

$$T(t) = -\frac{a_3(u(t), v(t))}{a_4(u(t), v(t))}. \tag{8}$$

Now using the values of u, v and T and performing all the necessary calculations and simplifications in order to get polynomial values of p, q, r, s, we obtain

$$p(t) = -\frac{108(c - d)^2 t^{12}}{(a - b)^2}(u(t)T(t) + 1)a_4(u(t), v(t)),$$

$$q(t) = -\frac{108(c - d)^2 t^{12}}{(a - b)^2}(v(t)T(t) + t)a_4(u(t), v(t)),$$

$$r(t) = -\frac{108(c - d)^2 t^{12}}{(a - b)^2}(T(t) + 1)a_4(u(t), v(t)),$$

$$s(t) = -\frac{108(c - d)^2 t^{12}}{(a - b)^2}(2T(t) + 1)a_4(u(t), v(t)).$$

Now we can compute the polynomial $D(t) = f(T_1(u, v), pT_1(u, v))/a$, where u, v are given by (7) and p is as above, which is the value of the proper twist that we are looking for

$$\begin{aligned}
D(t) = {} & 72t^4(a + b - (c + d)t^4)(a^2 + 14ab + b^2 - (c^2 + 14cd + d^2)t^8) \\
& \times (4(a + b)^2 + 4(a + b)(c + d)t^4 + (c^2 - 34cd + d^2)t^8) \\
& \times (a^2 - 34ab + b^2 + 4(a + b)(c + d)t^4 + 4(c + d)^2 t^8) \times G(t),
\end{aligned}$$

where $G(t) = \sum_{i=0}^{4} b_i t^{4i}$ and $b_i \in \mathbb{Z}[a, b, c, d]$ are given by

$b_0 = (a^2 - 34ab + b^2)^2$, $b_1 = -4(a + b)(c + d)(a^2 - 34ab + b^2)$,
$b_2 = 6(a^2 c^2 - 10abc^2 + b^2 c^2 - 10a^2 cd - 476abcd - 10b^2 cd + a^2 d^2 - 10abd^2 + b^2 d^2)$,
$b_3 = -4(a + b)(c + d)(c^2 - 34cd + d^2)$, $b_4 = (c^2 - 34cd + d^2)^2$.

From our computations we see that on $E_{i,D}$, which is the quartic twist of E_i by $D(t)$ for $i = 1, 2, 3, 4$ respectively, we have the points

$$\begin{aligned}
P_1 &= (x_1, \ y_1) = (T_1(p(t), q(t)), \ p(t)T_1(p(t), q(t))), \\
P_2 &= (x_2, \ y_2) = (T_1(p(t), q(t)), \ q(t)T_1(p(t), q(t))), \\
P_3 &= (x_3, \ y_3) = (T_2(r(t), s(t)), \ r(t)T_2(r(t), s(t))), \\
P_4 &= (x_4, \ y_4) = (T_2(r(t), s(t)), \ s(t)T_2(r(t), s(t))).
\end{aligned}$$

From the remark presented at the beginning of this section, the point P_i is of infinite order on the curve $E_{i,\ D}$ for $i = 1, 2, 3, 4$. $\qquad\square$

REFERENCES

1. M. Kuwata and L. Wang, Topology of rational points on isotrivial elliptic surfaces, *Int. Math. Res. Notices* **4** (1993), 113–123.

2. J. F. Mestre, Rang de courbes elliptiques d'invariant donné, *C. R. Acad. Sci. Paris Ser. 1, Math.* **314** (1992), 919–922.

3. L. J. Mordell, *Diophantine Equations* (Academic Press, London, 1969).

4. J. Silverman, *The Arithmetic of Elliptic Curves* (Springer-Verlag, New York, 1986).