ACTA ARITHMETICA
144.2 (2010)

Characterization of the torsion of the Jacobian of $y^2 = x^5 + Ax$ and some applications

by

Tomasz Jędrzejak (Szczecin) and
Maciej Ulas (Warszawa and Kraków)

1. Introduction. In [7] it is shown 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 ranks. A similar result was proved for quadruples of elliptic curves with j-invariant equal to 1728.

These results have been generalized in [4] to curves of the form $y^2 = x^n + A$, where n is divisible by an odd prime and $A \in \mathbb{Z} \setminus \{0\}$. The main tool in the proof was a (partial) characterization of possible torsion subgroups of the Jacobian variety associated with the curve $y^2 = x^p + A$, where p is an odd prime and $A \in \mathbb{Z} \setminus \{0\}$.

A natural question arises whether similar results could be obtained for k-tuples (for appropriate k) of hyperelliptic curves of the form $C : y^2 = x^5 + Ax$ (of genus 2), which are (in some sense) natural generalizations of elliptic curves with j-invariant equal to 1728. The quartic twist of the curve C by D has the form $C_D : y^2 = x^5 + AD^2x$. The octic twist of C by D is $C_D : y^2 = x^5 + ADx$. In view of the results obtained in [7] and [4] we ask the following question.

Question 1.1. *Let $C_i : y^2 = x^5 + a_i x$ where $a_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \ldots, n$, and suppose that $C_i \neq C_j$ for $i \neq j$. What is the maximal number, say N, for which there exists a polynomial $D \in \mathbb{Z}[u]$ such that the Jacobian of the octic twist of C_i by D has positive rank for all $i = 1, \ldots, N$?*

This is a difficult problem and we only give a lower bound on N. It is clear that to this end we need two things. We must be able to construct rational points on appropriate curves and show that these points lead to

2010 *Mathematics Subject Classification*: 11G05, 14G99.
Key words and phrases: torsion group of hyperelliptic Jacobians, higher twists of genus two curves, rational points.

DOI: 10.4064/aa144-2-7

divisor classes which are of infinite order in the Jacobian variety. In the case of elliptic curves we know a full characterization of possible torsions over $\mathbb{Q}$. This characterization of the torsion subgroup of elliptic curves with j-invariant $j \in \{0, 1728\}$ was used in the proofs of the results obtained in [7].

However, no characterization of the torsion of the Jacobian of the curve $y^2 = x^5 + Ax$ is known yet. So, in Section 2 we begin our investigations with a full characterization of the torsion subgroup of the Jacobian of the curve $C_A : y^2 = x^5 + Ax$, where $A \in \mathbb{Z} \setminus \{0\}$. We denote by $\mathcal{J}_A$ the Jacobian variety associated with C_A and by $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ its group of $\mathbb{Q}$-rational torsion points. Remember that, by definition, the divisor $D \in \mathrm{Div}(C_A)$ is $\mathbb{Q}$-rational if it is invariant under the action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Note that if $D = n_1P_1 + \cdots + n_rP_r$ with $n_1, \ldots, n_r \neq 0$ then to say that D is $\mathbb{Q}$-rational does not mean that $P_1, \ldots, P_r$ are $\mathbb{Q}$-rational. It suffices for $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to permute the P_i's in an appropriate fashion, or in other words, $\{P_1^\sigma, \ldots, P_r^\sigma\} = \{P_1, \ldots, P_r\}$ for each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. In Theorem 2.2 we characterize the set $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$. Next we show that for the constant N in Question 1.1 we have $N \geq 4$ (Theorem 3.1).

2. Characterization of the torsion subgroup of $\mathcal{J}_A(\mathbb{Q})$. Consider the family of curves (over $\mathbb{Q}$) $C_A : y^2 = x^5 + Ax$, where A is a nonzero rational. The curve C_A is hyperelliptic of genus 2. Without loss of generality we can (and will) assume that A is an 8-powerfree integer. In this section we describe the group $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ completely. Note that $\mathrm{disc}(x^5 + Ax) = 256A^5$. Let p denote a prime such that $p \nmid 2A$. We start with the following lemma.

LEMMA 2.1. *We have*

$$\mathcal{J}_A(\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } A \neq \pm\square \text{ or } (A = \square \text{ and } 2\sqrt{A} \neq \square) \text{ (case 1)}, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } (A = \square \text{ and } 2\sqrt{A} = \square) \\ & \text{or } (A = -\square \text{ and } \sqrt{-A} \neq \square) \text{ (case 2)}, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } \sqrt{-A} = \square \text{ (case 3)}. \end{cases}$$

In particular if A is as in case 1 then

$$\mathcal{J}_A(\mathbb{Q})[2] = \{0, [(0,0) - \infty]\}. \tag{1}$$

Let a denote a squarefree positive integer. If $A = a^4/4$ then

$$\mathcal{J}_A(\mathbb{Q})[2] = \left\{ \begin{array}{l} 0, [(0,0) - \infty], [((-a+ia)/2, 0) + ((-a-ia)/2, 0) - 2\infty], \\ [((a+ia)/2, 0) + ((a-ia)/2, 0) - 2\infty] \end{array} \right\}. \tag{2}$$

If $A = -a^2$ then

$$\mathcal{J}_A(\mathbb{Q})[2] = \left\{ \begin{array}{l} 0, [(0,0) - \infty], [(\sqrt{a}, 0) + (-\sqrt{a}, 0) - 2\infty], \\ [(i\sqrt{a}, 0) + (-i\sqrt{a}, 0) - 2\infty] \end{array} \right\}. \tag{3}$$

If $A = -a^4$ *then*

$$\mathcal{J}_A(\mathbb{Q})[2] = \left\{ \begin{array}{l} 0, [(0,0)-\infty], [(a,0)-\infty], \\ [(-a,0)-\infty], [(0,0)+(a,0)-2\infty], \\ [(0,0)+(-a,0)-2\infty], [(a,0)+(-a,0)-2\infty], \\ [(ia,0)+(-ia,0)-2\infty] \end{array} \right\}. \tag{4}$$

Proof. It is well known that every point in $\mathcal{J}_A(\bar{\mathbb{Q}})[2]$ can be uniquely written as $D = \sum n_i P_i - (\sum n_i)\infty$, where $P_i = (x_i, 0)$ are pairwise disjoint, $n_i \in \{0,1\}$, $\sum n_i \le 2$. Therefore the group $\mathcal{J}_A(\mathbb{Q})[2]$ is completely determined by the factorization of the polynomial $f(x) := x^4 + A$ over $\mathbb{Q}$. Note that f has a rational root if and only if $A = -a^4$. In this case $f(x)$ factors as $(x-a)(x+a)(x^2+a^2)$. Hence we have (4). It is easy to check that f is irreducible over $\mathbb{Q}$ if and only if A is as in case 1. Then $\mathcal{J}_A(\mathbb{Q})[2] = \{0, [(0,0)-\infty]\}$. If f has no rational roots but is reducible over $\mathbb{Q}$ then A is as in case 2. In particular if $A = a^4/4$ then $f(x) = (x^2 + ax + a^2/2)(x^2 - ax + a^2/2)$, hence we get (2). If $A = -a^2$ then $f(x) = (x^2 - a)(x^2 + a)$ and we are done. ∎

We shall prove the following theorem.

THEOREM 2.2. *We have* $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} = \mathcal{J}_A(\mathbb{Q})[2]$.

The proof of Theorem 2.2 splits into a few lemmas. In order to compute $\#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ consider $\mathcal{J}_A(\mathbb{F}_p)$ for several primes $p \nmid 2A$, since the reduction modulo p homomorphism induces an embedding $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \mathcal{J}_A(\mathbb{F}_p)$ (see for example [2, p. 70]) and therefore

$$\#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} \mid \#\mathcal{J}_A(\mathbb{F}_p). \tag{5}$$

Since ([2, formula (8.2.7)])

$$\#\mathcal{J}_A(\mathbb{F}_p) = \tfrac{1}{2}(\#C_A(\mathbb{F}_p)^2 + \#C_A(\mathbb{F}_{p^2})) - p, \tag{6}$$

it is enough to compute $\#C_A(\mathbb{F}_{p^k})$ for $k = 1, 2$.

LEMMA 2.3. *If* $p \not\equiv 1 \pmod 8$ *then* $\#C_A(\mathbb{F}_p) = 1 + p$.

Proof. The point $(0,0)$ and the point at infinity lie on the curve C_A. Let $p \equiv 3 \pmod 4$. Since -1 is not a square in $\mathbb{F}_p$, each pair $(x, -x)$, where $x \in \mathbb{F}_p^*$, contributes two points to $C_A(\mathbb{F}_p)$. If $p \equiv 5 \pmod 8$ then -1 is a square but not a fourth power in $\mathbb{F}_p$. Since $(ix)^5 + A(ix) = i(x^5 + Ax)$, each quadruple $x, -x, ix, -ix$ gives four points of $C_A(\mathbb{F}_p)$. Therefore our assertion follows. ∎

In order to compute $\#C_A(\mathbb{F}_{p^2})$ and $\#C_A(\mathbb{F}_p)$ for $p \equiv 1 \pmod 8$ we will use Jacobsthal sums.

Let $q = p^k$, $e \in \mathbb{N}$ and $a \in \mathbb{F}_q$. The *Jacobsthal sums* $\varphi_e(a)$ of order e are defined by

$$\varphi_e(a) = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\left(\frac{x^e + a}{q}\right),$$

where $\left(\frac{\cdot}{q}\right)$ is the quadratic character of $\mathbb{F}_q$. Following [5] we list a few of their properties.

LEMMA 2.4. *Let $\varphi_e(a)$ be the Jacobsthal sum of order e for a.*

(1) *If $(e, q-1) = e_1$ then $\varphi_e(a) = \varphi_{e_1}(a)$.*
(2) *If $e \mid (q-1)$ but $2e \nmid (q-1)$ then $\varphi_e(a) = 0$.*
(3) *$\varphi_e(ab^e) = (b/q)^{e+1}\varphi_e(a)$ for $b \in \mathbb{F}_q^\times$.*
(4) *$\#C_A(\mathbb{F}_q) = 1 + q + \varphi_4(A)$.*

LEMMA 2.5. *Let $q = p^2$.*

(1) *Suppose $p \equiv 1$ or $3 \pmod 8$ and write $p = u^2 + 2v^2$. Then*

$$\varphi_4(A) = \begin{cases} -4(2u^2 - p) & \text{if } A \text{ is an 8th power in } \mathbb{F}_q, \\ 4(2u^2 - p) & \text{if } A \text{ is a 4th power but not an 8th power in } \mathbb{F}_q, \\ 0 & \text{if } A \text{ is a square but not a 4th power in } \mathbb{F}_q, \\ \pm 8uv & \text{otherwise.} \end{cases}$$

(2) *Suppose $p \equiv 5$ or $7 \pmod 8$. Then*

$$\varphi_4(A) = \begin{cases} 4p & \text{if } A \text{ is an 8th power in } \mathbb{F}_q, \\ -4p & \text{if } A \text{ is a 4th power but not an 8th power in } \mathbb{F}_q, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The proof can be found in [1, pp. 420–421]. ∎

LEMMA 2.6. *The following properties hold:*

(1) *If $\left(\frac{a}{p}\right) = 1$ then a is a fourth power in $\mathbb{F}_{p^2}$.*
(2) *If $\left(\frac{a}{p}\right) = -1$ and $p \equiv 1 \pmod 4$ then a is a square but not a fourth power in $\mathbb{F}_{p^2}$.*

Proof. This is an easy calculation. ∎

Now, we are ready to prove the following

LEMMA 2.7. *The group $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group.*

Proof. One should consider a few cases. In all the cases we will compute $\#\mathcal{J}_A(\mathbb{F}_p)$ using the formula (6) and Lemmata 2.4–2.6. Fix an odd prime l.

Suppose that A is neither $\pm\square$ nor $\pm 5\square$. Then we can find a prime p such that $p \equiv 5 \pmod 8$, $\left(\frac{A}{p}\right) = -1$, $l \nmid (1 + p^2)$ and $p \nmid A$. Note that for $p \equiv 5 \pmod 8$ and $\left(\frac{A}{p}\right) = -1$ we have $\#\mathcal{J}_A(\mathbb{F}_p) = 1 + p^2$. Hence by (5) we get $l \nmid \#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$. Moreover, $1 + p^2 \equiv 2 \pmod 4$ so $\#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} = 2$. In general, if A is not $\pm\square$ we have only $\#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} = 2 \cdot 5^m$, $m \geq 0$.

Suppose that $A = a^2$ and $a > 0$. For $p \equiv 5 \pmod 8$ such that $\left(\frac{a}{p}\right) = 1$ we get $\#C_A(\mathbb{F}_p) = 1 + p$ and $\#C_A(\mathbb{F}_{p^2}) = 1 + p^2 + 4p$ (A is an 8th power in $\mathbb{F}_{p^2}$). Hence $\#\mathcal{J}_A(\mathbb{F}_p) = (p+1)^2 \equiv 4 \pmod 8$. If $l > 3$ or a is not $6\square$ then we can find a prime $p > A$ such that $p \equiv 5 \pmod 8$, $\left(\frac{a}{p}\right) = 1$ and $l \nmid (p+1)$. Therefore $\#J_{a^2}(\mathbb{Q})_{\mathrm{tors}} = 2^m 3^n$, where $1 \le m \le 2$, and where $n = 0$ if a is not $6\square$. Moreover by Lemma 2.1 we obtain $J_{c^4/4}(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Consider the case $a = 6c^2$ with $c > 0$. It is sufficient to show that $3 \nmid \#J_{36c^4}(\mathbb{Q})_{\mathrm{tors}}$. By Lemma 2.4(3) we have $\varphi_4(36c^4) = \left(\frac{c}{q}\right)\varphi_4(6^2)$ where $q = p$ or $q = p^2$. Let $p \equiv 17 \pmod{24}$ and $p = u^2 + 2v^2$. Since 6 is neither a square in $\mathbb{F}_p$ nor a 4th power in $\mathbb{F}_{p^2}$ we get $\#C_{36c^4}(\mathbb{F}_p) = 1 + p$ and $\#C_{36c^4}(\mathbb{F}_{p^2}) = 1 + p^2 + 8u^2 - 4p$. Consequently, $\#J_{36c^4}(\mathbb{F}_p) = (p-1)^2 + 4u^2 \not\equiv 0 \pmod 3$.

Suppose now that $A = -a^2$ with $a > 0$. It is easy to see that $\#J_{-a^2}(\mathbb{F}_p) = (p+1)^2 \equiv 4 \pmod 8$ for $p \equiv 5 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$. If a is not a square or $l > 3$ then we can find a prime $p \equiv 5 \pmod 8$ such that $\left(\frac{a}{p}\right) = -1$, $p > a$ and $l \nmid (p+1)$. Hence $\#J_{-a^2}(\mathbb{Q})_{\mathrm{tors}} = 2^m 3^n$, where $1 \le m \le 2$, and where $n = 0$ if in addition a is not $3\square$. By Lemma 2.1 in both cases we get $J_{-a^2}(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$. On the other hand if a is not a $2\square$ or $l > 3$ then we can find a prime $p \equiv 5 \pmod 8$ such that $\left(\frac{a}{p}\right) = 1$, $p > a$ and $l \nmid (p-1)$ (now $\#J_{-a^2}(\mathbb{F}_p) = (p-1)^2 \equiv 16 \pmod{32}$). Therefore if a is neither $2\square$ nor $3\square$ we have $\#J_{-a^2}(\mathbb{Q})_{\mathrm{tors}} = 2^m$ where $1 \le m \le 4$. Now let $a = 3c^2$, i.e. $A = -9c^4$. As in the earlier case, we take $p \equiv 17 \pmod{24}$ and get $3 \nmid \#J_{-9c^4}(\mathbb{F}_p) = (p-1)^2 + 4u^2$.

We are left with the case $A = \pm 5a^2$. In both cases it is enough to prove that $5 \nmid \#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$. For every $a \in \mathbb{N}$ there exists a prime $p > |A|$ such that $p \equiv 7 \pmod 8$, $p \equiv 1 \pmod 5$ and $\left(\frac{a}{p}\right) = 1$. Then, as in the previous cases, we combine Lemmata 2.4–2.6 to get $\#J_{\pm 5a^2}(\mathbb{F}_p) = (p+1)^2 \equiv 2 \pmod 5$ and we are done. ∎

LEMMA 2.8. *The group $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ contains no element of order* 4.

Proof. In view of the previous proof it is sufficient to investigate $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}}$ for $A = a^2$ where $a \neq 2\square$ and for $A = -c^4$. In the first case $\#\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} = 2$ or 4. For prime $p > a$ such that $p \equiv 5 \pmod 8$ choose b such that $b^2 \equiv -a^2 \pmod p$. Then $x^5 + Ax$ factors in $\mathbb{F}_p$ as $x(x^2 - b)(x^2 + b)$ (the factors are irreducible) and $4 \parallel \#J_{a^2}(\mathbb{F}_p)$. Hence $\#J_{a^2}(\mathbb{F}_p)[2] = 4$. By the embedding $\mathcal{J}_A(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \mathcal{J}_A(\mathbb{F}_p)$ we conclude that $J_{a^2}(\mathbb{Q})_{\mathrm{tors}}$ has no elements of order 4. Similarly for $A = -c^4$ taking $p \equiv 5 \pmod 8$ with $p > c$ we have $16 \parallel \#J_{-c^4}(\mathbb{F}_p)$ and $\#J_{-c^4}(\mathbb{F}_p)[2] = 16$. Therefore $J_{-c^4}(\mathbb{Q})_{\mathrm{tors}}$ contains no elements of order 4 and the assertion follows. ∎

Gathering the results from Lemmata 2.7 and 2.8 completes the proof of Theorem 2.2.

3. An interesting application. In this section we give an interesting application of Theorem 2.2 to Question 1.1. More precisely, we prove the following theorem.

THEOREM 3.1. *Let $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ be pairwise distinct and consider the curves*

$$C_1 : y_1^2 = x_1^5 + ax_1, \quad C_2 : y_2^2 = x_2^5 + bx_2,$$
$$C_3 : y_3^2 = x_3^5 + cx_3, \quad C_4 : y_4^2 = x_4^5 + dx_4.$$

Then there exists a polynomial $D \in \mathbb{Z}[u]$ such that the Jacobian variety of the octic twist of the curve C_i by D has positive rank for $i = 1, 2, 3, 4$. In other words, for the constant N defined in the introduction we have $N \geq 4$.

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

$$\mathcal{W} : \frac{y_1^2 - x_1^5}{ax_1} = \frac{y_2^2 - x_2^5}{bx_2} = \frac{y_3^2 - x_3^5}{cx_3} = \frac{y_4^2 - x_4^5}{dx_4}$$

is nonempty. Due to the characterization of the torsion of the Jacobian of the curve $y^2 = x^5 + Ax$ given in Theorem 2.2 it is enough to show the existence of a nontrivial rational curve on the variety $\mathcal{W}$, i.e. a curve $L : x_i = f_i(u)$, $y_i = g_i(u)$ which satisfies the condition $y_i^2 - x_i^5 \neq 0$ for $i = 1, 2, 3, 4$. Define a rational function $f(x, y) = (y^2 - x^5)/x$ and put

$$\begin{aligned} &x_1 = x_2 = x_3 = T,\ x_4 = u^2 T, \\ &y_1 = pT^2,\ y_2 = qT^2,\ y_3 = rT^2,\ y_4 = sT^2, \end{aligned} \tag{7}$$

where p, q, r, s and T are indeterminates. Now, if $T = (-bp^2 + aq^2)/(a - b)$, then the first equation defining the hypersurface $\mathcal{W}$ holds. On the other hand, if $T = (-cq^2 + br^2)/(b - c)$, then the second equation defining $\mathcal{W}$ holds. Finally, for $T = (dr^2u^2 - cs^2)/(u^2(d - cu^8))$ the third equation holds. Hence if the system of equations

$$\frac{-bp^2 + aq^2}{a - b} = \frac{-cq^2 + br^2}{b - c} = \frac{dr^2u^2 - cs^2}{u^2(d - cu^8)}$$

has a nontrivial $\mathbb{Q}(u)$-rational solution, then there exists a rational curve on $\mathcal{W}$. The above system is equivalent to

$$\begin{cases} (a - b)r^2 = (c - b)p^2 + (-c + a)q^2, \\ (a - b)s^2 = u^2((d - bu^8)p^2 + (-d + au^8)q^2). \end{cases} \tag{8}$$

From the geometric point of view the variety defined by (8), as an intersection of two quadratic surfaces with rational point $[p : q : r : s] = [1 : 1 : 1 : u^5]$, is birationally equivalent to an elliptic curve of the form $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{Z}[u]$ which depend 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 [6, p. 77]), for our purposes it is enough to find one nontrivial $\mathbb{Q}(u)$-point (i.e.

different from $[\pm 1 : \pm 1 : \pm 1 : \pm u^5]$) on the curve defined by (8). Now, we will construct the desired solution of (8). Using the standard method we can find parametric solutions to the first equation in (8):

$$\begin{aligned} p &= b - c - 2(2a - b - c)t + (b - c)t^2, \\ q &= 4a - 3b - c - 2(b - c)t + (b - c)t^2, \\ r &= 4a - b - 3c - 2(b - c)t + (-b + c)t^2, \end{aligned}$$

where t is a rational parameter. We substitute this parametrization into the second equation in (8), getting the curve defined over the field $\mathbb{Q}(u)$ by the equation $\mathcal{C} : s^2 = \sum_{i=0}^{4} A_i(u)t^{4-i} =: f(t)$, where

$$\begin{aligned} A_0 &= (b - c)^2 u^{10}, \\ A_1 &= 4u^4(b - c)(-2d + (b + c)u^8), \\ A_2 &= 8(2a - b - c)du^2 - 2(4ab - 3b^2 + 4ac - 2bc - 3c^2)u^{10}, \\ A_3 &= 4u^2(b - c)(2d - (4a - b + c)u^8), \\ A_4 &= -8(2a - b - c)du^2 + (16a^2 - 8ab + b^2 - 8ac - 2bc + c^2)u^{10}. \end{aligned}$$

Note that on $\mathcal{C}$ we have a $\mathbb{Q}(u)$-rational point at infinity $Q = [t : s : w] = [1 : (b-c)u^5 : 0]$. Moreover, under our assumption that $C_i \neq C_j$ for $i \neq j$, the polynomial f is not even (i.e. $f(t) \neq f(-t)$). We use the point Q to compute the value of $D(u)$ we are looking for. Set $t = S$, $s = (b - c)u^5S^2 + mS + n$, where m, n are indeterminates. We have $((b - c)u^5S^2 + mS + n)^2 - f(S) = \sum_{i=1}^{4} a_i(m, n)S^i$, where $a_i \in \mathbb{Z}[m, n, u]$. It is easy to check that the system of equations $a_1(m, n) = a_2(m, n) = 0$ has a unique solution m, n given by

$$\begin{aligned} m = m(u) &= \frac{2(-2d + (b + c)u^8)}{u^3}, \\ n = n(u) &= \frac{-8d^2 + 4(2a + b + c)du^8 - (4ab - b^2 + 4ac + 2bc - c^2)u^{16}}{(b - c)u^{11}}. \end{aligned}$$

For m, n as above the equation $a_3(m, n)S^3 + a_4(m, n)S^4 = 0$ has a triple root at $S = 0$ and a rational root S given by

$$S = S(u) = -\frac{a_3(m(u), n(u))}{a_4(m(u), n(u))} = \frac{au^8 - d}{(b - c)u^8}.$$

Thus, the point $P = (S(u), (b-c)u^5S(u)^2+m(u)S(u)+n(u))$ lies on $\mathcal{C}$. Using the computed values of m, n and S and performing all necessary calculations and simplifications in order to get polynomial values of p, q, r, s and

$$D(u) = \frac{y_1^2 - x_1^5}{ax_1} = \frac{y_2^2 - x_2^5}{bx_2} = \frac{y_3^2 - x_3^5}{cx_3} = \frac{y_4^2 - x_4^5}{dx_4},$$

we get

$$p(u) = d^2 + 2(a - b - c)du^8 - (3a^2 - 2ab - b^2 - 2ac + 2bc - c^2)u^{16},$$

$$q(u) = d^2 - 2(a-b+c)du^8 + (a^2+2ab-3b^2-2ac+2bc+c^2)u^{16},$$
$$r(u) = d^2 - 2(a+b-c)du^8 + (a^2-2ab+b^2+2ac+2bc-3c^2)u^{16},$$
$$s(u) = u^5(3d^2 - 2(a+b+c)du^8 - (a^2-2ab+b^2-2ac-2bc+c^2)u^{16}),$$

and

$$D(u) = 8u^8(d+(a-b-c)u^8)(-d+(a+b-c)u^8)(-d+(a-b+c)u^8)T(u)^3,$$

where

$$\begin{aligned} T(u) = {} & (a^2-2ab+b^2-2ac-2bc+c^2)^2u^{32} \\ & - 4(a^3-a^2b-ab^2+b^3-a^2c+10abc-b^2c-ac^2-bc^2+c^3)du^{24} \\ & + 2(3a^2+2ab+3b^2+2ac+2bc+3c^2)d^2u^{16} - 4(a+b+c)d^3u^8 + d^4. \end{aligned}$$

From the above we can see that the points

$$\begin{aligned} P_1 &= (x_1, y_1) = (T(u), p(u)T(u)), \\ P_2 &= (x_2, y_2) = (T(u), q(u)T(u)), \\ P_3 &= (x_3, y_3) = (T(u), r(u)T(u)), \\ P_4 &= (x_4, y_4) = (u^2T(u), s(u)T(u)), \end{aligned}$$

lie on curves $C_{i,D}$, which are the octic twists of C_i by $D(u)$ for $i = 1, 2, 3, 4$.

Note that for any $e \in \mathbb{Z} \setminus \{0\}$ the genus of the curve $C(e) : y^2 = eD(u)$ is ≥ 2. Thus from Faltings' theorem [3] the set of rational points on $C(e)$ is finite. We thus see that for all but finitely many u the Jacobian, say $\mathcal{J}_i$, of the curve $C_{i,D(u)}$ for $i = 1, 2, 3, 4$ has trivial torsion subgroup via our characterization from Theorem 2.2. But in the Jacobian $\mathcal{J}_i(\mathbb{Q})$ we have the class of the divisor $(P_i) - (\infty)$. This implies that the rank of $\mathcal{J}_i(\mathbb{Q})$ is positive. ∎

Remark 3.2. By the same arguments as in the proof of Theorem 3.1 one can find a polynomial $D \in \mathbb{Z}[u, v, w]$ such that the octic twist of the hyperelliptic curve C_i by $D(u, v, w)$ has positive $\mathbb{Q}(u, v, w)$-rank for $i = 1, 2, 3, 4$. Indeed, instead of (7), we take

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

and then the same reasoning leads to the intersection of two quadric surfaces defined over $\mathbb{Q}(u, v, w)$ by

$$\begin{cases} u^2v^2(bu^8 - av^8)r^2 = -v^2w^2(cv^8 - bw^8)p^2 + u^2w^2(cu^8 - aw^8)q^2, \\ u^2v^2(bu^8 - av^8)s^2 = v^2(b - dv^8)p^2 - u^2(a - du^8)q^2, \end{cases}$$

with $\mathbb{Q}(u, v, w)$-rational point $[p : q : r : s] = [u^5 : v^5 : w^5 : 1]$. Using the standard method it is possible to find a parametric solution (with parameter t) of the first equation of our system. Inserting the parametrization

obtained in the second equation of the system reduces the problem to finding a nontrivial $\mathbb{Q}(u,v,w)$-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 above. After necessary simplifications we get a polynomial $D \in \mathbb{Z}[u,v,w]$ and point $P_i = (x_i, y_i)$ on the curve $C_{i,D}$ which is the octic twist of the curve C_i for $i = 1,2,3,4$. Moreover, one can show that the set of $\mathbb{Q}(u,v,w)$-rational points on C is infinite.

References

[1] B. C. Berndt and R. J. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer*, Illinois J. Math. 23 (1979), 374–437.

[2] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, 1996.

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

[4] T. Jędrzejak and M. Ulas, *Higher twists of hyperelliptic curves*, submitted.

[5] S. A. Katre and A. R. Rajwade, *Jacobsthal sums of prime order,* Indian J. Pure Appl. Math. 17 (1986), 1345–1362.

[6] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

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

Tomasz Jędrzejak
Institute of Mathematics
University of Szczecin
Wielkopolska 15
70-451 Szczecin, Poland
E-mail: tjedrzejak@gmail.com

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

Received on 9.8.2009
and in revised form on 16.11.2009 (6113)