ACTA ARITHMETICA
150.2 (2011)

Tuples of hyperelliptic curves $y^2 = x^n + a$

by

Tomasz Jędrzejak (Szczecin), Jaap Top (Groningen)
and Maciej Ulas (Kraków)

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

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

where $a, b, c, d \in \mathbb{Q}$ satisfy $(a, c) \neq (0, 0) \neq (b, d)$. Considering the Euclidean topology on the set $\mathcal{E}(\mathbb{R})$ of all real points on $\mathcal{E}$, they showed that the set of rational points $\mathcal{E}(\mathbb{Q})$ is dense in $\mathcal{E}(\mathbb{R})$. Their argument uses a special rational curve on $\mathcal{E}$, which was also independently constructed by Mestre [Me]. Using this rational curve, Kuwata and Wang deduce that if E_1, E_2 are elliptic curves over $\mathbb{Q}$ with j-invariants $(j(E_1), j(E_2)) \notin \{(0, 0), (1728, 1728)\}$, then there exists a polynomial $d(t) \in \mathbb{Q}[t]$ such that the quadratic twists of E_1, E_2 by $d(t)$ both have positive rank over $\mathbb{Q}(t)$.

In [U] it is shown that if one allows sextic resp. quartic twists, then analogous results hold for pairs of elliptic curves with j-invariant 0 resp. 1728. Here we extend this to a special class of hyperelliptic curves.

Theorem 1.1. *Suppose $n \in \mathbb{Z}_{\geq 3}$. Given nonzero $a, b \in \mathbb{Q}$, there exists a polynomial $d(t) \in \mathbb{Q}[t]$ such that the Jacobians of the curves given by $y^2 = x^n + ad(t)$ and $y^2 = x^n + bd(t)$ both have positive rank over $\mathbb{Q}(t)$.*

In fact, more precise results will be given. For example, the question is considered whether or not the polynomial $d(t) \in \mathbb{Q}[t]$ can be required to be a square. Moreover, one can extend the result above to the case of more than two curves:

Theorem 1.2. *Suppose $n \in \mathbb{Z}_{\geq 3}$. Given nonzero $a, b, c \in \mathbb{Q}$, there exists a polynomial $d(t) \in \mathbb{Q}[t]$ such that the Jacobians of the curves given by $y^2 = x^n + ad(t)$ and $y^2 = x^n + bd(t)$ and $y^2 = x^n + cd(t)$ all have positive rank over $\mathbb{Q}(t)$.*

2010 *Mathematics Subject Classification*: Primary 11G30; Secondary 14H45.
Key words and phrases: hyperelliptic curve, twist, Mordell–Weil rank, Jacobian.

DOI: 10.4064/aa150-2-1

Theorem 1.3. *Suppose $n \in \mathbb{Z}_{\geq 3}$ is odd. Given nonzero $a_1, a_2, a_3, a_4 \in \mathbb{Q}$, there exists a polynomial $d(t) \in \mathbb{Q}[t]$ such that the Jacobians of the curves given by $y^2 = x^n + a_j d(t)$ all have positive rank over $\mathbb{Q}(t)$.*

Generalities concerning twists of varieties and in particular of curves can be found in [MT]. Note that in the special case where n is even, the curves considered here are equipped with two rational points ∞_+, ∞_- "at infinity". The difference $(\infty_+) - (\infty_-)$ then defines a nontrivial point in the Jacobian. However, this is a torsion point as follows by taking the divisor of the function $y + x^{n/2}$. This is a very special case of a topic already studied by Abel; see, for example, work of Schinzel [Sch], Hellegouarch and Lozach [HL], Berry [Be] and the many references they provide.

The proof of our result consists of two parts. Given a point $(x(t), y(t))$ on a curve with equation $y^2 = x^n + ad(t)$, we need a condition implying that this point minus a point at infinity defines a point of infinite order in the Jacobian. This is done by adapting ideas of [ST] to the present situation. Next, we need a rational function $d(t)$ and rational points $(x_a(t), y_a(t))$ resp. $(x_b(t), y_b(t))$ on the curve with equation $y^2 = x^n + ad(t)$ resp. $y^2 = x^n + bd(t)$. To this end, we construct rational curves on the threefold $\mathcal{X}$ with equation

$$\mathcal{X}: \ b(y_a^2 - x_a^n) = a(y_b^2 - x_b^n).$$

Parametrizing such a rational curve as $t \mapsto (x_a(t), y_a(t), x_b(t), y_b(t))$ gives us the required points by taking $d(t) := (y_a(t)^2 - x_a(t)^n)/a$. If one moreover demands that $d(t)$ is a square, then instead of $\mathcal{X}$ one considers the threefold $\mathcal{Y}$ given by the two equations

$$\mathcal{Y}: \ z^2 = b(y_a^2 - x_a^n) = a(y_b^2 - x_b^n),$$

which defines a double cover of $\mathcal{X}$.

Section 2 provides details on the method used to show that certain divisors have infinite order. Section 3 contains the construction of rational curves on the threefolds $\mathcal{X}$ and $\mathcal{Y}$, resulting in the proof of Theorem 1.1. Finally, in Section 4 we prove Theorems 1.2 and 1.3.

2. Infinite order. In this section we take $n \in \mathbb{Z}_{\geq 3}$. Suppose K is a field of characteristic not dividing $2n$. Fix $a \in K$ with $a \neq 0$ and take $d(t) \in K[t]$ of positive degree such that $d(t)$ is not divisible by a nonconstant $\mathrm{lcm}(2, n)$th power in $K[t]$. Let $\alpha \in K$ be the leading coefficient of $d(t)$. Define the hyperelliptic curve C_0/K by the equation

$$C_0: \ y^2 = x^n + a\alpha$$

and $C/K(t)$ by

$$C: \ y^2 = x^n + ad(t).$$

Fix a point $\infty \in C(K(t))$ at infinity. For any affine point $P = (x(t), y(t)) \in C(K(t))$, we will study the divisor class $(P) - (\infty)$ in the Jacobian of C.

Write $d(t) = \alpha f(t)^m$ with $f(t) \in K[t]$ monic and m the largest divisor of $\mathrm{lcm}(2,n)$ such that $d(t)$ is, up to a constant, an mth power. By the assumptions, $1 \le m < \mathrm{lcm}(2,n)$. Define $\ell := \mathrm{lcm}(2,n)/m \in \mathbb{Z}_{\ge 2}$. For every extension field $L \supset K$, the polynomial $s^\ell - f(t)$ is irreducible in $L[t,s]$ since otherwise $f(t)$ would be a kth power for some divisor $k > 1$ of ℓ, which is not the case. Hence we have an irreducible curve D/K, defined by

$$D:\ s^\ell = f(t).$$

Note that the curve D is taken such that over the function field $K(D) \supset K(t) \supset K$, the curves C and C_0 are isomorphic: over $K(D)$ one has

$$d(t) = \alpha f(t)^m = \alpha s^{\mathrm{lcm}(2,n)},$$

hence one obtains the isomorphism

$$C \xrightarrow{\sim} C_0:\ (x,y) \mapsto (x s^{-\mathrm{lcm}(2,n)/n}, y s^{-\mathrm{lcm}(2,n)/2}).$$

Now suppose that $P = (x(t), y(t)) \in C(K(t))$ is an affine point of C over $K(t)$. Via the isomorphism above, P defines a morphism $\varphi_P : D \to C_0$ given by

$$\varphi_P : (t,s) \mapsto (x(t) s^{-\mathrm{lcm}(2,n)/n}, y(t) s^{-\mathrm{lcm}(2,n)/2}).$$

The Jacobian of C_0 will be denoted J_0. Composing φ_P with an embedding $C_0 \to J_0$ we obtain a morphism, which we will also denote by φ_P, from D to J_0. Summarizing, this defines

$$C(K(t)) \to \mathrm{Mor}(D, J_0):\ P \mapsto \varphi_P.$$

(Note that the point(s) at infinity on C give rise to constant morphisms.) Since $\mathrm{Mor}(D, J_0)$ is a group (in fact, one may identify it with $J_0(K(D))$), the above assignment by linearity extends to a homomorphism

$$\varphi : J(K(t)) \to \mathrm{Mor}(D, J_0).$$

PROPOSITION 2.1. *Let $P \in C(K(t))$ with $P \notin C(K)$ and $y(P) \neq 0$. Then $\varphi((P) - (\infty)) \in \mathrm{Mor}(D, J_0)$ has infinite order. In particular, $(P) - (\infty)$ defines an element of infinite order in $J(K(t))$.*

The proof adapts the argument presented in Section 4 of [ST], and runs as follows. Using the above notation, suppose, on the contrary, that $\varphi((P) - (\infty))$ has finite order. This means that the map $D \to J_0$ it defines has a finite image. Since D is absolutely irreducible, so is this image, which implies it consists of only one point. This point is the image of D under the composition $D \xrightarrow{\varphi_P} C_0 \to J_0$. Because $C_0 \to J_0$ is injective, one concludes that $\varphi_P : D \to C_0$ is constant. A direct verification using the given conditions on P shows that this is impossible. ∎

REMARK 2.2. The equation $y^2 = x^n + \alpha a f(t)^m$ with $f \in K[t]$ of positive degree obviously has no solutions $(x, y) \in K \times K$. Hence the only points in $C(K)$ are the points at infinity. Furthermore, the definition of the integer m in this section implies that a point in $C(K(t))$ with y-coordinate 0 exists only when $m = n$ and $-\alpha a$ is an nth power in K. It is easy to verify that for such a point P, indeed $(P) - (\infty)$ defines a torsion point in $J(K(t))$ (of order 2 when n is odd, and of order dividing n otherwise).

3. Rational curves on some threefolds. In this section, a, b are nonzero rational numbers. First, the threefold $\mathcal{X}$ with equation $b(y_1^2 - x_1^n) = a(y_2^2 - x_2^n)$ is studied.

LEMMA 3.1. *$\mathcal{X}$ is birational to $\mathbb{A}^3$ over $\mathbb{Q}$.*

Proof. First suppose that $n = 2m + 1$. The birational map

$$(x_1, y_1, x_2, y_2) \mapsto (T, p, q, r) := (x_1, y_1 \cdot x_1^{-m}, x_2/x_1, y_2 \cdot x_1^{-m})$$

shows that $\mathcal{X}$ is birational to the threefold given by

$$(aq^n - b)T = ar^2 - bp^2.$$

Since this equation has degree one in the variable T, the conclusion follows for n odd.

Now suppose $n = 2m$. In this case, the map

$$(x_1, y_1, x_2, y_2) \mapsto (T, u, v, w) := (y_1 - x_1^m, x_1, x_2, (y_2 - x_2^m)/(y_1 - x_1^m))$$

shows that $\mathcal{X}$ is birational to the threefold given by

$$(aw^2 - b)T = -2(awv^m - bu^m).$$

Again, the equation has degree one in T, which finishes the proof. ∎

It is now straightforward to finish the proof of our main result. Namely, take, depending on n being even or odd, three (sufficiently general) rational functions $p(t), q(t), r(t)$ (or $u(t), v(t), w(t)$). Use the linear equation in the proof of the lemma above to find a corresponding $T(t)$. From this, via the birational map given above, find $x_1(t), y_1(t), x_2(t), y_2(t)$ and proceed as explained in the introduction to obtain a rational function $d(t)$. Clearing denominators one ends up with a situation where Proposition 2.1 is applicable, and the result follows. ∎

Now consider the threefold $\mathcal{Y}$ which corresponds to the case where moreover one desires the polynomial $d(t)$ in the main theorem to be a square. For this, one uses the birational map from $\mathcal{X}$ to $\mathbb{A}^3$ from the lemma. Since $\mathcal{Y}$ is a double cover of $\mathcal{X}$, this yields an explicit birational map over $\mathbb{Q}$ from $\mathcal{Y}$ to a double cover of $\mathbb{A}^3$. As before, the cases of n odd and n even are considered separately.

First, suppose $n = 2m + 1$. Using the variables p, q, r introduced before, one finds that $\mathcal{Y}$ is birational to the threefold with equation

$$(aq^n - b)h^2 = p^2q^n - r^2.$$

Now put $q = u^2$, where u is an indeterminate. Over $\mathbb{Q}(u)$ the above homogeneous quadratic equation in the variables p, r, h defines a quadratic curve with a rational point $(p : r : h) = (1 : u^n : 0)$. It is straightforward to parametrize this quadratic curve over $\mathbb{Q}(u)$. As a result, one obtains a dominant, rational map of degree 2 defined over $\mathbb{Q}$ from $\mathbb{A}^3$ to the threefold $\mathcal{Y}$. We have shown the following.

Corollary 3.2. *In case n is odd, for any pair a, b of nonzero rational numbers, one can choose the polynomial $d(t) \in \mathbb{Q}[t]$ as in Theorem* 1.1 *to be a square.*

Next, take $n = 2m$. Using the variables u, v, w, T and $\zeta := z/(2(aw^2 - b))$ one obtains the equation

$$\zeta^2 = -abw(u^m w - v^m)(av^m w - bu^m)$$

for a threefold birational to $\mathcal{Y}$ over $\mathbb{Q}$. Observe that this equation defines an elliptic curve E over the field $\mathbb{Q}(u, v)$. One way of constructing rational curves over $\mathbb{Q}$ on $\mathcal{Y}$ would be to find nontrivial points in $E(\mathbb{Q}(u, v))$. Indeed, if $(w(u, v), \zeta(u, v))$ is such a point, then for general rational functions $u(t), v(t)$ one obtains $w(t) := w(u(t), v(t))$ and this easily leads to a rational curve as desired. Unfortunately, this idea fails, as the following proposition shows.

Proposition 3.3. *With notation as above, $E(\mathbb{Q}(u, v))$ is a finite group.*

Proof. Put $Y := a^2bu^mv^m\zeta$ and $X := -a^2bu^mv^mw$. Then the equation for E becomes

$$Y^2 = X(X + a^2bv^{2m})(X + ab^2u^{2m}).$$

Let K be an algebraic closure of $\mathbb{Q}(v)$. We will show the even stronger result that over $K(u)$, the Mordell–Weil group is finite.

Observe that our elliptic curve over $K(u)$ is the generic fiber of an elliptic surface $\mathcal{E} \to \mathbb{P}^1$ over K. This surface has fibers of type I_{4m} over 0 and over ∞, and fibers of type I_2 over all u such that $bu^{2m} = av^{2m}$. From standard theory of elliptic surfaces (cf. [SchS, especially Sections 5, 6, 10]) one finds that the second Betti number $h^2(\mathcal{E})$ is $12m - 2$ and the Hodge number $h^{0,2}(\mathcal{E})$ is $m - 1$. As a result, the rank $\rho(\mathcal{E})$ of the Néron–Severi group of $\mathcal{E}$ satisfies $\rho \le h^2 - 2h^{0,2} = 10m$. The Shioda–Tate formula now implies that the

Mordell–Weil rank r of $\mathcal{E} \to \mathbb{P}^1$ over K satisfies

$$r + 2 + (4m - 1) + (4m - 1) + 2m \cdot (2 - 1) \le 10m,$$

hence $r = 0$. This implies the proposition. ∎

The argument above shows that for every $m > 0$, the elliptic surface $\mathcal{E} \to \mathbb{P}^1$ over K is a so-called semi-stable extremal elliptic surface (with geometric genus $p_g = m - 1$; cf. [Kl]). For $m \in \{1, 2, 4\}$ the surface corresponds to certain torsion-free genus zero congruence subgroups of $\mathrm{PSL}(2, \mathbb{Z})$ (of index 12, 24 and 48, respectively; see [TY]).

The (finite) group of sections of $\mathcal{E} \to \mathbb{P}^1$ over K is in fact isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Indeed, a straightforward calculation (cf. [Si, Chapter X, Prop. 1.4]) shows that in $E(K(u))$ the point $(0, 0)$ is divisible by 2 but not by 4, and other points of order 2 are not divisible by 2. So the 2-part of $E(K(u))$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z}$. If it contained a point of prime order $p > 2$, then the modular curve corresponding to $\Gamma(4; 2, 1, 1) \cap \Gamma_1(p)$ (see [TY] for notation) would be a rational curve, which is not the case.

Note that the points of order 4 in $E(K(u))$ are obtained by taking $X = \alpha u^m$ with $\alpha \in K$ satisfying $\alpha^2 = a^3 b^3 v^{2m}$. In particular, $\alpha \notin \mathbb{Q}(v)$ in general. The leading coefficient $\beta \in K$ of the corresponding Y-coordinate $Y = \beta u^{2m} + \cdots$ satisfies $\beta^2 = a^4 b^5 v^{2m}$. Hence only when a, b are both squares in $\mathbb{Q}$, can the point(s) of order 4 actually be used to construct rational curves as desired on the threefold $\mathcal{Y}$.

4. Three- and four-tuples of curves. In this last section Theorems 1.2 and 1.3 are proven. Obviously, Theorem 1.3 implies the conclusion of Theorem 1.2 for n odd. So we first prove Theorem 1.2 assuming that $n = 2m$ is even.

Let m be a positive integer, and $a, b, c \in \mathbb{Q}^\times$. Consider the four-dimensional variety $\mathcal{Z} = \mathcal{Z}_m$ defined by

$$\mathcal{Z}: \; bc(y_1^2 - x_1^{2m}) = ac(y_2^2 - x_2^{2m}) = ab(y_3^2 - x_3^{2m}).$$

Using the same ideas as in Section 3, we will construct sufficiently general (meaning that $y_1^2 - x_1^{2m}$ is nonconstant on them, and moreover not equal to a times a $2m$th power) rational curves in $\mathcal{Z}$ over $\mathbb{Q}$. Put $K := \mathbb{Q}(x_1, x_2, x_3)$. The equations defining $\mathcal{Z}$ may be regarded as defining a genus one curve E over K. This curve contains the K-rational points

$$(y_1, y_2, y_3) = (\pm x_1^m, \pm x_2^m, \pm x_3^m).$$

It is straightforward (e.g., using the computer algebra system Magma) to use one of these points as zero element for a group law on E and calculate a nontrivial linear combination of the other points. As an example, one finds

y_1, y_2, y_3 equal respectively to

$$\frac{(3a^2x_3^{4m}x_2^{4m} - 2acx_1^{2m}x_2^{4m}x_3^{2m} - 2abx_3^{4m}x_1^{2m}x_2^{2m} - c^2x_1^{4m}x_2^{4m} + 2bcx_1^{4m}x_2^{2m}x_3^{2m} - b^2x_3^{4m}x_1^{4m})x_1^m}{a^2x_3^{4m}x_2^{4m} - 2abx_3^{4m}x_1^{2m}x_2^{2m} + b^2x_3^{4m}x_1^{4m} - 2acx_1^{2m}x_2^{4m}x_3^{2m} - 2bcx_1^{4m}x_2^{2m}x_3^{2m} + c^2x_1^{4m}x_2^{4m}},$$

$$\frac{(a^2x_3^{4m}x_2^{4m} - 2acx_1^{2m}x_2^{4m}x_3^{2m} + 2abx_3^{4m}x_1^{2m}x_2^{2m} + c^2x_1^{4m}x_2^{4m} + 2bcx_1^{4m}x_2^{2m}x_3^{2m} - 3b^2x_3^{4m}x_1^{4m})x_2^m}{a^2x_3^{4m}x_2^{4m} - 2abx_3^{4m}x_1^{2m}x_2^{2m} + b^2x_3^{4m}x_1^{4m} - 2acx_1^{2m}x_2^{4m}x_3^{2m} - 2bcx_1^{4m}x_2^{2m}x_3^{2m} + c^2x_1^{4m}x_2^{4m}},$$

$$-\frac{(a^2x_3^{4m}x_2^{4m} - 2abx_3^{4m}x_1^{2m}x_2^{2m} + b^2x_3^{4m}x_1^{4m} + 2acx_1^{2m}x_2^{4m}x_3^{2m} + 2bcx_1^{4m}x_2^{2m}x_3^{2m} - 3c^2x_1^{4m}x_2^{4m})x_3^m}{a^2x_3^{4m}x_2^{4m} - 2abx_3^{4m}x_1^{2m}x_2^{2m} + b^2x_3^{4m}x_1^{4m} - 2acx_1^{2m}x_2^{4m}x_3^{2m} - 2bcx_1^{4m}x_2^{2m}x_3^{2m} + c^2x_1^{4m}x_2^{4m}}.$$

In fact, the following Magma code produces this (we use the notation $K = \mathbb{Q}(a,b,c,x_1,x_2,x_3)$ and take $m = 1$):

```
> P<y1,y2,y3,y4>:=ProjectiveSpace(K,3);
> C:=Curve(P,[a*c*(y2^2-y4^2*x2^2)-b*c*(y1^2-y4^2*x1^2),
             a*c*(y2^2-y4^2*x2^2)-b*a*(y3^2-y4^2*x3^2)]);
> P:=C![x1,x2,x3,1];
> E,phi:=EllipticCurve(C,P);
> Q:=C![-x1,x2,x3,1];
> S:=C![x1,x2,-x3,1];
> som:=phi(Q)+phi(S);
> Inverse(phi)(som);
```

It is easy to deduce, from this, rational curves in $\mathcal{Z}$ as desired. Hence Theorem 1.2 follows for n even. ∎

Lastly, consider $a, b, c, d \in \mathbb{Q}^\times$ and an integer $m \geq 1$. Clearly it suffices to prove Theorem 1.3 for a, b, c, d for pairwise distinct. We assume this condition from now on (it will guarantee that the variety introduced below is geometrically irreducible).

Define the five-dimensional variety $\mathcal{W}$ by

$$\frac{y_1^2 - x_1^{2m+1}}{a} = \frac{y_2^2 - x_2^{2m+1}}{b} = \frac{y_3^2 - x_3^{2m+1}}{c} = \frac{y_4^2 - x_4^{2m+1}}{d}.$$

Let u be an indeterminate. Working over $\mathbb{Q}(u)$, we intersect $\mathcal{W}$ with the linear space defined by

$$u^{-2}x_1 = x_2 = x_3 = x_4.$$

The intersection is a surface $\mathcal{S}$, in the variables y_1, y_2, y_3, y_4 and x $(= x_2 = x_3 = x_4 = x_1/u^2)$ given by

$$bcd(y_1^2 - u^{4m+2}x^{2m+1}) = acd(y_2^2 - x^{2m+1}) = abd(y_3^2 - x^{2m+1}) = abc(y_4^2 - x^{2m+1}).$$

Using new variables $\eta_j = y_j x^{-m}$ one shows that $\mathcal{S}$ is birational over $\mathbb{Q}(u)$ to the surface $\mathcal{T}$ with equations

$$bcd(\eta_1^2 - u^{4m+2}x) = acd(\eta_2^2 - x) = abd(\eta_3^2 - x) = abc(\eta_4^2 - x).$$

Eliminating x from these equations shows that $\mathcal{T}$ is birational over $\mathbb{Q}(u)$ to the cone in $\mathbb{A}^3$ over the curve C defined as

$$C: \begin{cases} (d-c)(d\eta_2^2 - b) = (d-b)(d\eta_3^2 - c), \\ (d-c)(d\eta_1^2 - a) = (du^{4m+2} - a)(d\eta_3^2 - c). \end{cases}$$

The curve C has genus one and contains the rational points

$$(\eta_1, \eta_2, \eta_3) = (\pm u^{2m+1}, \pm 1, \pm 1).$$

Using one of them as zero for a group law on C, it is easy to combine others and construct new $\mathbb{Q}(u)$-rational points on C. An example of a point obtained in this way, using Magma quite analogously to the case described above, is

$$\eta_1 = \frac{v(-c^2v^4 + 2bcv^4 + 2cdv^4 - b^2v^4 + 2bdv^4 - d^2v^4 - 2acv^2 - 2abv^2 - 2adv^2 + 3a^2)}{c^2v^4 - 2bcv^4 + 2cdv^4 + b^2v^4 + 2bdv^4 - 3d^2v^4 - 2acv^2 - 2abv^2 + 2adv^2 + a^2},$$

$$\eta_2 = \frac{c^2v^4 + 2bcv^4 - 2cdv^4 - 3b^2v^4 + 2bdv^4 + d^2v^4 - 2acv^2 + 2abv^2 - 2adv^2 + a^2}{c^2v^4 - 2bcv^4 + 2cdv^4 + b^2v^4 + 2bdv^4 - 3d^2v^4 - 2acv^2 - 2abv^2 + 2adv^2 + a^2},$$

$$\eta_3 = -\frac{-3c^2v^4 + 2bcv^4 + 2cdv^4 + b^2v^4 - 2bdv^4 + d^2v^4 + 2acv^2 - 2abv^2 - 2adv^2 + a^2}{c^2v^4 - 2bcv^4 + 2cdv^4 + b^2v^4 + 2bdv^4 - 3d^2v^4 - 2acv^2 - 2abv^2 + 2adv^2 + a^2}.$$

with $v = u^{2m+1}$. Now it is straightforward, as in the previous cases, to complete the proof of Theorem 1.3 (and hence of Theorem 1.2). ∎

References

[Be] T. G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) 55 (1990), 259–266.

[HL] Y. Hellegouarch et M. Lozach, *Équation de Pell et points d'ordre fini*, Publ. Math. Orsay 86 (1986), 72–95.

[Kl] R. Kloosterman, *Extremal elliptic surfaces and infinitesimal Torelli*, Michigan Math. J. 52 (2004), 141–161.

[KW] M. Kuwata and L. Wang, *Topology of rational points on isotrivial elliptic surfaces*, Int. Math. Res. Notices 1993, no. 4, 113–123.

[MT] S. J. Meagher and J. Top, *Twists of genus three curves over finite fields*, Finite Fields Appl. 16 (2010), 347–368.

[Me] J.-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), 919–922.

[Sch] A. Schinzel, *On some problems in the arithmetical theory of continued fractions, II*, Acta Arith. 7 (1962), 287–298; Corrigendum, ibid. 47 (1986), 295.

[SchS] M. Schütt and T. Shioda, *Elliptic surfaces*, in: Algebraic Geometry in East Asia—Seoul 2008, Adv. Stud. Pure Math. 60, Math. Soc. Japan, Tokyo, 2010, 51–160.

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin, 1986.

[ST] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. 8 (1995), 943–973.

[TY] J. Top and N. Yui, *Explicit equations of some elliptic modular surfaces*, Rocky Mountain J. Math. 37 (2007), 663–687.

[U] 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

Jaap Top
JBI-RuG, P.O. Box 407
9700AK Groningen, the Netherlands
E-mail: j.top@rug.nl

Maciej Ulas
Institute of Mathematics
Jagiellonian University
Łojasiewicza 6
30-348 Kraków, Poland
E-mail: Maciej.Ulas@im.uj.edu.pl, maciej.ulas@gmail.com

Received on 15.6.2009
and in revised form on 6.7.2011 (6058)