ACTA ARITHMETICA
174.2 (2016)

On the torsion of the Jacobians of the hyperelliptic curves $y^2 = x^n + a$ and $y^2 = x(x^n + a)$

by

Tomasz Jędrzejak (Szczecin)

1. Introduction. The hyperelliptic curves (over $\mathbb{Q}$)

$$C^{n,a} : y^2 = x^n + a, \quad C_{n,a} : y^2 = x(x^n + a)$$

(where n is a positive integer and a is a nonzero rational) and their respective Jacobian varieties $J^{n,a}$ and $J_{n,a}$ are the natural generalization of the famous families of elliptic curves

$$E^a : y^2 = x^3 + a, \quad E_a : y^2 = x^3 + ax.$$

The j-invariants of E^a and E_a are 0 and 1728 respectively. Both families of curves have complex multiplication: E^a by a third and E_a by a fourth root of unity. Let $E^a(\mathbb{Q})_{\mathrm{tors}}$ and $E_a(\mathbb{Q})_{\mathrm{tors}}$ denote the torsion subgroups of the Mordell–Weil groups $E^a(\mathbb{Q})$ and $E_a(\mathbb{Q})$ respectively. The following results are well known (cf. [12, Theorems 5.2 and 5.3, p. 134]):

$$E^a(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } a \neq \text{square and } a \neq \text{cube and } a \neq -432, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } a \neq \text{square and } a = \text{cube}, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } a = \text{square and } a \neq \text{cube or } a = -432, \\ \mathbb{Z}/6\mathbb{Z} & \text{if } a = \text{square and } a = \text{cube}. \end{cases} \tag{1.1}$$

$$E_a(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } a \neq 4 \text{ and } a \neq -\text{ square}, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } a = -\text{ square}, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } a = 4. \end{cases} \tag{1.2}$$

(without loss of generality we can assume that a is a nonzero integer, 6th or 4th powerfree respectively).

2010 *Mathematics Subject Classification*: Primary 11G10, 11G20, 11G25; Secondary 11L05, 11L10.
Key words and phrases: hyperelliptic curve, Jacobian, Gauss sum, Jacobi sum, Jacobstahl sum, torsion part, zeta function.
Received 19 April 2015; revised 20 January 2016.
Published online 22 June 2016.

It is of interest to characterize the torsion parts $J^{n,a}(\mathbb{Q})_{\rm tors}$ and $J_{n,a}(\mathbb{Q})_{\rm tors}$ of the Mordell–Weil groups $J^{n,a}(\mathbb{Q})$ and $J_{n,a}(\mathbb{Q})$. One may expect that there are analogies between $E^a(\mathbb{Q})_{\rm tors}$ and $J^{n,a}(\mathbb{Q})_{\rm tors}$, and between $E_a(\mathbb{Q})_{\rm tors}$ and $J_{n,a}(\mathbb{Q})_{\rm tors}$.

In [9, Theorem 4.1] the author proved that

$$
\begin{aligned}
(1.3)\quad & J^{p,a}(\mathbb{Q})_{\rm tors} \\
&\cong \begin{cases}
\{0\} & \text{if } a \neq \text{square and } a \neq p^* \text{ times a square and} \\
 & \quad a \neq p\text{th power}, \\
\mathbb{Z}/2\mathbb{Z} & \text{if } a \neq \text{square and } a \neq p^* \text{ times a square and} \\
 & \quad a = p\text{th power}, \\
\mathbb{Z}/p\mathbb{Z} & \text{if } a = \text{square and } a \neq p\text{th power}, \\
\mathbb{Z}/2p\mathbb{Z} & \text{if } a = \text{square and } a = p\text{th power}, \\
\{0\} \text{ or } \mathbb{Z}/p\mathbb{Z} & \text{if } a = p^* \text{ times a square and } a \neq p\text{th power}, \\
\mathbb{Z}/2\mathbb{Z} \text{ or } \mathbb{Z}/2p\mathbb{Z} & \text{if } a = p^* \text{ times a square and } a = p\text{th power},
\end{cases}
\end{aligned}
$$

where p is an odd prime and $p^* = (-1)^{(p-1)/2}\, p$. For $a \notin p^*\mathbb{Z}^2$ we have a nice analogy between (1.3) and (1.1). Moreover, the author also considered in [10] another generalization, namely the superelliptic curves

$$C^{q,p,a} : y^q = x^p + a,$$

where $q < p$ are primes, and proved that

$$
(1.4)\quad J^{3,5,a}(\mathbb{Q})_{\rm tors} \cong \begin{cases}
\{0\} & \text{if } a \neq 3\text{th power and } a \neq 5\text{th power}, \\
\mathbb{Z}/3\mathbb{Z} & \text{if } a \neq 3\text{th power and } a = 5\text{th power}, \\
\mathbb{Z}/5\mathbb{Z} & \text{if } a = 3\text{th power and } a \neq 5\text{th power}, \\
\mathbb{Z}/15\mathbb{Z} & \text{if } a = 3\text{th power and } a = 5\text{th power}.
\end{cases}
$$

Note that $E_a(\mathbb{Q})_{\rm tors}$ is a 2-group for any nonzero a. Moreover, by (1.2),

$$(1.5)\qquad E_a(\mathbb{Q})_{\rm tors} = E_a(\mathbb{Q})[2] \quad \text{for } a \neq 4$$

(note that $E_4(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$). In [11, Theorem 2.2] we proved an analogous result for $J_{4,a}(\mathbb{Q})$:

$$(1.6)\qquad J_{4,a}(\mathbb{Q})_{\rm tors} = J_{4,a}(\mathbb{Q})[2] \quad \text{for any } a \in \mathbb{Q}\backslash\{0\}.$$

Such a characterization was used to give interesting applications to ranks of octic twists. Obviously we explicitly determined $J_{4,a}(\mathbb{Q})[2]$ in terms of a.

In [9, Theorems 3.2, 3.11] the author proved that $J_{6,a}(\mathbb{Q})_{\rm tors}$ is a 2-group of order ≤ 64 for any nonzero rational a. Moreover,

$$J_{6,a}(\mathbb{Q})_{\rm tors} = J_{6,a}(\mathbb{Q})[2] \quad \text{for } a \notin 4\mathbb{N}^4 \cup \{-1728, -1259712\}$$

(note that here without loss of generality we assume that a is a 12th powerfree integer). For the excluded values a, with possible exception of $a = -1728$, the group $J_{6,a}(\mathbb{Q})$ has an element of order 4.

In this paper we consider the curves $C^{n,a}$ and $C_{n,a}$, and their Jacobians $J^{n,a}$ and $J_{n,a}$. Our aim is to characterize the torsion parts of $J^{n,a}(\mathbb{Q})$ and of $J_{n,a}(\mathbb{Q})$. We show that any prime divisor of $\#J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ and $\#J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ is equal to 2 or divides n. Moreover, we give explicit upper bounds for these orders, and say something about the structure of these groups (see Theorems 1 and 2 below). We also prove that $J_{8,a}(\mathbb{Q})_{\mathrm{tors}} = J_{8,a}(\mathbb{Q})[2]$ for any $a \in \mathbb{Q}\backslash\{0\}$, and explicitly compute $J_{8,a}(\mathbb{Q})[2]$ in terms of a (Theorem 4). In Section 5 we give an (almost full) characterization of $J_{p,a}(\mathbb{Q})_{\mathrm{tors}}$, where p is an odd prime, and of $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$, where n is a composite number ≤ 8. This, together with the results from Section 4 and from [9] and [11], gives an almost complete description of the groups $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ and $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$, where $n \leq 8$ or n is an odd prime.

The main ingredients in the proofs are explicit computations of zeta functions of the title curves in some cases, which are of independent interest, and applications of the Chebotarev Density Theorem (in the formulation of [16, pp. 35–36]) and its consequences (e.g. the Dirichlet Prime Number Theorem).

THEOREM 1. *For any prime p we have*

$$p \,|\, \#J_{n,a}(\mathbb{Q})_{\mathrm{tors}} \;\Rightarrow\; p = 2 \vee p \,|\, n,$$

and

$$\mathrm{ord}_2(\#J_{n,a}(\mathbb{Q})_{\mathrm{tors}}) \leq \begin{cases} \frac{1}{2}n\,\mathrm{ord}_2(2n) & \text{if } 2 \,|\, n, \\ \frac{1}{2}(n-1) & \text{if } 2 \nmid n, \end{cases}$$

and for odd primes

$$\mathrm{ord}_p(\#J_{n,a}(\mathbb{Q})_{\mathrm{tors}}) \leq \begin{cases} \frac{1}{2}n\,\mathrm{ord}_p(n) & \text{if } 2 \,|\, n, \\ \frac{1}{2}(n-1)\,\mathrm{ord}_p(n) & \text{if } 2 \nmid n. \end{cases}$$

Moreover, for any nonzero a,

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} &\subset J_{n,a}(\mathbb{Q})_{\mathrm{tors}} \quad \text{if } 2 \mid n, \\ \mathbb{Z}/n\mathbb{Z} &\subset J_{n,a}(\mathbb{Q})_{\mathrm{tors}} \quad \text{if } 2 \nmid n. \end{aligned}$$

THEOREM 2. *For any prime p we have*

$$p \,|\, \#J^{n,a}(\mathbb{Q})_{\mathrm{tors}} \;\Rightarrow\; p = 2 \vee p \,|\, n,$$

and

$$\mathrm{ord}_2(\#J^{n,a}(\mathbb{Q})_{\mathrm{tors}}) \leq \begin{cases} \frac{1}{2}(n-2)\,\mathrm{ord}_2(n) & \text{if } 2 \,|\, n, \\ \frac{1}{2}(n-1) & \text{if } 2 \nmid n, \end{cases}$$

and for odd primes p,

$$\operatorname{ord}_p(\#J^{n,a}(\mathbb{Q})_{\mathrm{tors}}) \le \begin{cases} \frac{1}{2}(n-2)\operatorname{ord}_p(n) & \text{if } 2 \mid n, \\ \frac{1}{2}(n-1)\operatorname{ord}_p(n) & \text{if } 2 \nmid n. \end{cases}$$

Moreover,

$$\mathbb{Z}/m\mathbb{Z} \subset J^{2m,a}(\mathbb{Q})_{\mathrm{tors}},$$
$$(\mathbb{Z}/m\mathbb{Z})^2 \subset J^{2m,c^2}(\mathbb{Q})_{\mathrm{tors}},$$
$$\mathbb{Z}/(2m+1)\mathbb{Z} \subset J^{2m+1,c^2}(\mathbb{Q})_{\mathrm{tors}},$$

for any nonzero a, c, and any positive integer m.

Corollary 3. *If $n = 2^k$ then (for any a) $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ and $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ are 2-groups of order $\le 2^{(k+1)2^{k-1}}$ and $\le 2^{k(2^{k-1}-1)}$ respectively. On the other hand, if n is odd then $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ is never a 2-group. Similarly, if n is even but not a power of 2 then $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ is never a 2-group.*

Theorem 4. *We have*

$$J_{8,a}(\mathbb{Q})_{\mathrm{tors}} = J_{8,a}(\mathbb{Q})[2] \quad \text{for any } a \in \mathbb{Q} \setminus \{0\}.$$

Explicitly (here without loss of generality a is a 16th powerfree integer)

$$J_{8,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } a \ne 4c^4 \text{ and } a \ne -c^2, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } a = 4c^4 \text{ or } (a = -c^2 \text{ and } c \ne b^2), \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } a = -c^4 \text{ and } c \ne b^2 \text{ and } c \ne 2b^2, \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } a = -c^8 \text{ or } a = -16c^8. \end{cases}$$

2. Jacobians of hyperelliptic curves. In this preliminary section we collect necessary notation and results concerning Jacobians of algebraic curves.

For a smooth projective curve C defined over a field K let $\operatorname{Div}(C)$ denote its divisor group, i.e., the free abelian group generated by the points of C. By definition, the divisor $D \in \operatorname{Div}(C)$ is *K-rational* if it is invariant under the action of the absolute Galois group $\operatorname{Gal}(\overline{K}/K)$. Note that if $D = n_1P_1 + \cdots + n_rP_r$ with $n_1, \ldots, n_r$ nonzero integers, then to say that D is K-rational does not mean that $P_1, \ldots, P_r \in C(K)$. It suffices for $\operatorname{Gal}(\overline{K}/K)$ to permute the P_i's in an appropriate fashion. The number $n_1 + \cdots + n_r$ is called the *degree* of D. Note that if h is an element of the function field of C then the divisor $\operatorname{div}(h) := \sum_{P \in C} \operatorname{ord}_P(h)P$ is called *principal* and has degree 0. Let J_C denote the Jacobian variety of C. Note that as a group, J_C is the quotient group of the degree zero divisors modulo the principal divisors. We denote the corresponding equivalence relation by $\sim$. Let $J_C(K)_{\mathrm{tors}}$ denote

the subgroup of K-rational torsion elements of $J_C(K)$, and by $J_C(K)[m]$ the kernel of multiplication by m on $J_C(K)$.

By a *hyperelliptic curve* of genus g defined over K ($\operatorname{char} K \neq 2$) we mean an absolutely irreducible nonsingular curve C defined by an equation of the form $y^2 = f(x)$ where $f \in K[x]$ is monic and has degree $2g+1$ or $2g+2$. In the first case, C is called an *imaginary hyperelliptic curve*, and in the second a *real hyperelliptic curve*. In the imaginary model there exists only one point at infinity, say ∞, but in the real model we have two points at infinity, ∞^+ and ∞^-. Let S denote the set of points at infinity on C. Then elements of the set $C(\overline{K}) := \{(x,y) \in \overline{K}^2 : y^2 = f(x)\} \cup S$ are called *$\overline{K}$-rational points* on C (if they do not belong to S, we call them *finite* or *affine points*). Similarly we define $C(L)$ for any field $K \subset L \subset \overline{K}$. It is always possible to transform an imaginary model to a real model, but for the converse direction one needs a finite K-rational point on C. For a point $P = (x,y) \in C(\overline{K})$, the *hyperelliptic involution* is given by $\tau(P) := (x,-y)$. Note that $\tau(\infty^{\pm}) = \infty^{\mp}$ and $\tau(\infty) = \infty$.

The following two lemmas concern representations of divisors in J_C.

LEMMA 5. *Any $\overline{K}$-rational divisor of degree 0 on an imaginary hyperelliptic curve C over K of genus g is equivalent to a unique reduced divisor, i.e., a divisor D of the form*

$$D = \sum_{i=1}^{d} P_i - d\infty,$$

where $P_i \in C(\overline{K}) \setminus S$, $P_i \neq \tau(P_j)$ for $i \neq j$, and $0 \leq d \leq g$.

Proof. See [13, Theorem 47]. ∎

LEMMA 6. *Any $\overline{K}$-rational divisor of degree 0 on a real hyperelliptic curve C over K of genus g is equivalent to a unique divisor D of the form*

$$D = \sum_{i=1}^{d_1} P_i - d_1\infty^- + d_2(\infty^+ - \infty^-),$$

where $P_i \in C(\overline{K}) \setminus S$, $P_i \neq \tau(P_j)$ for $i \neq j$, $0 \leq d_1, d_2$, and $d_1 + d_2 \leq g$. In particular, the divisors $k(\infty^+ - \infty^-)$ for $k = 1, \ldots, g$ are not principal and are pairwise inequivalent.

Proof. The first claim follows from [14]. For the second, set $d_1 = 0$ and $d_2 = k$. ∎

The next lemma allows us to compute the group $J_C(K)[2]$.

LEMMA 7. *Let $f(x) = f_1(x) \cdots f_s(x)$, where $f_i \in K[x]$ are distinct monic polynomials of degree t_i irreducible over K, and $t := t_1 + \cdots + t_s$. Let r denote*

the $\mathbb{F}_2$-dimension of $J_C(K)[2]$, i.e.,

$$J_C(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^r, \quad \textit{where} \quad C : y^2 = f(x).$$

If K is a finite field of odd characteristic, then

$$r = \begin{cases} s-2 & \text{if } t \text{ is even and some } t_i \text{ is odd,} \\ s-1 & \text{if } t \text{ is odd or } (s=1 \text{ and } t \equiv 2 \pmod 4), \\ s & \text{if } (s>1 \text{ and all } t_i \text{ are even}) \text{ or } (s=1 \text{ and } t \equiv 0 \pmod 4). \end{cases}$$

If K is an extension of $\mathbb{Q}$, and either t is odd, or t is even and g is even, then

$$r = \begin{cases} s-2 & \text{if } t \text{ is even and some } t_i \text{ is odd,} \\ s-1 & \text{if } t \text{ is odd or all } t_i \text{ are even.} \end{cases}$$

Proof. The first case follows from [5, Theorem 1.4]. The second one follows from [15, Lemmas 6.1 and 12.9]. ∎

3. The curves $y^2 = x\,(x^n + a)$ and $y^2 = x^n + a$. In this section we will prove Theorems 1 and 2. We start with some preliminaries.

The curves $C_{n,a} : y^2 = x(x^n + a)$ and $C^{n,a} : y^2 = x^n + a$ are hyperelliptic of genus $[n/2]$ and $[(n-1)/2]$ respectively, where $[x]$ denotes the integer part of x. Without loss of generality we may assume that a is a $2n$th power-free integer (for both curves). Note that $|\mathrm{disc}(x(x^n + a))| = n^n a^{n+1}$ and $|\mathrm{disc}(x^n + a)| = n^n a^{n-1}$, hence the curves $C_{n,a}$ and $C^{n,a}$ have good reduction at primes $p \nmid 2na$. Consequently, over such primes the Jacobians $J_{n,a}$ and $J^{n,a}$ have good reduction too. The curve $C_{n,a}$ has one point at infinity if n is even, and two such points if n is odd. Conversely, $C^{n,a}$ has two points at infinity if n is even, and one such point if n is odd. All points at infinity are defined over prime fields (i.e., $\mathbb{Q}$ and $\mathbb{F}_p$ after reduction).

In order to compute $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ and $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ it is helpful to consider $J_{n,a}(\mathbb{F}_p)$ and $J^{n,a}(\mathbb{F}_p)$, respectively, for primes $p \nmid 2na$. This is because reduction modulo p induces embeddings (cf. [8, Theorem C.1.4, p. 263])

$$J_{n,a}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow J_{n,a}(\mathbb{F}_p), \tag{3.1}$$

$$J^{n,a}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow J^{n,a}(\mathbb{F}_p), \tag{3.2}$$

and therefore

$$\#J_{n,a}(\mathbb{Q})_{\mathrm{tors}} \,|\, \#J_{n,a}(\mathbb{F}_p), \tag{3.3}$$

$$\#J^{n,a}(\mathbb{Q})_{\mathrm{tors}} \,|\, \#J^{n,a}(\mathbb{F}_p). \tag{3.4}$$

It is well known that the zeta functions of the curves $C_{n,a}$ and $C^{n,a}$ over $\mathbb{F}_p$

($p \nmid 2na$) have the form

$$Z(C_{n,a}/\mathbb{F}_p, T) = \frac{P_{n,a}(T)}{(1-T)(1-pT)},$$
$$Z(C^{n,a}/\mathbb{F}_p, T) = \frac{Q_{n,a}(T)}{(1-T)(1-pT)},$$

where $P_{n,a}(T)$ and $Q_{n,a}(T)$ are polynomials with integer coefficients of degrees $2[n/2]$ and $2[(n-1)/2]$ respectively. Moreover (see for example [8, exercise A.8.11]),

$$\#J_{n,a}(\mathbb{F}_p) = P_{n,a}(1), \tag{3.5}$$

$$\#J^{n,a}(\mathbb{F}_p) = Q_{n,a}(1), \tag{3.6}$$

and

$$P_{n,a}(T) = \prod_{i=1}^{2[n/2]} (1-\alpha_i T), \tag{3.7}$$

$$Q_{n,a}(T) = \prod_{i=1}^{2[(n-1)/2]} (1-\beta_i T), \tag{3.8}$$

where

$$\#C_{n,a}(\mathbb{F}_{p^k}) = p^k + 1 - (\alpha_1^k + \cdots + \alpha_{2[n/2]}^k), \tag{3.9}$$

$$\#C^{n,a}(\mathbb{F}_{p^k}) = p^k + 1 - (\beta_1^k + \cdots + \beta_{2[(n-1)/2]}^k), \tag{3.10}$$

and

$$P_{n,a}(T) = p^{[n/2]} T^{2[n/2]} P_{n,a}(1/(pT)),$$
$$Q_{n,a}(T) = p^{[(n-1)/2]} T^{2[(n-1)/2]} Q_{n,a}(1/(pT)).$$

Therefore we need to calculate $\#C_{n,a}(\mathbb{F}_{p^k})$ for $k = 1, \ldots, [n/2]$ and $\#C^{n,a}(\mathbb{F}_{p^k})$ for $k = 1, \ldots, [(n-1)/2]$. To this end we will use the Jacobi, Gauss and Jacobsthal sums. For the convenience of the reader we list some definitions and give their basic properties (we set $q = p^k$ below).

Definition 8. Let χ denote a character on the finite field $\mathbb{F}_q$ and let $\beta \in \mathbb{F}_q$. The *Gauss sum* $G_k(\beta, \chi)$ over $\mathbb{F}_q$ is defined by

$$G_k(\beta, \chi) := \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e^{2\pi i \operatorname{Tr}(\alpha\beta)/p},$$

where Tr denotes the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. We shall abbreviate $G_k(\chi) := G_k(1, \chi)$.

DEFINITION 9. Let χ and ψ denote characters of orders n and m respectively on $\mathbb{F}_q$.The *Jacobi sum* $J_k(\chi,\psi)$ is defined by

$$J_k(\chi,\psi) := \sum_{\alpha\in\mathbb{F}_q} \chi(\alpha)\psi(1-\alpha)$$

(we set $\chi(0)=0$ if χ is nontrivial, and $\chi(0)=1$ if χ is trivial). The order of $J_k(\chi,\psi)$ is equal to $\operatorname{lcm}(n,m)$.

DEFINITION 10. Let $e\in\mathbb{N}$ and $a\in\mathbb{F}_q$. Let $\left(\frac{\cdot}{q}\right)$ denote the quadratic character of $\mathbb{F}_q$. The *Jacobsthal sums* $\phi_{e,k},\psi_{e,k}$ of order e over $\mathbb{F}_q$ are defined by

$$\phi_{e,k}(a)=\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\left(\frac{x^e+a}{q}\right),\qquad \psi_{e,k}(a)=\sum_{x\in\mathbb{F}_q}\left(\frac{x^e+a}{q}\right).$$

For $a\in\mathbb{Z}$, we define $\phi_{e,k}(a):=\phi_{e,k}(a \bmod p)$ and $\psi_{e,k}(a):=\psi_{e,k}(a \bmod p)$.

LEMMA 11. *Let χ and ψ denote characters on $\mathbb{F}_{p^k}$.*

(1) *A Jacobi sum of order m is an integer of the cyclotomic field $\mathbb{Q}(e^{2\pi i/m})$.*
(2) *If χ and ψ are both trivial then $J_k(\chi,\psi)=p^k$.*
(3) *If exactly one of χ and ψ is trivial then $J_k(\chi,\psi)=0$.*
(4) *If χ is nontrivial then $J_k(\chi,\bar\chi)=-\chi(-1)$.*
(5) *If χ, ψ and $\chi\psi$ are nontrivial then*

$$J_k(\chi,\psi)=\psi(-1)J_k(\bar\chi\bar\psi,\psi)=\chi(-1)J_k(\bar\chi\bar\psi,\chi),$$

and $|J_k(\chi,\psi)|=\sqrt{p^k}$.
(6) *If $\chi\psi$ is nontrivial then*

$$J_k(\chi,\psi)=\frac{G_k(\chi)G_k(\psi)}{G_k(\chi\psi)}.$$

Proof. See [2, Theorems 2.1.1, 2.1.3, and 2.1.5]. ∎

LEMMA 12. *Let $\beta_1,\dots,\beta_l$ be positive integers. Let $\alpha_1,\dots,\alpha_l,\alpha\in\mathbb{F}_q^*$. Set $d_i=\gcd(\beta_i,q-1)$, and let χ_i be a character on $\mathbb{F}_q$ of order d_i $(i=1,\dots,l)$. Then the number of solutions of the diagonal equation $\alpha_1x_1^{\beta_1}+\cdots+\alpha_lx_l^{\beta_l}=\alpha$ in $\mathbb{F}_q$ is given by*

$$q^{l-1}+\sum_{j_1=1}^{d_1-1}\cdots\sum_{j_l=1}^{d_l-1}\chi_1^{j_1}(\alpha\alpha_1^{-1})\cdots\chi_l^{j_l}(\alpha\alpha_l^{-1})J_k(\chi_1^{j_1},\dots,\chi_l^{j_l}).$$

Proof. See [2, Theorem 10.4.2]. ∎

LEMMA 13.

(1) *If $\gcd(e,q-1)=e_1$ then $\phi_{e,k}=\phi_{e_1,k}$.*
(2) *If $e\mid(q-1)$ but $2e\nmid(q-1)$ then $\phi_{e,k}=0$.*
(3) *$\phi_{e,k}(ab^e)=\left(\frac{b}{q}\right)^{e+1}\phi_{e,k}(a)$ for $b\in\mathbb{F}_q^\times$.*

(4) $\#C_{n,a}(\mathbb{F}_q) = q + \phi_{n,k}(a) + \begin{cases} 1 & \text{if } 2 \mid n, \\ 2 & \text{if } 2 \nmid n. \end{cases}$

(5) $\#C^{n,a}(\mathbb{F}_q) = q + \psi_{n,k}(a) + \begin{cases} 2 & \text{if } 2 \mid n, \\ 1 & \text{if } 2 \nmid n. \end{cases}$

(6) $\psi_{2e,k} = \psi_{e,k} + \phi_{e,k}$.

Proof. Generalize the proofs from [2, pp. 184–188] for $\mathbb{F}_p$ to an arbitrary finite field. Note that our definition of $\psi_{e,k}$ differs from the one from [2] by $\left(\frac{a}{q}\right)$ (but agrees with [1]). ∎

Now we show that the title curves are connected to each other.

PROPOSITION 14. *For any a and n we have*

$$Q_{2n,a} = Q_{n,a} \times P_{n,a}.$$

In particular,

$$\#J^{2n,a}(\mathbb{F}_p) = \#J^{n,a}(\mathbb{F}_p)\,\#J_{n,a}(\mathbb{F}_p).$$

Proof. By Lemma 13, we get

$$\#C^{2n,a}(\mathbb{F}_{p^k}) = 2 + p^k + \psi_{2n,k}(a),$$

and

$$\begin{aligned} \#C^{n,a}(\mathbb{F}_{p^k}) + \#C_{n,a}(\mathbb{F}_{p^k}) &= \begin{cases} 2 \\ 1 \end{cases} + p^k + \psi_{n,k}(a) + \begin{cases} 1 \\ 2 \end{cases} + p^k + \phi_{n,k}(a) \\ &= 3 + 2p^k + \psi_{2n,k}(a). \end{aligned}$$

Hence

$$\#C^{2n,a}(\mathbb{F}_{p^k}) = \#C^{n,a}(\mathbb{F}_{p^k}) + \#C_{n,a}(\mathbb{F}_{p^k}) - (1 + p^k).$$

Now by (3.7)–(3.10), we have

$$\begin{aligned} Q_{2n,a}(T) &= \prod_{i=1}^{2(n-1)} (1 - \alpha_i T), \\ Q_{n,a}(T) &= \prod_{i=1}^{2[(n-1)/2]} (1 - \beta_i T), \\ P_{n,a}(T) &= \prod_{i=1}^{2[n/2]} (1 - \gamma_i T), \end{aligned}$$

where

$$\begin{aligned} \#C^{2n,a}(\mathbb{F}_{p^k}) &= 1 + p^k - (\alpha_1^k + \cdots + \alpha_{2(n-1)}^k), \\ \#C^{n,a}(\mathbb{F}_{p^k}) &= 1 + p^k - (\beta_1^k + \cdots + \beta_{2[(n-1)/2]}^k), \\ \#C_{n,a}(\mathbb{F}_{p^k}) &= 1 + p^k - (\gamma_1^k + \cdots + \gamma_{2[n/2]}^k). \end{aligned}$$

Since $n-1=[(n-1)/2]+[n/2]$, we obtain

$$\alpha_1^k+\cdots+\alpha_{2(n-1)}^k=\beta_1^k+\cdots+\beta_{2[(n-1)/2]}^k+\gamma_1^k+\cdots+\gamma_{2[n/2]}^k$$

for any $k\in\mathbb{N}$. Consequently, the polynomials $Q_{2n,a}(T)$ and $Q_{n,a}(T)\times P_{n,a}(T)$ have the same coefficients, and we are done. ∎

REMARK 15. By Proposition 14 and the famous result of Tate [17], the abelian varieties $J^{2n,a}$ and $J^{n,a}\times J_{n,a}$ are isogenous over $\mathbb{F}_p$. This can be proved directly by using the maps $C^{2n,a}\to C^{n,a}$, $(x,y)\mapsto(x^2,y)$, and $C^{2n,a}\to C_{n,a}$, $(x,y)\mapsto(x^2,xy)$.

Using properties of Gauss and Jacobi sums, in some cases we can explicity compute the zeta functions of these curves. First, let us write down a useful result concerning indices.

LEMMA 16. *Let p be an odd prime and let $k\geq 1$ be an integer. Let γ_k denote a generator of the multiplicative group $\mathbb{F}_{p^k}^*$. For $c\in\mathbb{F}_{p^k}^*$ let $\operatorname{ind}_{\gamma_k} c$ denote the index of c with respect to γ_k, i.e., the unique number $n\in\{0,\dots,p^k-2\}$ such that $c=\gamma_k^n$. Set $\gamma:=\gamma_k^{1+p+\cdots+p^{k-1}}$. Then γ is a primitive root modulo p (i.e., a generator of $\mathbb{F}_p^*$) and for $a\in\mathbb{F}_p^*$ we have*

$$\operatorname{ind}_{\gamma_k} a\equiv(1+p+\cdots+p^{k-1})\operatorname{ind}_{\gamma} a \pmod{p^k-1}. \tag{3.11}$$

Proof. This is well known: see for example [6, p. 665]. ∎

PROPOSITION 17. *If $p\equiv -1 \pmod n$ and $p\nmid 2a$ then*

$$Q_{n,a}(T)=(1+pT^2)^{[(n-1)/2]}.$$

In particular,

$$\#J^{n,a}(\mathbb{F}_p)=\begin{cases}(1+p)^{(n-1)/2} & \text{if } 2\nmid n,\\ (1+p)^{(n-2)/2} & \text{if } 2\mid n.\end{cases}$$

Proof. We give the proof only for n even. The case of n odd is similar, and it is left to the reader. Assume that $n=2m$. In order to compute $Q_{n,a}$ we need to find $\#C^{n,a}(\mathbb{F}_{p^k})$ for $k=1,\dots,m-1$. For this purpose we will apply Lemma 12 to the equation $y^2-x^{2m}=a$. By assumption,

$$p^k\equiv\begin{cases}1 \pmod{2m} & \text{if } 2\mid k,\\ -1 \pmod{2m} & \text{if } 2\nmid k,\end{cases}$$

hence

$$\gcd(2m,p^k-1)=\begin{cases}2m & \text{if } 2\mid k,\\ 2 & \text{if } 2\nmid k.\end{cases}$$

Therefore by Lemma 12,

$$\#C^{n,a}(\mathbb{F}_{p^k}) = 2 + p^k + \chi^m(a) \times \begin{cases} \sum_{j=1}^{2m-1} \chi^j(-a) J_k(\chi^m, \chi^j) & \text{if } 2 \mid k, \\ \chi^m(-a) J_k(\chi^m, \chi^m) & \text{if } 2 \nmid k, \end{cases}$$

where χ denotes a character of order $2m$ on $\mathbb{F}_{p^k}$. Note that by Lemma 11, we have $\chi^m(a)\chi^m(-a)J_k(\chi^m, \chi^m) = -\chi^{2m}(-1) = -1$. Hence we can rewrite the above formula as

$$\#C^{n,a}(\mathbb{F}_{p^k}) = 1 + p^k + \chi^m(a) \times \begin{cases} \sum_{\substack{1 \le j \le 2m-1 \\ j \ne m}} \chi^j(-a) J_k(\chi^m, \chi^j) & \text{if } 2 \mid k, \\ 0 & \text{if } 2 \nmid k. \end{cases}$$

Now assume that $k = 2r$. By the Hasse–Davenport formula [2, Corollary 11.5.3] we have

$$J_{2r}(\chi^m, \chi^j) = (-1)^{r-1}(J_2(\widetilde{\chi}^m, \widetilde{\chi}^j))^r,$$

where $\widetilde{\chi}$ denotes a character of order $2m$ on $\mathbb{F}_{p^2}$ such that $\chi = \widetilde{\chi} \circ N_{\mathbb{F}_{p^{2r}}/\mathbb{F}_{p^2}}$. Consequently,

$$\#C^{n,a}(\mathbb{F}_{p^{2r}}) = 1 + p^{2r} + \widetilde{\chi}^{mr}(a) \sum_{\substack{1 \le j \le 2m-1 \\ j \ne m}} (-1)^{r-1} \widetilde{\chi}^{jr}(-a)(J_2(\widetilde{\chi}^m, \widetilde{\chi}^j))^r.$$

In the notation of Lemma 16, any character η of order $2m$ on $\mathbb{F}_{p^2}$ has the form $\eta(x) = \zeta_n^{t \operatorname{ind}_{\gamma_2}(x)}$, where ζ_n is a primitive nth root of unity and $1 \le t \le n$, $\gcd(t, n) = 1$. Then by the same lemma, we have $\widetilde{\chi}(\pm a) = 1$, and so

$$\#C^{n,a}(\mathbb{F}_{p^{2r}}) = 1 + p^{2r} + \sum_{\substack{1 \le j \le 2m-1 \\ j \ne m}} (-1)^{r-1}(J_2(\widetilde{\chi}^m, \widetilde{\chi}^j))^r.$$

Now we compute the Jacobi sums $J_2(\widetilde{\chi}^m, \widetilde{\chi}^j)$. Let $j \in \{1, \dots, 2m-1\}$ and $j \ne m$. By Lemma 11,

$$J_2(\widetilde{\chi}^m, \widetilde{\chi}^j) = \frac{G_2(\widetilde{\chi}^m) G_2(\widetilde{\chi}^j)}{G_2(\widetilde{\chi}^{m+j})}.$$

Since $p \equiv -1 \pmod{2m}$, by [2, Theorem 11.6.1] we get $G_2(\widetilde{\chi}^i) = (-1)^{(p+1)/r_i} p$, where $r_i = 2m/\gcd(2m, i)$ is the order of character $\widetilde{\chi}^i$. Therefore $J_2(\widetilde{\chi}^m, \widetilde{\chi}^j) = p$, and consequently

$$\#C^{n,a}(\mathbb{F}_{p^k}) = \begin{cases} 1 + p^{2r} + (-1)^{r-1} 2(m-1) p^r & \text{if } k = 2r, \\ 1 + p^k & \text{if } 2 \nmid k. \end{cases}$$

Thus, by (3.8) and (3.10), we conclude that

$$Q_{2m,a}(T) = (1 + pT^2)^{m-1},$$

and by (3.6) we get

$$\#J^{2m,a}(\mathbb{F}_p) = (1+p)^{m-1},$$

and the assertion follows. ∎

PROPOSITION 18. *If $p \equiv -1 \pmod{2n}$ and $p \nmid a$ then*

$$P_{n,a}(T) = (1+pT^2)^{[n/2]}.$$

In particular,

$$\#J_{n,a}(\mathbb{F}_p) = \begin{cases} (1+p)^{(n-1)/2} & \text{if } 2 \nmid n, \\ (1+p)^{n/2} & \text{if } 2 \mid n. \end{cases}$$

Proof. By Propositions 14 and 17, we have

$$P_{n,a}(T) = \frac{Q_{2n,a}(T)}{Q_{n,a}(T)} = \frac{(1+pT^2)^{[(2n-1)/2]}}{(1+pT^2)^{[(n-1)/2]}} = (1+pT^2)^{[n/2]},$$

and we are done. ∎

Now we are ready to prove the first two main results of this paper.

Proof of Theorem 1. First assume that n is even, say $n = 2m$. Let l be a prime such that $l \nmid 2m$. We will show that $l \nmid \#J_{2m,a}(\mathbb{Q})_{\mathrm{tors}}$. By the Chinese Remainder Theorem and the Dirichlet Prime Number Theorem, there exists a prime p such that $p \nmid a$, $p \equiv -1 \pmod{2n}$ and $p \equiv 1 \pmod{l}$. Then by Proposition 18, we get $\#J_{2m,a}(\mathbb{F}_p) = (1+p)^m \equiv 2^m \not\equiv 0 \pmod{l}$, and consequently by (3.3), $l \nmid \#J_{2m,a}(\mathbb{Q})_{\mathrm{tors}}$.

Now we will give the desired upper bound for $\#J_{2m,a}(\mathbb{Q})_{\mathrm{tors}}$. Let $2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ be the prime factorization of n. Choose a prime p such that $p \nmid a$ and $p \equiv -1 + p_i^{\alpha_i} \pmod{p_i^{\alpha_i+1}}$ $(i = 1, \ldots, t)$, and $p \equiv -1 + 2^{\alpha_0+1} \pmod{2^{\alpha_0+2}}$. Again by Proposition 18, we have $\#J_{2m,a}(\mathbb{F}_p) = (1+p)^m$. Since $\mathrm{ord}_2(1+p) = \alpha_0 + 1 = \mathrm{ord}_2(2n)$ and $\mathrm{ord}_{p_i}(1+p) = \alpha_i = \mathrm{ord}_{p_i}(n)$, we see that $\mathrm{ord}_2(\#J_{2m,a}(\mathbb{F}_p)) = m\,\mathrm{ord}_2(2n)$ and $\mathrm{ord}_{p_i}(\#J_{2m,a}(\mathbb{F}_p)) = m\,\mathrm{ord}_{p_i}(n)$. Then (3.3) establishes the formula for even n. Moreover, in the notation of Lemma 7, t is odd and $s \geq 2$, hence $r = \dim_{\mathbb{F}_2} J_{2m,a}(\mathbb{Q})[2] \geq 1$ (in fact the divisor $(0,0) - \infty$ has order 2 in $J_{2m,a}(\mathbb{Q})_{\mathrm{tors}}$).

Now let $n = 2m+1$. We proceed in a similar way. Let l be a prime such that $l \nmid 2(2m+1)$. Then we choose a prime p such $p \nmid a$, $p \equiv -1 \pmod{2n}$ and $p \equiv 1 \pmod{l}$. Consequently, by Proposition 18 and (3.3), we deduce that $l \nmid \#J_{2m+1,a}(\mathbb{Q})_{\mathrm{tors}}$. If we take a prime p such that $p \nmid a$, $p \equiv 1 \pmod 4$ and $p \equiv -1 + p_i^{\alpha_i} \pmod{p_i^{\alpha_i+1}}$ for $i = 1, \ldots, t$, then again by Proposition 18 and (3.3), we have $\mathrm{ord}_2(\#J_{2m+1,a}(\mathbb{Q})_{\mathrm{tors}}) \leq m$ and $\mathrm{ord}_{p_i}(\#J_{2m+1,a}(\mathbb{Q})_{\mathrm{tors}}) \leq m\,\mathrm{ord}_{p_i}(n)$. Now consider the divisor $D = \infty^+ - \infty^- \in J_{2m+1,a}(\mathbb{Q})$. By Lemma 6, D has order $> m$ (= the genus of $C_{2m+1,a}$). On the other hand, $nD = \mathrm{div}(h(x,y))$ where $h(x,y) = -2yx^m + 2x^n + a$. Indeed, h has a zero at ∞^+ of order n, a pole at ∞^- of order n, and no other zeroes or poles.

Consequently, the order of D divides $2m+1$ and is $\geq m+1$, hence it is $2m+1=n$, which is our claim. ∎

Proof of Theorem 2. We only prove the 'moreover' part; the proof of the rest follows by the same method as in the proof of Theorem 1, and it is left to the reader.

Assume that $n=2m$. Let $D_1 := \infty^+ - \infty^- \in J^{2m,a}(\mathbb{Q})$. By Lemma 6, D_1 has order $> m-1$ (= the genus of $C^{2m,a}$). On the other hand, $mD_1 = \operatorname{div}(y-x^m)$, hence D_1 has order m, and so $\mathbb{Z}/m\mathbb{Z} \subset J^{2m,a}(\mathbb{Q})_{\mathrm{tors}}$.

Now assume moreover $a=c^2$ and consider the divisor $D_2 = (0,c)-\infty^-$. Then $mD_2 = \operatorname{div}(x^m+c-y)$. By Lemma 6, the divisors lD_2 for $1 \leq l \leq m-1$ are not principal and are pairwise inequivalent (indeed, take $d_1 = l$ and $d_2 = 0$). Consequently, D_2 has order m. Moreover, by Lemma 6, the divisors kD_1 and lD_2 are pairwise inequivalent for $1 \leq k,l \leq m-1$. Therefore $(\mathbb{Z}/m\mathbb{Z})^2 \subset J^{2m,a}(\mathbb{Q})_{\mathrm{tors}}$.

Now assume $a=c^2$ but $n=2m+1$. Consider the divisor $D_3 = (0,c)-\infty$. By Lemma 5, the divisors kD_3 for $k=1,\dots,m$ are not principal and are pairwise inequivalent, so D_3 has order $\geq m+1$. On the other hand, $(2m+1)D_3$ is principal (it is the divisor of the function $y-c$). Consequently, D_3 has order n, and we are done. ∎

4. The curve $y^2 = x(x^8+a)$. In this section we will prove Theorem 4. By Corollary 3 we know that $J_{8,a}(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group of order $\leq 2^{12} = 4096$. In order to prove Theorem 4, it is sufficient to show that this group has no elements of order 4. To this end we compare $\#J_{8,a}(\mathbb{F}_p)$ with $\#J_{8,a}(\mathbb{F}_p)[2]$, and then use the embedding (3.1).

We start with the description of the groups $J_{8,a}(\mathbb{F}_p)[2]$ (for $p \nmid 2a$) and $J_{8,a}(\mathbb{Q})\,[2]$ (note that we do not need the full characterization over $\mathbb{F}_p$).

Proposition 19. *We have* (*without loss of generality a is a 16th powerfree integer*)*:*

(1)

$$J_{8,a}(\mathbb{F}_p)[2] \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 1 \pmod 4,\ a=-b^2 \text{ and } \left(\frac{b}{p}\right)=-1,\\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } p \equiv 1 \pmod 8,\ a=-b^4 \text{ and } \left(\frac{b}{p}\right)=-1,\\ (\mathbb{Z}/2\mathbb{Z})^5 & \text{if } p \equiv 3 \pmod 4 \text{ and } a=-b^2,\\ (\mathbb{Z}/2\mathbb{Z})^6 & \text{if } p \equiv 5 \pmod 8 \text{ and } a=-b^4,\\ (\mathbb{Z}/2\mathbb{Z})^8 & \text{if } p \equiv 1 \pmod 8 \text{ and } a=-b^8. \end{cases}$$

and

$$(\mathbb{Z}/2\mathbb{Z})^2 \subset J_{8,a}(\mathbb{F}_p)[2] \quad \text{if } a=4b^4.$$

(2)

$$J_{8,a}(\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } a \neq 4b^4 \text{ and } a \neq -b^2, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } a = 4b^4 \text{ or } (a = -c^2 \text{ and } c \neq b^2), \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } a = -b^4 \text{ and } b \neq c^2 \text{ and } b \neq 2c^2, \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } a = -c^8 \text{ or } a = -16c^8. \end{cases}$$

Proof. Let $K = \mathbb{Q}$ or $\mathbb{F}_p$. By Lemma 7, the group $J_{8,a}(K)[2]$ is completely determined by the factorization of the polynomial $f_a(x) := x(x^8+a)$ over K. More precisely, $J_{8,a}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^r$ where r is 1 less than the number of irreducible factors of $f_a(x)$ over K. Obviously for any a, $f_a(x)$ is reducible and has at most nine factors, therefore $\mathbb{Z}/2\mathbb{Z} \subset J_{8,a}(K)[2] \subset (\mathbb{Z}/2\mathbb{Z})^8$ for any a.

We need to consider a few cases. Let ζ_n denote an nth primitive root of unity. First assume that $-a$ is an 8th power in K and $\zeta_8 \in K$. Note that $\zeta_8 \notin \mathbb{Q}$, and $\zeta_8 \in \mathbb{F}_p$ if and only if $p \equiv 1 \pmod 8$. In this case $f(x)$ splits completely over K, hence $J_{8,a}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^8$.

Now assume that $-a = b^8$ ($b \in K$), $\zeta_8 \notin K$ and $\zeta_4 \in K$. Clearly, $\zeta_4 \notin \mathbb{Q}$, and $\zeta_4 \in \mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. In this case we have the factorization

$$f_a(x) = x(x-b)(x+b)(x-b\zeta_4)(x+b\zeta_4)(x^2-b^2\zeta_4)(x^2+b^2\zeta_4),$$

and consequently $J_{8,a}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^6$.

Assume $-a = b^8$ and $\zeta_4 \notin K$. If $K = \mathbb{Q}$ then

$$f_a(x) = x(x-b)(x+b)(x^2+b^2)(x^4+b^4),$$

and so $J_{8,a}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$. If $K = \mathbb{F}_p$ then $p \equiv 3 \pmod 4$. Therefore $\sqrt{2} \in \mathbb{F}_p$ if $p \equiv 7 \pmod 8$ and $\sqrt{-2} \in \mathbb{F}_p$ if $p \equiv 3 \pmod 8$. Consequently, $f_a(x)$ has the factorization

$$x(x-b)(x+b)(x^2+b^2)(x^2-\sqrt{2}\,bx+b^2)(x^2+\sqrt{2}bx+b^2)$$

or

$$x(x-b)(x+b)(x^2+b^2)(x^2-\sqrt{-2}bx-b^2)(x^2+\sqrt{-2}bx-b^2),$$

and $J_{8,a}(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^5$.

Now observe that if $K = \mathbb{F}_p$ where $p \equiv 3 \pmod 4$ and $-a$ is a square then it is an 8th power in K (in fact $-a$ is a 2^kth power for any k). Indeed, let $a = -b^2$. Since $\left(\frac{-1}{p}\right) = -1$, we have $\left(\frac{b}{p}\right) = 1$ or $\left(\frac{-b}{p}\right) = 1$. Hence $a = -(\pm b)^2 = -c^4$. Similarly, $\left(\frac{c}{p}\right) = 1$ or $\left(\frac{-c}{p}\right) = 1$, and $a = -(\pm c)^4 = -d^8$ etc. Also if $K = \mathbb{F}_p$ where $p \equiv 5 \pmod 8$ and $-a$ is a 4th power then it is an 8th power in K. Indeed, let $a = -b^4$. We know that $\zeta_4 \in K$ but $\zeta_8 \notin K$, hence $\left(\frac{\zeta_4}{p}\right) = -1$. Consequently, $\left(\frac{b}{p}\right) = 1$ or $\left(\frac{b\zeta_4}{p}\right) = 1$, i.e., $b = c^2$ or $b\zeta_4 = c^2$, and so $a = -c^8$.

Assume that $-a$ is a 4th power but not an 8th power in K. Then in particular, by the above, $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ with $p \equiv 1 \pmod 8$. Assume $a = -b^4$ and $\pm b$ is not a square in K. Over the rationals, $f_a(x)$ has the factorization $x(x^2 - b)(x^2 + b)(x^4 + b^2)$ if b is not twice a square, and

$$x(x^2 - 2c^2)(x^2 + 2c^2)(x^2 - 4cx + 2c^2)(x^2 + 4cx + 2c^2)$$

if $b = 2c^2$ (so $a = -16c^8$). Therefore $J_{8,a}(\mathbb{Q})\,[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ if $a = -16c^8$, and $J_{8,a}(\mathbb{Q})\,[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$ if $a = -b^4$ and $b \neq c^2, 2c^2$. Over $\mathbb{F}_p$ we have

$$f_a(x) = x(x^2 - b)(x^2 + b)(x^2 + b\zeta_4)(x^2 - b\zeta_4),$$

hence $J_{8,a}(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ for such a and p.

Now suppose that $-a$ is a square but not a 4th power in K. Hence in particular, $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ with $p \equiv 1 \pmod 4$. Let $a = -b^2$ where $\pm b \in K$ is not a square. Then over K the polynomial $f_a(x)$ factors as $x(x^4 - b)(x^4 + b)$, and so $J_{8,a}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Note that if $a = 4b^4$ in K then $f_a(x) = x(x^4 + 2bx^2 + 2b^2)(x^4 - 2bx^2 + 2b^2)$, and consequently $(\mathbb{Z}/2\mathbb{Z})^2 \subset J_{8,a}(K)[2]$, which establishes part (1). Now let $K = \mathbb{Q}$. Then $J_{8,4b^4}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ because the above factors are irreducible over the rationals.

It remains to check the case $a \neq 4b^4$ and $a \neq -b^2$. But then $x^8 + a$ is irreducible over $\mathbb{Q}$, by [18, Lemma 4.6.9], which completes the proof. ∎

In order to calculate $\#J_{8,a}(\mathbb{F}_p)$ we apply [7]. We write down only selected cases from [7, Section 6], useful for our purposes. The values of $\#J_{8,a}(\mathbb{F}_p)$ will be displayed in the tables below, and we indicate the residuacity of $a \in \mathbb{F}_p \setminus \{0\}$.

Lemma 20.

(1) *If* $p \equiv 3 \pmod 8$ *then*

$\#J_{8,a}(\mathbb{F}_p)$	*square*
$(1 - p^2)^2$	*no*
$(1 + p^2)^2$	*yes*

(2) *If* $p \equiv 5 \pmod 8$ *then*

$\#J_{8,a}(\mathbb{F}_p)$	*square*	*4th power*
$1 + p^4$	*no*	*no*
$(1 - p)^2(1 + p)^2$	*yes*	*no*
$(1 + p^2)^2$	*yes*	*yes*

(3) *If* $p \equiv 9 \pmod{16}$ *then*

$\#J_{8,a}(\mathbb{F}_p)$	*square*	*4th power*	*8th power*
$1+p^4$	*no*	*no*	*no*
$(1+p^2)^2$	*yes*	*no*	*no*
$(1-p)^4$	*yes*	*yes*	*no*
$(1+p)^4$	*yes*	*yes*	*yes*

Proof. See [7, Section 6.3]. ∎

Now we are ready to prove our third main result.

Proof of Theorem 4. First note that $J_{8,a}(\mathbb{Q})_{\mathrm{tors}} = J_{8,a}(\mathbb{Q})[2]$ if and only if $J_{8,a}(\mathbb{Q})_{\mathrm{tors}}$ contains no element of order 4. Next, if $p \nmid 2a$ for a prime p, then $J_{8,a}(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $J_{8,a}(\mathbb{F}_p)$; in particular $\mathrm{ord}_2(\#J_{8,a}(\mathbb{Q})_{\mathrm{tors}}) \leq \mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p))$. If $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)[2])$ then $J_{8,a}(\mathbb{F}_p)$ contains no elements of order 4, and hence the same is true for $J_{8,a}(\mathbb{Q})_{\mathrm{tors}}$. Now we need to consider a few cases.

Assume that a is not of the form $\pm 1, \pm 2$ times a square in $\mathbb{Z}$. By the Chinese Remainder Theorem and the Dirichlet Prime Number Theorem, we can choose a prime p such that $p \nmid a$, $p \equiv 9 \pmod{16}$, and $\left(\frac{a}{p}\right) = -1$. Hence, by Lemma 20, we obtain $\#J_{8,a}(\mathbb{F}_p) = 1 + p^4 \equiv 2 \pmod{16}$. Therefore obviously $J_{8,a}(\mathbb{F}_p)$ has no point of order 4, and consequently $J_{8,a}(\mathbb{Q})_{\mathrm{tors}} = J_{8,a}(\mathbb{Q})[2]$ for such a.

Now assume that $a = \pm c^2$ (without loss of generality $c \in \mathbb{N}$) and c is neither a square nor twice a square. Then, as above, there exists a prime p such that $p \nmid a$, $p \equiv 9 \pmod{16}$, and $\left(\frac{c}{p}\right) = -1$. In particular, $\sqrt{-1} \in \mathbb{F}_p$, and moreover $\left(\frac{\sqrt{-1}}{p}\right) = 1$. Hence, a is a square but not a 4th power in $\mathbb{F}_p$, and by Lemma 20, we get $\#J_{8,a}(\mathbb{F}_p) = (1+p^2)^2 \equiv 4 \pmod{16}$. So $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)) = 2$. Next, writing $a = -(\sqrt{-1}\, c)^2$ or $a = -c^2$, and applying Proposition 19, we obtain $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p))[2] = 2$, and consequently $J_{8,\pm c^2}(\mathbb{Q})_{\mathrm{tors}} = J_{8,\pm c^2}(\mathbb{Q})[2]$ for such c.

Now let $a = \pm 2c^2$ ($c \in \mathbb{N}$). In this case we choose a prime p such that $p \nmid a$, $p \equiv 5 \pmod{8}$. Since $\left(\frac{a}{p}\right) = \left(\frac{\pm 2}{p}\right) = -1$, we have, by Lemma 20, $\#J_{8,a}(\mathbb{F}_p) = 1 + p^4 \equiv 2 \pmod{8}$. Hence $J_{8,\pm 2c^2}(\mathbb{F}_p)$ has no point of order 4, and consequently $J_{8,\pm 2c^2}(\mathbb{Q})_{\mathrm{tors}} = J_{8,\pm 2c^2}(\mathbb{Q})[2]$.

It remains to check the case $a = \pm b^4, \pm 4b^4$ ($b \in \mathbb{N}$). Let $a = 4b^4$. Then take a prime p such that $p \nmid a$ and $p \equiv 3 \pmod{8}$. Clearly a is a square in $\mathbb{F}_p$, hence by Lemma 20, we get $\#J_{8,a}(\mathbb{F}_p) = (1+p^2)^2 \equiv 4 \pmod{8}$, so $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)) = 2$. On the other hand, by Proposition 19, we have $(\mathbb{Z}/2\mathbb{Z})^2 \subset J_{8,a}(\mathbb{F}_p)[2]$. Therefore $J_{8,a}(\mathbb{F}_p)$ has no point of order 4, and so $J_{8,4b^4}(\mathbb{Q})_{\mathrm{tors}} = J_{8,4b^4}(\mathbb{Q})[2]$.

Let $a = -4b^4$ or $a = b^4$, and choose a prime p such that $p \nmid a$ and $p \equiv 5 \pmod 8$. Note that $\sqrt{-1} \in \mathbb{F}_p$ and $\left(\frac{\sqrt{-1}}{p}\right) = -1$. Hence $\left(\frac{2\sqrt{-1}}{p}\right) = 1$, and $a = (2b^2\sqrt{-1})^2$ or $a = b^4$, so in both cases a is a 4th power in $\mathbb{F}_p$. Consequently, by Lemma 20, we obtain $\#J_{8,a}(\mathbb{F}_p) = (1+p^2)^2 \equiv 4 \pmod 8$. Moreover, $a = -(2b^2)^2$ and $\left(\frac{2b^2}{p}\right) = -1$ or $a = -(b^2\sqrt{-1})^2$ and $\left(\frac{b^2\sqrt{-1}}{p}\right) = -1$, therefore by Proposition 19, we get $J_{8,a}(\mathbb{F}_p)\,[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, and $J_{8,a}(\mathbb{Q})_{\mathrm{tors}} = J_{8,a}(\mathbb{Q})[2]$ for $a = -4b^4, b^4$.

Now assume $a = -b^4$. Consider a prime p with $p \nmid a$ and $p \equiv 5 \pmod 8$. In the same manner we can see that a is a square but not a 4th power in $\mathbb{F}_p$. Then by Lemma 20, we have $\#J_{8,a}(\mathbb{F}_p) = (1-p)^2(1+p)^2$, and $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)) = 6$. Clearly, by Proposition 19, we also have $\mathrm{ord}_2(\#J_{8,a}(\mathbb{F}_p)[2]) = 6$. Therefore $J_{8,-b^4}(\mathbb{Q})_{\mathrm{tors}} = J_{8,-b^4}(\mathbb{Q})[2]$, which completes the proof. ∎

5. Other title curves with special n. In this section we compute the torsion part of $J_{p,a}(\mathbb{Q})$, where p is an odd prime, and of $J^{n,a}(\mathbb{Q})$, where $n = 4, 6, 8$.

5.1. The curves $y^2 = x(x^p + a)$. For odd n (say $n = 2m+1$) the curve $C_{n,a}$ is isomorphic to $C^{n,a^{n-1}}$. Indeed, the map $C_{2m+1,a} \to C^{2m+1,a^{2m}}$ given by

$$(x, y) \mapsto \left(\frac{a}{x}, \frac{a^m y}{x^{m+1}}\right),$$

has inverse $C^{2m+1,a^{2m}} \to C_{2m+1,a}$ given by

$$(x, y) \mapsto \left(\frac{a}{x}, \frac{ay}{x^{m+1}}\right).$$

In particular, the curves $y^2 = x(x^p + a)$ and $y^2 = x^p + a^{p-1}$ are isomorphic (p is an odd prime, a is a $2p$th powerfree integer). Therefore, by (1.3), we obtain the following.

PROPOSITION 21. *We have*

$$J_{p,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } a \text{ is not a } p\text{th power,} \\ \mathbb{Z}/2p\mathbb{Z} & \text{if } a \text{ is a } p\text{th power.} \end{cases}$$

5.2. The curves $y^2 = x^4 + a$. The curve $C^{4,a} : y^2 = x^4 + a$ is an elliptic curve (so we can identify $C^{4,a}$ with $J^{4,a}$) and has Weierstrass equation

$$Y^2 = X^3 - 4aX.$$

Indeed, setting $u = y + x^2$, we get $y - x^2 = a/u$, and so $2x^2 = u - a/u$. Multiplying by u^2 and setting $v = xu$, we obtain $2v^2 = u^3 - au$. Finally, on setting $X = 2u$ and $Y = 4v$, the equation takes the required Weierstrass form. Consequently, by (1.2), we have the following (note that a is 8th powerfree):

PROPOSITION 22.

$$J^{4,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } a = c^2, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } a = -c^4, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } a \neq c^2 \text{ and } a \neq -c^4. \end{cases}$$

5.3. The curves $y^2 = x^6 + a$. By Theorem 2, we know that $\#J^{6,a}(\mathbb{Q})_{\mathrm{tors}} = 2^\alpha 3^\beta$, where $0 \leq \alpha \leq 2$ and $1 \leq \beta \leq 2$. In this subsection we will give an almost full characterization of these groups. More precisely, we will prove

PROPOSITION 23. *For any nonzero a,*

$$J^{6,a}(\mathbb{Q})_{\mathrm{tors}} = J^{6,a}(\mathbb{Q})[2] \times J^{6,a}(\mathbb{Q})[9],$$

where

$$J^{6,a}(\mathbb{Q})[2] \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } a = -c^6 \text{ or } a = 27c^6, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } a = b^3 \text{ and } b \neq 3c^2 \text{ and } b \neq -c^2, \\ 0 & \text{if } a \neq b^3, \end{cases}$$

$$J^{6,a}(\mathbb{Q})[9] \cong \begin{cases} (\mathbb{Z}/3\mathbb{Z})^2 & \text{if } a = c^2 \text{ or } a = -432b^6, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } a \neq c^2 \text{ and } a \neq -3c^2 \text{ and } a \neq 2b^3, \\ \mathbb{Z}/9\mathbb{Z} \text{ or } (\mathbb{Z}/3\mathbb{Z})^2 \text{ or } \mathbb{Z}/3\mathbb{Z} & \text{if } (a = -3c^2 \text{ and } a \neq -432b^6) \text{ or} \\ & (a = 2b^3 \text{ and } a \neq -3c^2 \text{ and } a \neq c^2). \end{cases}$$

REMARK 24. Numerical computations in Magma [3] suggest that in fact $J^{6,a}(\mathbb{Q})[9] \cong \mathbb{Z}/3\mathbb{Z}$ in the last case.

Before proving Proposition 23, let us prepare some introductory results. First, by Proposition 14, we have $\#J^{6,a}(\mathbb{F}_p) = \#J^{3,a}(\mathbb{F}_p)\#J_{3,a}(\mathbb{F}_p)$ for any prime $p \nmid 6a$. Secondly, $J^{3,a}$ is simply the elliptic curve $C^{3,a} : y^2 = x^3 + a$. Similarly $J_{3,a}$ is the elliptic curve $y^2 = x(x^3 + a)$, which after the transformation $(x, y) \mapsto (a/x, ay/x^2)$ has Weierstrass form $C^{3,a^2} : y^2 = x^3 + a^2$. Therefore combining Proposition 17, Lemma 13 and evaluation of Jacobsthal sum $\psi_{3,1}$ given in [1, Thm. 4.1], we obtain

LEMMA 25. *Let $p \nmid 6a$. Then*

$$\#J^{6,a}(\mathbb{F}_p) = \begin{cases} (1+p)^2 & \text{if } p \equiv 2 \pmod 3, \\ \big(1 + p + 2u\big(\frac{a}{p}\big)\big)(1 + p + 2u) & \text{if } p \equiv 1 \pmod 3 \text{ and} \\ & a \text{ is a cube in } \mathbb{F}_p, \\ \big(1 + p - \big(\frac{a}{p}\big)(u + 3|v|\varepsilon)\big)(1 + p - (u + 3|v|\varepsilon)) & \text{if } p \equiv 1 \pmod 3 \text{ and} \\ & a \text{ is not a cube in } \mathbb{F}_p, \end{cases}$$

where $p = u^2 + 3v^2$ *with* $u \equiv 2 \pmod 3$, *and* $\varepsilon = \pm 1$. *Moreover, if* 2 *is cubic nonresidue modulo* p *then*

$$\varepsilon \equiv \begin{cases} |v| \pmod 3 & \text{if } 2a \text{ is a cube in } \mathbb{F}_p, \\ -|v| \pmod 3 & \text{if } 4a \text{ is a cube in } \mathbb{F}_p. \end{cases}$$

REMARK 26. One can show (using Lemma 25) that if $a = -3c^2$ or $a = 2b^3$ then $9 \mid \#J^{6,a}(\mathbb{F}_p)$ for any $p \nmid 6a$. Therefore in this case the "reduction method" (i.e., formula (3.4)) is useless.

Proof of Proposition 23. Since $\#J^{6,a}(\mathbb{Q})_{\mathrm{tors}} = 2^\alpha 3^\beta$ with $0 \le \alpha \le 2$ and $1 \le \beta \le 2$, we see that

$$J^{6,a}(\mathbb{Q})_{\mathrm{tors}} = J^{6,a}(\mathbb{Q})[4] \times J^{6,a}(\mathbb{Q})[9].$$

Therefore it remains to show that $J^{6,a}(\mathbb{Q})_{\mathrm{tors}}$ has no point of order 4, and to prove the above formulae for $J^{6,a}(\mathbb{Q})[m]$ for $m = 2, 9$.

We begin by proving the formula for $J^{6,a}(\mathbb{Q})[2]$. By Lemma 7, the group $J^{6,a}(\mathbb{Q})[2]$ is completely determined by factorization of the polynomial $g_a(x) := x^6 + a$ over $\mathbb{Q}$. Note that g_a has a rational root if and only if $a = -c^6$ for some integer c. In this case $g_a(x)$ factors over $\mathbb{Q}$ as

$$(x - c)(x + c)(x^2 - cx + c^2)(x^2 + cx + c^2).$$

Hence, by Lemma 7, we obtain $r = 2$. It is easy to check that g_a is irreducible over $\mathbb{Q}$ if and only if a is neither a cube nor minus a square. Then $J^{6,a}(\mathbb{Q})[2]$ is trivial. Assume now that g_a has no rational roots but is reducible over $\mathbb{Q}$. If $a = b^3$ and $b \neq 3c^2, -c^2$ then $g_a(x) = (x^2 + b)(x^4 - bx^2 + b^2)$, so by Lemma 7, we get $r = 1$. If $a = -b^2$ and $b \neq c^3$ then $g_a(x) = (x^3 - b)(x^3 + b)$, and consequently $J^{6,a}(\mathbb{Q})[2]$ is trivial. If $a = 27c^6$ then

$$g_a(x) = (x^2 + 3c^2)(x^2 - 3cx + 3c^2)(x^2 + 3cx + 3c^2),$$

and we get $r = 2$, which proves the desired formula.

Now consider $J^{6,a}(\mathbb{Q})[9]$. By Theorem 2, we have $\mathbb{Z}/3\mathbb{Z} \subset J^{6,a}(\mathbb{Q})\,[9]$, and moreover $(\mathbb{Z}/3\mathbb{Z})^2 = J^{6,a}(\mathbb{Q})\,[9]$ if $a = c^2$. Assume that $a = -432b^6 = -3(12b^3)^2$ and consider the divisor $D = (2b\sqrt{3}, 36b^3) + (-2b\sqrt{3}, 36b^3) - \infty^+ - \infty^-$. It is easy to see that D is $\mathbb{Q}$-rational divisor on $C^{6,-432b^6}$, and by Lemma 6, D is not principal. But using the algorithm from [4, Chapter 8], we see that $2D \sim -D$, and consequently $J^{6,-432b^6}(\mathbb{Q})\,[9] = (\mathbb{Z}/3\mathbb{Z})^2$. Now assume $a \neq c^2$, $a \neq -3c^2$ and $a \neq 2b^3$. Then, by the Chebotarev Density Theorem, there exist (in fact infinitely many) primes p such that $p \nmid 2a$, $p \equiv 1 \pmod 3$, $\left(\frac{a}{p}\right) = -1$, a is a cube in $\mathbb{F}_p$, and 2 is not a cube in $\mathbb{F}_p$. For such p, we have $p = u^2 + 3v^2$ with $u \equiv 2 \pmod 3$ and $3 \nmid v$ (note that 2 is a

cubic residue modulo p iff $3 \mid v$), and moreover by Lemma 25, we get

$$\begin{aligned}\#J^{6,a}(\mathbb{F}_p) &= (1+p-2u)(1+p+2u)\\ &= ((1-u)^2+3v^2)((1+u)^2+3v^2),\end{aligned}$$

so $\operatorname{ord}_3(\#J^{6,a}(\mathbb{F}_p)) = 1$. Hence by (3.4), $9 \nmid J^{6,a}(\mathbb{Q})_{\mathrm{tors}}$, and consequently $J^{6,a}(\mathbb{Q})[9] = \mathbb{Z}/3\mathbb{Z}$, which proves the desired formula.

Now we prove (much as in the proof of Theorem 4) that $J^{6,a}(\mathbb{Q})_{\mathrm{tors}}$ has no point of order 4. Let p be a prime such that $p \nmid a$ and $p \equiv 5 \pmod{12}$. Then, by Lemma 25, we obtain $\#J^{6,a}(\mathbb{F}_p) = (1+p)^2 \equiv 4 \pmod 8$, i.e., $\operatorname{ord}_2(\#J^{6,a}(\mathbb{F}_p)) = 2$. On the other hand, for such p, $-a$ is necessarily a cube in $\mathbb{F}_p$, say $a = -b^3$. If moreover $\left(\frac{b}{p}\right) = 1$ then $a = -c^6$, and $x^6 + a$ factors over $\mathbb{F}_p$ as

$$(x-c)(x+c)(x^2-cx+c^2)(x^2+cx+c^2).$$

But if $\left(\frac{b}{p}\right) = -1$ then $\left(\frac{-3b}{p}\right) = 1$, and

$$x^6 + a = (x^2-b)(x^2+\sqrt{-3b}\,x-b)(x^2-\sqrt{-3b}\,x-b).$$

Therefore, by Lemma 7, we have $J^{6,a}(\mathbb{F}_p)[2] = (\mathbb{Z}/2\mathbb{Z})^2$. Consequently, $J^{6,a}(\mathbb{F}_p)$ has no point of order 4, and we are done. ∎

5.4. The curves $y^2 = x^8 + a$. By Theorem 2, we know that $J^{8,a}(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group of order $\le 2^9 = 512$ and has an element of order 4 (so $J^{8,a}(\mathbb{Q})_{\mathrm{tors}} \neq J^{8,a}(\mathbb{Q})[2]$, in contrast to $J_{8,a}(\mathbb{Q})_{\mathrm{tors}}$). Moreover, $(\mathbb{Z}/4\mathbb{Z})^2 \subset J^{8,a}(\mathbb{Q})_{\mathrm{tors}}$ if a is a square. In this subsection we will improve those results. We will show

PROPOSITION 27. *We have*

$$J^{8,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} (\mathbb{Z}/4\mathbb{Z})^2 & \text{if } a = c^2 \text{ and } a \neq 4b^4,\\ \mathbb{Z}/4\mathbb{Z} & \text{if } a \neq \pm c^2.\end{cases}$$

Before the proof of Proposition 27, we give some preliminary results. By Proposition 14, we have $\#J^{8,a}(\mathbb{F}_p) = \#J^{4,a}(\mathbb{F}_p)\#J_{4,a}(\mathbb{F}_p)$ for any prime $p \nmid 2a$. As we can see above, $J^{4,a}$ is simply the elliptic curve $C^{4,a}$ which has Weierstrass form $C_{2,-4a} : y^2 = x^3 - 4ax$. On the other hand, $J_{4,a}$ is the Jacobian of the genus 2 hyperelliptic curve $C_{4,a} : y^2 = x(x^4 + a)$, which we considered in [11]. Therefore combining Lemma 13 and evaluation of appropriate Jacobsthal sums given in [2, Chapter 6] and [11], we get

LEMMA 28. *If $p \equiv 5 \pmod 8$ and $p \nmid a$ then*

$$\#J^{8,a}(\mathbb{F}_p) = \begin{cases} (1+p)^2(1+p+2u) & \text{if } a \text{ is a 4th power in } \mathbb{F}_p,\\ (1-p)^2(1+p-2u) & \text{if } a \text{ is a square but not a 4th power in } \mathbb{F}_p,\\ (1+p^2)(1+p\pm 2|v|) & \text{if } a \text{ is not a square in } \mathbb{F}_p,\end{cases}$$

where $p = u^2 + v^2$ and $u \equiv 3 \pmod 4$.

Proof of Proposition 27. Assume that a is neither a square nor minus a square in $\mathbb{Z}$. Then by the Dirichlet Prime Number Theorem, there exists a prime p such that $p \equiv 5 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$. For such p, by Lemma 28, we get $\operatorname{ord}_2(\#J^{8,a}(\mathbb{F}_p)) = 2$, and consequently, by (3.4) and Theorem 2, $J^{8,a}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/4\mathbb{Z}$.

Similarly, if $a = c^2$ and $a \neq 4b^4$ (so $c \neq \pm 2b^2$) then there exists a prime p such that $p \equiv 5 \pmod 8$ and $\left(\frac{c}{p}\right) = 1$. Hence, by Lemma 28, we obtain $\operatorname{ord}_2(\#J^{8,a}(\mathbb{F}_p)) = 4$, which combined with (3.4) and Theorem 2 completes the proof. ∎

6. Problems. In the light of the above results it is natural to state the following problems.

PROBLEM 29. *For which even positive integers $n \neq 2^k$, is the group $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ a 2-group for all nonzero a?*

We know only one such n, namely $J_{6,a}(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group. For those n for which $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group for all $a \neq 0$ one can ask:

PROBLEM 30. *For which positive integers n, do we have*

$$J_{n,a}(\mathbb{Q})_{\mathrm{tors}} = J_{n,a}(\mathbb{Q})[2]$$

for all nonzero a?

We only know that for $n = 4, 8$ we have $J_{n,a}(\mathbb{Q})_{\mathrm{tors}} = J_{n,a}(\mathbb{Q})\,[2]$ for all nonzero a, and for $n = 2, 6$ this is not the case: for some a (even infinitely many a for $n = 6$) there are points of order 4. Note that the analogous problems for $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ are easy. Indeed, by Theorem 2, if $n \neq 2^k$ then the statement '$J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group for all nonzero a' is false. Even for $n = 2^k \geq 4$, the statement '$J^{n,a}(\mathbb{Q})_{\mathrm{tors}} = J^{n,a}(\mathbb{Q})[2]$ for all nonzero a' is false because $J^{2^k,a}(\mathbb{Q})_{\mathrm{tors}}$ has an element of order 4 for some a.

The following problem is of interest.

PROBLEM 31. *Give a complete characterization of $J_{n,a}(\mathbb{Q})_{\mathrm{tors}}$ and $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$ for all positive integers n and all nonzero $2n$th powerfree integers a.*

In particular one can ask about a possible analogy between the formulae (1.3), (1.4) and the formula for $J^{n,a}(\mathbb{Q})_{\mathrm{tors}}$.

References

[1] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory 11 (1979), 349–498.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monogr. Adv. Texts 21, Wiley-Interscience, 1998.

[3] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.
[4] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, 1996.
[5] G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. (Basel) 77 (2001), 241–246.
[6] C. Friesen, J. B. Muskat, B. K. Spearman and K. S. Williams, *Cyclotomy of order 15 over* $GF(p^2), p \equiv 4, 11 \pmod{15}$, Int. J. Math. Math. Sci. 9 (1986), 665–704.
[7] M. Haneda, M. Kawazoe and T. Takahashi, *Formulae of the order of Jacobians for certain hyperelliptic curves*, in: Symposium on Cryptography and Information Security (Sendai, 2004), 885–890.
[8] M. Hindry and J. H. Silverman, *Diophantine Geometry*, Grad. Texts in Math. 201, Springer, 2000.
[9] T. Jędrzejak, *Characterization of the torsion of the Jacobians of two families of hyperelliptic curves*, Acta Arith. 161 (2013), 201–218.
[10] T. Jędrzejak, *On the torsion of the Jacobian of of superelliptic curves* $y^q = x^p + a$, J. Number Theory 145 (2014), 402–425.
[11] T. Jędrzejak and M. Ulas, *Characterization of the torsion of the Jacobian of* $y^2 = x^5 + Ax$ *and some applications*, Acta Arith. 144 (2010), 183–191.
[12] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.
[13] A. Menezes, Y. Wu and R. Zuccherato, *An elementary introduction to hyperelliptic curves*, appendix in: Algebraic Aspects of Cryptography by Neal Koblitz, Springer, 1998, 155–178.
[14] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comput. 68 (1999), 1233–1241.
[15] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.
[16] P. Stevenhagen and H. W. Lenstra, *Chebotarev and his Density Theorem,* Math. Intelligencer 18, (1996), no. 2, 26–37.
[17] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1996), 134–144.
[18] S. Weintraub, *Galois Theory*, Universitext, Springer, 2009.

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