ACTA ARITHMETICA
161.3 (2013)

Characterization of the torsion of the Jacobians of two families of hyperelliptic curves

by

Tomasz Jędrzejak (Szczecin)

1. Introduction. Using the classical Nagell–Lutz Theorem, Mazur's deep result, and the reduction modulo primes homomorphism, it is relatively easy to calculate the torsion of any given elliptic curve over $\mathbb{Q}$. This calculation may be slighty more complicated for infinite (one-parameter) families of such curves. Among them the families $E^a : y^2 = x^3 + ax$ and $E_b : y^2 = x^3 + b$ occupy a special place (without loss of generality we can and will assume that a and b are nonzero integers 4th and 6th power free respectively). Their respective j-invariants are 1728 and 0. Both families have complex multiplication by a fourth and third root of unity respectively. For $E = E^a$ or E_b, let $E(\mathbb{Q})_{\mathrm{tors}}$ denote the torsion subgroup of the Mordell–Weil group $E(\mathbb{Q})$. The following results are well known (see for instance [K, Theorems 5.2, 5.3, p. 134].

Proposition 1.1. *We have*

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

Proposition 1.2. *We have*

$$E_b(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } b \neq \text{square and } b \neq \text{cube and } b \neq -432, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } b = \text{cube and } b \neq 1, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } b = -432 \text{ or } (b = \text{square and } b \neq 1), \\ \mathbb{Z}/6\mathbb{Z} & \text{if } b = 1. \end{cases}$$

Note that $E^a(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group. Let $E(\mathbb{Q})[2]$ denote the kernel of the multiplication by 2 map in $E(\mathbb{Q})$. It is easy to see that $E^a(\mathbb{Q})[2] =$

2010 *Mathematics Subject Classification*: Primary 11G10, 11G30; Secondary 11G20, 11L10.

Key words and phrases: hyperelliptic curves, Jacobian varieties, Jacobsthal sums.

DOI: 10.4064/aa161-3-1

$\{\infty\} \cup \{(x,0) \in \mathbb{Q}\times\mathbb{Q} : x^3+ax=0\}$. Then by Proposition 1.1, we get

$$E^a(\mathbb{Q})_{\mathrm{tors}} = E^a(\mathbb{Q})[2] \quad \text{for } a \neq 4 \tag{1.1}$$

(note that $E^4(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$). On the other hand, for $b \neq -432 = -2^4 3^3$ we have the following alternative formulation of Proposition 1.2:

$$E_b(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } b \neq \text{square and } b \neq \text{cube},\\ \mathbb{Z}/2\mathbb{Z} & \text{if } b \neq \text{square and } b = \text{cube},\\ \mathbb{Z}/3\mathbb{Z} & \text{if } b = \text{square and } b \neq \text{cube},\\ \mathbb{Z}/6\mathbb{Z} & \text{if } b = \text{square and } b = \text{cube}. \end{cases} \tag{1.2}$$

In some sense the natural generalizations of elliptic curves with j-invariants 1728 and 0 are the hyperelliptic curves $C^{n,A} : y^2 = x^n + Ax$ and $C_{n,A} : y^2 = x^n + A$ (and their Jacobians $J^{n,A}$ and $J_{n,A}$) respectively. In [JU, Theorem 2.2] we proved that

$$J^{5,A}(\mathbb{Q})_{\mathrm{tors}} = J^{5,A}(\mathbb{Q})[2] \quad \text{for all } A \in \mathbb{Q}\backslash\{0\}. \tag{1.3}$$

This was used to give interesting applications to ranks of octic twists. Let us also mention that, in the case of twisted Fermat curves $C_m^p : x^p + y^p = m$, uniform boundedness of $\#\,\mathrm{Jac}(C_m^p)(\mathbb{Q})_{\mathrm{tors}}$ for a fixed odd prime p was used to obtain certain information about the behaviour of ranks in the infinite family $\mathrm{Jac}(C_m^p)(\mathbb{Q})$ (see [DJ]).

In this paper we show that for any nonzero rational A the torsion subgroup of $J^{7,A}(\mathbb{Q})$ is a 2-group (Theorem 3.2), and for $A \neq 4a^4, -1728, -1259712$ this subgroup is equal to $J^{7,A}(\mathbb{Q})[2]$ (Theorem 3.11). This is a variant of the corresponding results for $J^{3,A}$ ($A \neq 4$) and $J^{5,A}$ (formulas (1.1) and (1.3)). We prove that for the excluded values of A (possibly except -1728) the group $J^{7,A}(\mathbb{Q})$ has a point of order 4 and for almost all such A we completely determine its torsion subgroup (Theorem 3.12). We give an explanation of the case $A = -1728$ (Remarks 3.16). We also completely determine the $\mathbb{Q}$-rational torsion of $J_{p,A}$ for all odd primes p, and for $A \in \mathbb{Q}\backslash\{0\}$ such that $A \neq (-1)^{(p-1)/2}p$ times a square (Theorem 4.1). This is a generalization of formula (1.2). We discuss the excluded case and explain difficulties (Remarks 4.5). Note that in [JTU] we investigated the ranks of $2n$-twists of k-tuples of $J_{n,A}$ without computing the torsion subgroups.

2. Useful lemmas.

For a smooth projective curve C defined over a field K let J_C denote its Jacobian variety. Let $J_C(K)_{\mathrm{tors}}$ denote the subgroup of K-rational torsion points of $J_C(K)$ and let $J_C(K)[2]$ be the kernel of multiplication by 2 on $J_C(K)$. By definition, a divisor $D \in \mathrm{Div}(C)$ is K-rational if it is invariant under the action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. 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

K-rational does not mean that $P_1, \ldots, P_r \in C(K)$. It suffices for $\mathrm{Gal}(\overline{K}/K)$ to permute the P_i's in an appropriate fashion.

The following lemma will be used in both Sections 3 and 4.

LEMMA 2.1. *Let C be a smooth projective curve of genus $g \geq 1$ defined over the finite field $\mathbb{F}_q$. Set $N_k := \#C(\mathbb{F}_{q^k})$ for $k \in \mathbb{N}$. Then $\#J_C(\mathbb{F}_q)$ is completely determined by $N_1, \ldots, N_g$. Moreover,*

- *if $g = 2$ then*

$$\#J_C(\mathbb{F}_q) = \frac{N_1^2 + N_2}{2} - q,$$

- *if $g = 3$ then*

$$\#J_C(\mathbb{F}_q) = \frac{N_1^3}{6} + \frac{N_1 N_2}{2} + \frac{N_3}{3} - qN_1, \tag{2.1}$$

- *if $N_k = 1 + q^k$ for $k = 1, \ldots, g$ then*

$$\#J_C(\mathbb{F}_q) = 1 + q^g. \tag{2.2}$$

Proof. It is known (see for example [HS, Exercise A.8.11]) that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha_1^n + \cdots + \alpha_{2g}^n), \tag{2.3}$$

where $P(T) := \prod_{i=1}^{2g}(1 - \alpha_i T)$ is a polynomial with integer coefficients which satisfies $P(T) = q^g T^{2g} P\big(\frac{1}{qT}\big)$. Then

$$\#J(\mathbb{F}_q) = P(1) = \prod_{i=1}^{2g}(1 - \alpha_i),$$

therefore

$$\#J(\mathbb{F}_q) = (-1)^g s_g + \sum_{i=0}^{g-1}(-1)^i(1 + q^{g-i})s_i, \tag{2.4}$$

where $s_i = s_i(\alpha_1, \ldots, \alpha_{2g})$ denotes the ith fundamental symmetric polynomial (by definition $s_0 := 1$). Let $t_i = t_i(\alpha_1, \ldots, \alpha_{2g}) := \alpha_1^i + \cdots + \alpha_{2g}^i$ be the ith Newton polynomial. Since $N_k = q^k + 1 - t_k(\alpha_1, \ldots, \alpha_{2g})$, using the Newton formulas

$$ks_k = \sum_{i=1}^{k}(-1)^{i-1} t_i s_{k-i} \tag{2.5}$$

and (2.4), we are done. ∎

In the proof of our main result in Section 3 we use the following formulation of the Chebotarev Density Theorem (cf. [SL]).

LEMMA 2.2. *Let f be a polynomial with integer coefficients and leading coefficient* 1. *Assume that its discriminant Δ_f does not vanish. Let C be a conjugacy class of the Galois group G of f (i.e. $G = \mathrm{Gal}(K/\mathbb{Q})$ where K is* *the splitting field of f). Let $\sigma_p \in G$ denote the Frobenius substitution of the prime p (i.e. $\sigma_p(x) \equiv x^p \pmod{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime lying above p in $\mathcal{O}_K$). Then the set of primes p not dividing Δ_f for which σ_p belongs to C has a density, and this density equals $\#C/\#G$.*

Proof. See for example [SL, pp. 35–36]. ■

COROLLARY 2.3. *Under the above assumptions there are infinitely many primes p such that the polynomial f has the same decomposition type over $\mathbb{F}_p$ as the cycle pattern of σ_p viewed as an element of the permutation group of the zeroes of f.*

3. The curves $y^2 = x^7 + Ax$. Consider the family of curves (over $\mathbb{Q}$) $C_A := C^{7,A} : y^2 = x^7 + Ax$ where A is a nonzero rational. The curve C_A is hyperelliptic of genus 3. Without loss of generality we may assume that A is a 12th power free integer. Note that $\operatorname{disc}(x^7 + Ax) = -46656A^7 = -2^6 3^6 A^7$, hence the curve C_A has good reduction at primes $p \nmid 6A$. Let J_A be the Jacobian variety of C_A. The aim of this section is to describe the torsion subgroup of $J_A(\mathbb{Q})$. We start with some useful information about the curve C_A and its Jacobian J_A (cf. [KTW]).

The curve C_A has the automorphisms $\sigma(x,y) := (\sqrt[3]{A}/x, \sqrt[3]{A^2}\, y/x^4)$ defined over $\mathbb{Q}(\sqrt[3]{A})$ and $\rho(x,y) = (\zeta_{12}^2 x, \zeta_{12} y)$ defined over $\mathbb{Q}(\zeta_{12})$ where ζ_{12} is a primitive 12th root of unity. Clearly, ρ has order 12, σ has order 2 and $\sigma\rho = \rho^5\sigma$. These morphisms induce endomorphisms on the Jacobian J_A. Thus the endomorphism ring of J_A contains $\mathbb{Z}[\zeta_{12}]$.

The quotient of C_A by the group generated by σ is the elliptic curve $E_{A,1}$ with equation

$$E_{A,1} : y^2 = x^3 - 3\sqrt[3]{A}\, x, \tag{3.1}$$

and an explicit quotient map is given by

$$(x,y) \mapsto \left(x + \frac{\sqrt[3]{A}}{x}, \frac{y}{x^2}\right). \tag{3.2}$$

A regular differential on C_A invariant under σ is $(x^2 - \sqrt[3]{A})dx/y$.

The quotient of C_A by the group $\langle \rho^4 \rangle$ is the elliptic curve $E_{A,2}$ with equation

$$E_{A,2} : y^2 = x^3 + Ax, \tag{3.3}$$

and an explicit quotient map is given by

$$(x,y) \mapsto (x^3, xy). \tag{3.4}$$

A regular differential on C_A invariant under ρ^4 is $x\,dx/y$.

Since the elliptic curves $E_{A,1}$, $E_{A,2}$ correspond to linearly independent differentials on C_A, one concludes that the Jacobian J_A is isogenous (over $\overline{\mathbb{Q}}$)

to a product of three elliptic curves $E_{A,1}$, $E_{A,2}$, $E_{A,3}$. Moreover,

$$E_{A,3} = (1-\sigma)(1-\rho^4)(1-\rho^8)J_A. \tag{3.5}$$

This is because $(1-\sigma)(1-\rho^4)(1-\rho^8)$ acts as multiplication by 6 on the differential $(x^2+\sqrt[3]{A})dx/y$ and sends the two differentials $(x^2-\sqrt[3]{A})dx/y$ and xdx/y to 0.

Now we give a full characterization of the group $J_A(\mathbb{Q})[2]$.

Lemma 3.1. *We have*

$$J_A(\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \textit{if } A \neq \textit{cube and } A \neq -\textit{square} \text{ (case 1)},\\ (\mathbb{Z}/2\mathbb{Z})^2 & \textit{if } (A = \textit{cube and } A \neq -\textit{square} \\ & \quad \textit{and } A \neq 27 \times \textit{sixth power}) \\ & \quad \textit{or } (A = -\textit{square and } A \neq \textit{cube}) \text{ (case 2)},\\ (\mathbb{Z}/2\mathbb{Z})^3 & \textit{if } A = 27 \times \textit{sixth power} \text{ (case 3)},\\ (\mathbb{Z}/2\mathbb{Z})^4 & \textit{if } A = -\textit{sixth power} \text{ (case 4)}. \end{cases}$$

In particular, if A is as in case 1 *then*

$$J_A(\mathbb{Q})[2] = \langle [(0,0)-\infty] \rangle. \tag{3.6}$$

Let a denote a square free positive integer. If $A = a^3$ $(a \neq 3)$ then

$$J_A(\mathbb{Q})[2] = \langle [(0,0)-\infty], [(\sqrt{-a},0)+(-\sqrt{-a},0)-2\infty] \rangle; \tag{3.7}$$

if $A = -a^2$ then

$$J_A(\mathbb{Q})[2] = \left\langle [(0,0)-\infty], \left[(\sqrt[3]{a},0) + \left(\frac{-1+i\sqrt{3}}{2}\sqrt[3]{a},0 \right) + \left(\frac{-1-i\sqrt{3}}{2}\sqrt[3]{a},0 \right) - 3\infty \right] \right\rangle; \tag{3.8}$$

if $A = 27a^6$ then

$$J_A(\mathbb{Q})[2] = \left\langle [(0,0)-\infty], [(ia\sqrt{3},0)+(-ia\sqrt{3},0)-2\infty], \left[\left(\frac{3a+ia\sqrt{3}}{2} \right) + \left(\frac{3a-ia\sqrt{3}}{2} \right) - 2\infty \right] \right\rangle; \tag{3.9}$$

and if $A = -a^6$ then

$$J_A(\mathbb{Q})[2] = \left\langle [(0,0)-\infty], [(a,0)-\infty], [(-a,0)-\infty], \left[\left(\frac{a-ia\sqrt{3}}{2},0 \right) + \left(\frac{a+ia\sqrt{3}}{2},0 \right) - 2\infty \right] \right\rangle. \tag{3.10}$$

Here $[D]$ denotes the equivalence class of the divisor D in J_A.

Proof. Note that $(0,0)\in C_A(\mathbb{Q})$, hence $[(0,0)-\infty]\in J_A(\mathbb{Q})[2]$. It is well known that every point in $J_A(\overline{\mathbb{Q}})[2]$ can be uniquely written as $D=\sum n_iP_i-(\sum n_i)\infty$, where $P_i=(x_i,0)\in C_A(\overline{\mathbb{Q}})$ are pairwise distinct, $n_i\in\{0,1\}$ and $\sum n_i\le 3$. Therefore the group $J_A(\mathbb{Q})[2]$ is completely determined by factorization of the polynomial $f(x):=x^6+A$ over $\mathbb{Q}$.

Note that f has a rational root if and only if $A=-a^6$. In this case $f(x)$ factors over $\mathbb{Q}$ as $(x-a)(x+a)(x^2-ax+a^2)(x^2+ax+a^2)$. Hence we obtain (3.10). It is easy to check that f is irreducible over $\mathbb{Q}$ if and only if A is as in case 1. Then $J_A(\mathbb{Q})[2]=\{\mathcal{O},[(0,0)-\infty]\}$.

If f has no rational roots but is reducible over $\mathbb{Q}$ then A is as in case 2 or 3. In particular, if $A=a^3$ $(a\neq 3)$ then $f(x)=(x^2+a)(x^4-ax^2+a^2)$, hence we get (3.7). If $A=-a^2$ then $f(x)=(x^3-a)(x^3+a)$ and we get (3.8). If $A=27a^6$ then $f(x)=(x^2+3a^2)(x^2-3ax+3a^2)(x^2+3ax+3a^2)$, and we are done. ■

Now we attempt to describe $J_A(\mathbb{Q})_{\mathrm{tors}}$.

THEOREM 3.2. *For all $A\in\mathbb{Q}\setminus\{0\}$ the group $J_A(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group of order ≤ 64. Moreover, if A is not a cube then $\#J_A(\mathbb{Q})_{\mathrm{tors}}\le 4$.*

The proof of Theorem 3.2 splits into a few lemmas. In order to compute $\#J_A(\mathbb{Q})_{\mathrm{tors}}$ it is helpful to consider $J_A(\mathbb{F}_p)$ for several primes $p\nmid 6A$. This is because reduction modulo p induces an embedding $J_A(\mathbb{Q})_{\mathrm{tors}}\hookrightarrow J_A(\mathbb{F}_p)$ (cf. [HS, Theorem C.1.4, p. 263]) and therefore

$$\#J_A(\mathbb{Q})_{\mathrm{tors}}\mid \#J_A(\mathbb{F}_p). \tag{3.11}$$

By Lemma 2.1, we have

$$\begin{aligned}\#J_A(\mathbb{F}_p)=\frac{\#C_A(\mathbb{F}_p)^3}{6}&+\frac{\#C_A(\mathbb{F}_p)\#C_A(\mathbb{F}_{p^2})}{2}\\&+\frac{\#C_A(\mathbb{F}_{p^3})}{3}-p\#C_A(\mathbb{F}_p),\end{aligned}\tag{3.12}$$

so it is enough to compute $\#C_A(\mathbb{F}_{p^k})$ for $k=1,2,3$.

LEMMA 3.3. *If $p\equiv 3 \pmod 4$ then $\#C_A(\mathbb{F}_{p^l})=1+p^l$ for all odd positive integers l.*

Proof. Let l be an odd positive integer. The curve C_A has the point $(0,0)$ and the point at infinity. Since $p\equiv 3\pmod 4$, -1 is not a square in $\mathbb{F}_{p^l}$. Moreover $(-x)^7+A(-x)=-(x^7+Ax)$, hence each pair $\{x,-x\}$ with $x\in\mathbb{F}_{p^l}^\times$ gives two distinct points of $C_A(\mathbb{F}_{p^l})$, namely either $(\pm x,0)$, or $(x,\pm\sqrt{x^7+Ax})$, or $(-x,\pm\sqrt{-x^7-Ax})$. This establishes the formula. ■

In order to compute $\#C_A(\mathbb{F}_{p^2})$ as well as $\#C_A(\mathbb{F}_p)$, $\#C_A(\mathbb{F}_{p^3})$ for $p \equiv 1 \pmod 4$, we will use Jacobsthal sums. Let $q = p^k$, $e \in \mathbb{N}$ and $a \in \mathbb{F}_q$. The Jacobsthal sum $\phi_e(a)$ of order e is defined by

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

where $\left(\frac{\cdot}{q}\right)$ is the quadratic character of $\mathbb{F}_q$. For $a \in \mathbb{Z}$ we define $\phi_e(a) := \phi_e\,(a \bmod p)$. We list their basic properties (see [KR1]):

Lemma 3.4.

(i) *If* $\gcd(e, q-1) = e_1$ *then* $\phi_e(a) = \phi_{e_1}(a)$.
(ii) *If* $e \mid (q-1)$ *but* $2e \nmid (q-1)$ *then* $\phi_e(a) = 0$.
(iii) $\phi_e(ab^e) = \left(\frac{b}{q}\right)^{e+1}\phi_e(a)$ *for* $b \in \mathbb{F}_q^\times$.
(iv) $\#C_A(\mathbb{F}_q) = 1 + q + \phi_6(A)$.

It will be helpful to consider ϕ_6 and ϕ_2 too. The next lemma is due to Katre and Rajwade [KR2, Theorem 2].

Lemma 3.5. *Let* $p \equiv 1 \pmod 4$, $q = p^n$ *and* $a \in \mathbb{F}_q \setminus \{0\}$. *Let* $p = u_0^2 + v_0^2$ *where* $u_0 \equiv 1 \pmod 4$ *and in case* a *is not a square in* $\mathbb{F}_q$, v_0 *is uniquely given by* $a^{(q-1)/4} \equiv u_0/v_0 \pmod p$. *Then*

$$\phi_2(a) = \begin{cases} -2u & \textit{if } a \textit{ is a 4th power in } \mathbb{F}_q, \\ 2u & \textit{if } a \textit{ is a square but not a 4th power in } \mathbb{F}_q, \\ 2v & \textit{if } a \textit{ is not a square in } \mathbb{F}_q, \end{cases}$$

where

$$u = u_0^n - \binom{n}{2} u_0^{n-2} v_0^2 + \binom{n}{4} u_0^{n-4} v_0^4 - \cdots,$$
$$v = v_0\left(\binom{n}{1} u_0^{n-1} - \binom{n}{3} u_0^{n-3} v_0^3 + \cdots\right).$$

The following two lemmas are due to Berndt and Evans [BE, p. 423].

Lemma 3.6. *Let* $q = p^2$, $p \equiv 3 \pmod 4$ *and* $a \in \mathbb{F}_{p^2} \setminus \{0\}$. *Then*

$$\phi_6(a) = \begin{cases} 6p & \textit{if } a \textit{ is a 12th power in } \mathbb{F}_q, \\ -6p & \textit{if } a \textit{ is a 6th power but not a 12th power in } \mathbb{F}_q, \\ 0 & \textit{otherwise.} \end{cases}$$

In the next lemma the values of $\phi_6(a)$ will be displayed in a table. Columns will indicate the residuacity of $a \in \mathbb{F}_{p^2} \setminus \{0\}$.

Lemma 3.7. *Let $p = 12k + 5$. Write $p = u_0^2 + v_0^2$, where u is odd. Then*

$\phi_6(a)$	*square*	*cube*	*4th power*
$-2(p-2u_0^2)$	*yes*	*yes*	*yes*
$2(p-2u_0^2)$	*yes*	*yes*	*no*
$4(p-2u_0^2)$	*yes*	*no*	*yes*
$-4(p-2u_0^2)$	*yes*	*no*	*no*
$\pm 12\lvert u_0v_0\rvert$	*no*	*yes*	*no*
0	*no*	*no*	*no*

The above lemmas do not allow us to calculate $\#J_A(\mathbb{F}_p)$ for $p \equiv 1 \pmod{12}$. In these cases we will apply Lemma 3.8 below (due to Haneda, Kawazoe and Takahashi [HKT]). We write down only selected cases from [HKT, Theorems 5.1, 5.2] useful for our purposes. The values of $\#J_A(\mathbb{F}_p)$ will be displayed in tables; columns will indicate the residuacity of $A \in \mathbb{F}_p \setminus \{0\}$.

Lemma 3.8. *Let $p \equiv 1 \pmod{12}$ and write $p = u^2 + v^2$, where $u \equiv 1 \pmod 4$. Then if $3 \mid u$, we have*

$\#J_A(\mathbb{F}_p)$	*square*	*cube*	*4th power*
$(1-2u+p)(1+2u+p)^2$	*yes*	*yes*	*yes*
$(1-2u+p)(1-2u+4u^2-p-2pu+p^2)$	*yes*	*no*	*yes*
$(1+2u+p)(1+2u+4u^2-p+2pu+p^2)$	*yes*	*no*	*no*
$(1+2u+p)(1-2u+p)^2$	*yes*	*yes*	*no*

and if $3 \mid v$, we have

$\#J_A(\mathbb{F}_p)$	*square*	*cube*	*4th power*
$(1-2u+p)^3$	*yes*	*yes*	*yes*
$(1-2u+p)(1+2u+4u^2-p+2pu+p^2)$	*yes*	*no*	*yes*
$(1+2u+p)(1-2u+4u^2-p-2pu+p^2)$	*yes*	*no*	*no*
$(1+2u+p)^3$	*yes*	*yes*	*no*

The following elementary lemma is useful when computing the residuacity of $a \in \mathbb{F}_{p^n}$ $(n = 1, 2, 3)$.

Lemma 3.9. *Let $p > 3$ be a prime. Then:*

(i) *-1 is a 4th power in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 8$,*

(ii) *if $\left(\frac{a}{p}\right) = 1$ then a is a 4th power in $\mathbb{F}_{p^2}$,*

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

(iv) *if a is a square and a cube in $\mathbb{F}_p$ then a is a 12th power in $\mathbb{F}_{p^2}$,*

(v) *if $p \equiv 3 \pmod 4$ then every integer is a 4th power in $\mathbb{F}_{p^2}$,*

(vi) *a is a cube in $\mathbb{F}_p$ if and only if a is a cube in $\mathbb{F}_{p^2}$,*

(vii) *a is a square in $\mathbb{F}_p$ if and only if a is a square in $\mathbb{F}_{p^3}$,*

(viii) *a is a 4th power in $\mathbb{F}_p$ if and only if a is a 4th power in $\mathbb{F}_{p^3}$,*

(ix) *if $p \equiv 2 \pmod 3$ then every integer is a cube in $\mathbb{F}_p$ (hence in $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ too),*

(x) *if $p \equiv 1 \pmod{12}$ then -3 is a 4th power in $\mathbb{F}_p$ if and only if $3 \mid v$ where $p = u^2 + v^2$ with odd u.*

Proof. The proof of (i)–(ix) is straightforward. The assertion (x) follows from [L, pp. 158–159]. ∎

Proof of Theorem 3.2. We will show that $\#J_A(\mathbb{Q})_{\text{tors}}$ is a power of 2. Indeed, let r be an odd prime. By the Chinese Remainder Theorem and the Dirichlet Prime Number Theorem, we can choose a prime p such that $p > 6|A|$, $p \equiv 3 \pmod 8$, $p \equiv 1 \pmod r$. Then, by Lemma 3.3, we have $\#C_A(\mathbb{F}_p) = 1 + p$, $\#C_A(\mathbb{F}_{p^3}) = 1 + p^3$.

If A is a cube in $\mathbb{F}_p$ then by Lemma 3.9, we deduce that A is a 12th power in $\mathbb{F}_{p^2}$. Therefore by Lemma 3.6, we have $\#C_A(\mathbb{F}_{p^2}) = 1 + p^2 + 6p$, so by (3.12) we get $\#J_A(\mathbb{F}_p) = (1 + p)^3$, and by (3.11), $\#J_A(\mathbb{Q})_{\text{tors}} \mid (1 + p)^3$. Hence $r \nmid \#J_A(\mathbb{Q})_{\text{tors}}$ and $\operatorname{ord}_2(\#J_A(\mathbb{Q})_{\text{tors}}) \le 6$.

If A is not a cube in $\mathbb{F}_p$ then by Lemmas 3.6 and 3.9, we obtain $\#C_A(\mathbb{F}_{p^2}) = 1+p^2$. Hence $\#J_A(\mathbb{F}_p) = 1+p^3$, and so $r \nmid \#J_A(\mathbb{Q})_{\text{tors}}$ and $\operatorname{ord}_2(\#J_A(\mathbb{Q})_{\text{tors}}) \le 2 < 6$.

If A is not a cube in $\mathbb{Z}$, then by the Chebotarev Density Theorem, there exists a prime p such that $p > 6|A|$, $p \equiv 3 \pmod 8$ and A is not a cube in $\mathbb{F}_p$. By the above, $\#J_A(\mathbb{Q})_{\text{tors}} \le 4$, and the assertion follows. ∎

The following lemma will be helpful in proving Theorem 3.11, our second main result of this section.

Lemma 3.10. *Let $p \nmid 6A$. Then*

(i) *if $p \equiv 3 \pmod 8$ and A is a cube in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 6$,

(ii) *if $p \equiv 3 \pmod 8$ and A is not a cube in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 2$,

(iii) *if $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$ and A is not a square in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 6$,

(iv) *if $p \equiv 1 \pmod 8$, $p \equiv 2 \pmod 3$ and A is a square but not a 4th power in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 4$,

(v) *if $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$ and A is a 4th power in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 4$,

(vi) *if $p \equiv 5 \pmod 8$, $p \equiv 1 \pmod 3$, -3 is a 4th power and A is a 12th power in $\mathbb{F}_p$ then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 6$,

(vii) *if $p \equiv 1 \pmod 3$ and ($p \equiv 5 \pmod 8$ and A is a 4th power but not a cube in $\mathbb{F}_p$ or $p \equiv 1 \pmod 8$ and A is a square but neither a 4th power nor a cube in $\mathbb{F}_p$) then* $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) = 2$,

(viii) $\#J_A(\mathbb{F}_p)[2] = 64$ *if and only if $p \equiv 1 \pmod 3$ and $-A$ is a 6th power in $\mathbb{F}_p$,*

(ix) $\#J_A(\mathbb{F}_p)[2] = 16$ *if and only if* $p \equiv 2 \pmod 3$ *and* $-A$ *is a square in* $\mathbb{F}_p$*,*

(x) $\#J_A(\mathbb{F}_p)[2] = 8$ *if and only if* $-A$ *is not a square but is a cube in* $\mathbb{F}_p$*,*

(xi) $\#J_A(\mathbb{F}_p)[2] = 4$ *if and only if* $-A$ *is not a cube but is a square in* $\mathbb{F}_p$*,*

(xii) $\#J_A(\mathbb{F}_p)[2] = 2$ *if and only if* $-A$ *is neither a square nor a cube in* $\mathbb{F}_p$*.*

Proof. Parts (i) and (ii) follow from the proof of Theorem 3.2.

(iii) For such p, by Lemma 3.9, A is a square and a cube (but not a 4th power) in $\mathbb{F}_{p^2}$, and A is not a square in $\mathbb{F}_p$ or $\mathbb{F}_{p^3}$. Since $\gcd(6, p-1) = 2$ we have $\phi_6 = \phi_2$ in $\mathbb{F}_p$ and $\mathbb{F}_{p^3}$ (note that the same is true for (iv) and (v)). Moreover, $A^{(p^3-1)/4} \equiv -A^{(p-1)/4} \pmod p$. Hence, by Lemmas 3.5 and 3.7, we get $\#C_A(\mathbb{F}_p) = 1+p-2v_0^2$, $\#C_A(\mathbb{F}_{p^2}) = 1+p^2+2p-4u_0^2$ and $\#C_A(\mathbb{F}_{p^3}) = 1+p^3+6u_0^2v_0-2v_0^3$ where $p = u_0^2+v_0^2$, $u_0 \equiv 1 \pmod 4$ and $v_0 \equiv 2 \pmod 4$. By (3.12) we obtain $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 6$.

(iv) By Lemma 3.9, A is also a square but not a 4th power in $\mathbb{F}_{p^3}$ and is a 12th power in $\mathbb{F}_{p^2}$. Hence, by Lemmas 3.5 and 3.7, we obtain $\#C_A(\mathbb{F}_p) = 1+p+2u_0$, $\#C_A(\mathbb{F}_{p^2}) = 1+p^2-2p+4u_0^2$ and $\#C_A(\mathbb{F}_{p^3}) = 1+p^3+2u_0^3-6u_0v_0^2$ where $p = u_0^2+v_0^2$, $u_0 \equiv 1 \pmod 4$, $v_0 \equiv 0 \pmod 4$. Therefore by (3.12) we get $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 4$.

(v) This follows by the same method as in (iii) and (iv).

(vi)–(vii) These follow directly from Lemmas 3.8 and 3.9.

(viii)–(xi) We argue similarly to the proof of Lemma 3.1. Note that $\#J_A(\mathbb{F}_p)[2] = 64$ if and only if $x^7 + Ax$ has seven roots in $\mathbb{F}_p$. The polynomial $x^7 + Ax$ splits into linear factors in $\mathbb{F}_p$ if and only if $A = -6$th power in $\mathbb{F}_p$ and a primitive 6th root of unity belongs to $\mathbb{F}_p$. The latter condition is equivalent to $p \equiv 1 \pmod 3$. ∎

Now we are ready to give a full characterization of $J_A(\mathbb{Q})_{\mathrm{tors}}$ for almost all A's. Remember that, without loss of generality, we assume that A is a 12th power free integer.

THEOREM 3.11. *If* $A \notin 4\mathbb{N}^4 \cup \{-1728, -1259712\}$ *then* $J_A(\mathbb{Q})_{\mathrm{tors}} = J_A(\mathbb{Q})[2]$.

Proof. First of all note that by Theorem 3.2, we have $J_A(\mathbb{Q})_{\mathrm{tors}} = J_A(\mathbb{Q})[2]$ if and only if $J_A(\mathbb{Q})_{\mathrm{tors}}$ contains no element of order 4. Next, observe that if a prime $p \nmid 6A$ then $J_A(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $J_A(\mathbb{F}_p)$, in particular $\mathrm{ord}_2(\#J_A(\mathbb{Q})_{\mathrm{tors}}) \le \mathrm{ord}_2(\#J_A(\mathbb{F}_p))$. Note that if $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_A(\mathbb{F}_p)[2])$ then $J_A(\mathbb{F}_p)$ contains no elements of order 4 and hence the same is true for $J_A(\mathbb{Q})_{\mathrm{tors}}$. Now we need to consider a few (not necessarily disjoint) cases.

Assume that A is neither a cube nor $1, -2, -3, 6$ times a square (in $\mathbb{Z}$). By the Chebotarev Density Theorem (see Lemma 2.2 and Corollary 2.3), there exists a prime p such that $p > 6|A|$, $p \equiv 3 \pmod 8$, A is not a cube modulo p and $-A$ is a square in $\mathbb{F}_p$ (in fact the set of such primes has positive analytic density).

Indeed, consider the polynomial $h(x) := (x^2+1)(x^2-2)(x^2+A)(x^3-A)$ and its splitting field K (over $\mathbb{Q}$). Then $K = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{A}, \sqrt[3]{A})$ and $K/\mathbb{Q}$ is a Galois extension of degree ≤ 48. There exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(i) = -i$, $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$, $\sigma(\sqrt{A}) = -\sqrt{A}$ and $\sigma(\sqrt[3]{A}) = \omega\sqrt[3]{A}$ where $\omega^3 = 1$, $\omega \ne 1$. If we arrange the zeroes of h in the following order: $i, -i, \sqrt{2}, -\sqrt{2}, \sqrt{-A}, -\sqrt{-A}, \sqrt[3]{A}, \omega\sqrt[3]{A}, \omega^2\sqrt[3]{A}$ then σ, viewed as an element of the symmetric group on nine letters, is the product $(1,2)(3,4)(5)(6)(7,8,9)$ of disjoint cycles, i.e. has cycle pattern $2,2,1,1,3$. By Corollary 2.3, there exist infinitely many primes p such that h has decomposition type $2,2,1,1,3$ over $\mathbb{F}_p$, i.e. the polynomials x^2+1, x^2-2 and x^3-A are irreducible over $\mathbb{F}_p$ but x^2+A splits over $\mathbb{F}_p$. Therefore such primes p have the desired properties. By Lemma 3.10(ii) & (xi), for such p we get $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 2$ and $\#J_A(\mathbb{F}_p)[2] = 4$. Hence $J_A(\mathbb{Q})_{\mathrm{tors}} = J_A(\mathbb{Q})[2]$ for such A.

Now let A be a square, say $A = a^2$ (without loss of generality $a > 0$). If a is neither a square nor twice a square then we can find a prime p such that $p > 6|A|$, $p \equiv 1 \pmod 8$, $p \equiv 2 \pmod 3$ and $\left(\frac{a}{p}\right) = -1$. Then by Lemma 3.10(iv) & (ix), $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 4$ and $\#J_A(\mathbb{F}_p)[2] = 16$. Therefore $J_{a^2}(\mathbb{Q})_{\mathrm{tors}} = J_{a^2}(\mathbb{Q})[2]$. If a is a square (so A is a 4th power) then we choose a prime $p > 6|A|$ such that $p \equiv 5 \pmod 8$ and $p \equiv 2 \pmod 3$. Hence again by Lemma 3.10(v) & (ix), we conclude that $J_{c^4}(\mathbb{Q})_{\mathrm{tors}} = J_{c^4}(\mathbb{Q})[2]$. Note that the case $a = 2c^2$ is excluded.

Let $A = -2a^2$ ($a > 0$). Again by the Chebotarev Density Theorem (we omit the details because the explanation is similar to that above), there exists a prime $p > 6|A|$ such that $p \equiv 1 \pmod 8$, $p \equiv 2 \pmod 3$ and A is a square but not a 4th power in $\mathbb{F}_p$ (note that $\left(\frac{A}{p}\right) = \left(\frac{-2}{p}\right) = 1$, hence by Lemma 3.9 the last condition is equivalent to $\left(\frac{\sqrt{2}\,a}{p}\right) = -1$ where $\sqrt{2}$ denotes any square root of 2 in $\mathbb{F}_p$). Then by Lemma 3.10(iv) & (ix), we get $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 4$ and $\#J_A(\mathbb{F}_p)[2] = 16$. Hence $J_A(\mathbb{Q})_{\mathrm{tors}} = J_A(\mathbb{Q})[2]$ for such A.

Let $A = 6a^2$ ($a > 0$). Once again by the Chebotarev Density Theorem, there exists a prime $p > 6|A|$ such that $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$ and A is a 4th power in $\mathbb{F}_p$ (as previously, the last condition is equivalent to $\left(\frac{\sqrt{6}a}{p}\right) = 1$ where $\sqrt{6}$ denotes any square root of 6 in $\mathbb{F}_p$). Hence by Lemma 3.10(v) & (ix), we obtain $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_A(\mathbb{F}_p)[2]) = 4$.

Now let $A = -3a^2$ ($a > 0$). Assume that a is not three times a cube in $\mathbb{Z}$ (then A is not a cube). For a prime $p \equiv 1 \pmod{12}$ write $p = u^2 + v^2$ where

$u \equiv 1 \pmod 4$. By the Chebotarev Density Theorem, there exists a prime $p > 6|A|$ such that $p \equiv 1 \pmod 3$, A is not a cube in $\mathbb{F}_p$, $p \equiv 1 \pmod 8$ and A is not a 4th power in $\mathbb{F}_p$, and similarly there exists a prime $p > 6|A|$ such that $p \equiv 1 \pmod 3$, A is not a cube in $\mathbb{F}_p$, $p \equiv 5 \pmod 8$ and A is a 4th power in $\mathbb{F}_p$. Note that A is a 4th power in $\mathbb{F}_p$ if and only if $\bigl(\frac{\sqrt{-3}\,a}{p}\bigr) = 1$, and by Lemma 3.9(x), the last condition is equivalent to $\bigl(\frac{a}{p}\bigr) = 1$ and $3 \mid v$, or $\bigl(\frac{a}{p}\bigr) = -1$ and $3 \mid u$. Hence (in both cases) by Lemma 3.10(vii) & (xi), we get $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_A(\mathbb{F}_p)[2]) = 2$.

Assume now that $a = 3c^3$ where $c \neq 2, 6$ (without loss of generality c is positive and square free) so $A = -27c^6$, $A \neq -1728, -1259712$. Once again, by the Chebotarev Density Theorem, there exists a prime $p > 6|A|$ such that $p \equiv 5 \pmod 8$, $p \equiv 1 \pmod 3$, and -3 and A are both 4th powers in $\mathbb{F}_p$ (the last two conditions are equivalent to $3 \mid v$ and $\bigl(\frac{c}{p}\bigr) = 1$). Therefore by Lemma 3.10(vi) & (viii), we obtain

$$\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = \mathrm{ord}_2(\#J_A(\mathbb{F}_p)[2]) = 6.$$

Now assume that A is a cube, say $A = b^3$ (by the above we may assume that b is not $1, -2, -3, 6$ times a square in $\mathbb{Z}$). Then we can find a prime $p > 6|A|$ such that $p \equiv 3 \pmod 8$, $p \equiv 1 \pmod 3$ and $\bigl(\frac{b}{p}\bigr) = -1$. Hence $-A$ is a 6th power in $\mathbb{F}_p$, and by Lemma 3.10(i) & (viii), we obtain $\mathrm{ord}_2(\#J_A(\mathbb{F}_p)) = 6$ and $\#J_A(\mathbb{F}_p)[2] = 64$, so $J_{b^3}(\mathbb{Q})_{\mathrm{tors}} = J_{b^3}(\mathbb{Q})[2]$ and we are done. ∎

THEOREM 3.12. *For $A = 4a^4$ and -1259712 the group $J_A(\mathbb{Q})_{\mathrm{tors}}$ has an element of order* 4. *Moreover,*

(i) *if $a \neq 2$ then*

$$\begin{aligned} J_{4a^4}(\mathbb{Q})_{\mathrm{tors}} &= \langle [(\sqrt[3]{2a^2}, 2a^2\sqrt[3]{4a}) + (\omega\sqrt[3]{2a^2}, 2a^2\omega^2\sqrt[3]{4a}) \\ &\qquad + (\omega^2\sqrt[3]{2a^2}, 2a^2\omega\sqrt[3]{4a}) - 3\infty]\rangle \\ &\cong \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

(*ω is a primitive* 3*rd root of unity*),

(ii) *we have*

$$\begin{aligned} J_{-1259712}(\mathbb{Q})_{\mathrm{tors}} &\supset \langle [(0,0) - \infty]\rangle \times \langle [(9 - 3\sqrt{21}, 29160 - 5832\sqrt{21}) \\ &\qquad + (9 + 3\sqrt{21}, 29160 + 5832\sqrt{21}) - 2\infty]\rangle \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Proof. Assume that $A = 4a^4$. By (3.4) we have a map (over $\mathbb{Q}$) from C_A to the elliptic curve $E_{A,2} : y^2 = x^3 + 4a^4x$. The curve $E_{A,2}$ is isomorphic over $\mathbb{Q}$ to $E_{4,2} : y^2 = x^3 + 4x$. The elliptic curve $E_{4,2}$ has a point of order 4, namely $P = (2, 4)$. Taking the preimage of P we get three points $P_1 = (\sqrt[3]{2a^2}, 2a^2\sqrt[3]{4a})$, $P_2 = (\omega\sqrt[3]{2a^2}, 2a^2\omega^2\sqrt[3]{4a})$ and $P_3 = (\omega^2\sqrt[3]{2a^2}, 2a^2\omega\sqrt[3]{4a})$

on $C_A(\mathbb{Q}(\omega, \sqrt[3]{2a^2}))$. Then the divisor $D = P_1 + P_2 + P_3 - 3\infty$ is $\mathbb{Q}$-rational. Using Cantor's algorithm (see for instance [MWZ, Theorem 51]) we easily check that $2D \sim (0,0) - \infty$, hence $[D]$ has order 4 in $J_A(\mathbb{Q})$. Next, by Theorem 3.2, we have $\#J_{4a^4}(\mathbb{Q})_{\mathrm{tors}} \le 4$ for $a \ne 2$ (note that a is positive and cube free), and (i) is proved.

Now assume that $A = -1259712 = -2^6 3^9$. In this case we have the map (3.2), defined over $\mathbb{Q}$, from C_A to the elliptic curve $E_{A,1} : y^2 = x^3 + 324x$ (which is isomorphic to $y^2 = x^3 + 4x$). Just as above, taking the preimage of $(2, 4)$ we obtain a $\mathbb{Q}$-rational divisor

$$D' = (9 - 3\sqrt{21}, 29160 - 5832\sqrt{21}) + (9 + 3\sqrt{21}, 29160 + 5832\sqrt{21})$$

on C_A and we check that

$$2D' \sim (0,0) + (6\sqrt{3}, 0) + (-6\sqrt{3}, 0) - 3\infty.$$

Therefore $[D']$ has order 4 in $J_A(\mathbb{Q})$. Using Lemma 3.1, we obtain the assertion. ■

The case $A = -1728 = -2^6 3^3$ is more delicate. We are unable to give a complete answer in this case (see explanations in Remarks 3.16(iii)). But we present some information below.

PROPOSITION 3.13. *The Jacobian J_{-1728} is isogenous over $\mathbb{Q}$ to the product of three elliptic curves $y^2 = x^3 + 36x$, $y^2 = x^3 - 108x$, $y^2 = x^3 + 4x$. In particular* $J_{-1728}(\mathbb{Q})$ has rank 0.

Proof. Observe that for $A = -1728$ the maps (3.2), (3.4) and the elliptic curves $E_{A,1}$, $E_{A,2}$ (3.1), (3.3) are defined over $\mathbb{Q}$. In fact, $E_{-1728,1} : y^2 = x^3 + 36x$ and $E_{-1728,2} : y^2 = x^3 - 1728x \cong y^2 = x^3 - 108x$. Note that, as an endomorphism of J_{-1728}, the map $(1-\sigma)(1-\rho^4)(1-\rho^8)$ is Galois-invariant, therefore indeed its image is an abelian variety of dimension 1 defined over $\mathbb{Q}$. Hence the elliptic curve $E_{-1728,3} = (1-\sigma)(1-\rho^4)(1-\rho^8)J_{-1728}$ is defined over $\mathbb{Q}$ too, and J_{-1728} is isogenous over $\mathbb{Q}$ to $E_{-1728,1} \times E_{-1728,2} \times E_{-1728,3}$.

Now we give an explicit equation for $E_{-1728,3}$ with accuracy up to 2-isogeny (cf. [KTW]). First observe that ρ^3 commutes with ρ and σ, hence it defines an automorphism of order 4 on $E_{-1728,3}$. It follows that $E_{-1728,3}$ (as well as $E_{-1728,1}$ and $E_{-1728,2}$) has complex muliplication by $\mathbb{Z}[i]$. Next, since J_{-1728} has good reduction at all primes >3, the same holds for $E_{-1728,3}$. Therefore an equation for $E_{-1728,3}$ is of the form $y^2 = x^3 + dx$ where $d = \pm 2^s 3^t$ with $0 \le s, t \le 3$. Since the curve with d is 2-isogenous to the one with $-4d$, we may assume that $d > 0$. The exact value of d is then found using the equality

$$\#C_A(\mathbb{F}_p) = \#E_{A,1}(\mathbb{F}_p) + \#E_{A,2}(\mathbb{F}_p) + \#E_{A,3}(\mathbb{F}_p) - 2(p+1),$$

which holds for all primes p of good reduction. Evaluating this for $p = 5$ shows $d \in \{4, 9, 24, 54\}$. The case $p = 13$ shows that $d \notin \{9, 24, 54\}$. So one concludes $E_{-1728,3} : y^2 = x^3 + 4x$. Using Magma [BCP] we find that the Mordell–Weil groups $E_{-1728,k}(\mathbb{Q})$ have rank 0 ($k = 1, 2, 3$), and hence $J_{-1728}(\mathbb{Q})$ has rank 0 too. The proof is complete. ∎

Corollary 3.14. *The point at infinity and* $(0, 0)$ *are the only* $\mathbb{Q}$*-rational points on the curve* C_{-1728}.

Proof. Assume that $P = (a, b) \in C_{-1728}(\mathbb{Q})$. By Proposition 3.13, the divisor $D = P - \infty$ is torsion in $J_{-1728}(\mathbb{Q})$. Due to Grant's analogue of the Lutz–Nagell Theorem [G, Theorem 3, p. 968], it follows that $a, b \in \mathbb{Z}$, and either $b = 0$ or $b^2 \mid \operatorname{disc}(x^7 - 1728x) = 2^{48}3^{27}$. Checking all possible values of a and b using Magma [BCP], we complete the proof. ∎

Proposition 3.15. *For all primes* $p > 3$ *the group* $J_{-1728}(\mathbb{F}_p)$ *has a point of order* 4.

Proof. Let $A = -1728 = -2^6 3^3$ and let $p > 3$ be a prime. By Lemma 3.10(viii)–(xii), we obtain

$$\operatorname{ord}_2(\#J_A(\mathbb{F}_p)[2]) = \begin{cases} 6 & \text{if } p \equiv 1 \pmod{12}, \\ 4 & \text{if } p \equiv 11 \pmod{12}, \\ 3 & \text{if } p \equiv 5, 7 \pmod{12}. \end{cases}$$

On the other hand, by Lemmas 3.5–3.8 (the details are left to the reader), we get

$$\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) \ge \begin{cases} 7 & \text{if } p \equiv 1 \pmod{12}, \\ 6 & \text{if } p \equiv 5, 7, 11 \pmod{12}. \end{cases}$$

Hence in all cases $\operatorname{ord}_2(\#J_A(\mathbb{F}_p)) > \operatorname{ord}_2(\#J_A(\mathbb{F}_p)[2])$, which completes the proof. ∎

Remarks 3.16. (i) As in the proof of Proposition 3.13, we can show that for $A = -1259712$ the Jacobian J_A is isogenous over $\mathbb{Q}$ to $E_{A,1} \times E_{A,2} \times E_{-A,3}$ where

$$E_{A,1} : y^2 = x^3 + 4x, \quad E_{A,2} : y^2 = x^3 - 12x \quad \text{and} \quad E_{A,3} : y^2 = x^3 + 36x.$$

Moreover, $E_{A,1}$ and $E_{A,3}$ have rank 0 over $\mathbb{Q}$ but $E_{A,2}$ has rank 1 and the point $(-2, -4)$ generates $E_{A,2}(\mathbb{Q})$ modulo torsion. Hence $J_A(\mathbb{Q})$ has rank 1 and taking an appropriate preimage we find the divisor

$$(-6\sqrt[3]{3}, 3888/\sqrt[3]{3}) + (-6\omega\sqrt[3]{3}, 3888\omega^2/\sqrt[3]{3}) + (-6\omega^2\sqrt[3]{3}, 3888\omega/\sqrt[3]{3}) - 3\infty$$

of infinite order in $J_A(\mathbb{Q})$.

(ii) Note that the curves C_{-1728} and $C_{-1259712}$ are isomorphic over $\mathbb{Q}(\sqrt{3})$. In fact, the group $J_{-1728}(\mathbb{Q}(\sqrt{3}))$ contains an element of order 4. Namely,

$$D = (3 + \sqrt{21}, 72(5\sqrt{3} + 3\sqrt{7})) + (3 - \sqrt{21}, 72(5\sqrt{3} - 3\sqrt{7})) - 2\infty$$

is the divisor on C_{-1728} defined over $\mathbb{Q}(\sqrt{3})$ and $2D \sim (0,0) + (2\sqrt{3},0) + (-2\sqrt{3},0) - 3\infty$.

(iii) The group $J_{-1728}(\mathbb{Q})$ has an element of order 4 if and only if there exists $D \in J_{-1728}(\mathbb{Q})$ such that $2D \sim D_i$ where $D_i \in J_{-1728}(\mathbb{Q})[2] \setminus \{\mathcal{O}\}$, i.e. ($i = 1,2,3$) $D_1 = (0,0) - \infty$, $D_2 = (\sqrt{12},0) + (-\sqrt{12},0) - 2\infty$ and $D_3 = (0,0) + (\sqrt{12},0) + (-\sqrt{12},0) - 3\infty$. Reduction over $\mathbb{F}_5$ and the embedding $J_{-1728}(\mathbb{Q}) \hookrightarrow J_{-1728}(\mathbb{F}_5)$ show that D_1, $D_2 \notin 2J_{-1728}(\mathbb{Q})$, so it only remains to check D_3.

Any divisor on the curve is equivalent to the unique reduced divisor (see [MWZ, Theorem 47]), hence it is enough to consider three cases: $D = P_1 - \infty$, $D = P_1 + P_2 - 2\infty$ and $D = P_1 + P_2 + P_3 - 3\infty$. Let $P_j = (x_j, y_j)$ for $j = 1,2,3$ and let $\langle A(x), B(x)\rangle$ denote the Mumford representation of the divisor $2D$ (see [MWZ, pp. 17–19] for details). It is easy to see that the Mumford representation of the divisor D_3 is $\langle x^3 - 12x, 0\rangle$.

In the first case $2D$ is still reduced, so clearly it is not equivalent to D_3.

In the second case, first note that $P_1 \neq P_2$. Indeed, otherwise $P_1 \in C_{-1728}(\mathbb{Q})$, and by Corollary 3.14, $P_1 = (0,0)$, so $D = 2(0,0) - 2\infty \sim \mathcal{O}$. Using Cantor's algorithm [MWZ, Theorem 51] we have computed $A(x) = x^3 + a_2x^2 + a_1x + a_0$ and $B(x) = b_2x^2 + b_1x + b_0$ where $a_i, b_j \in \mathbb{Q}(x_1, x_2, y_1, y_2)$. The divisor $2D$ is $\mathbb{Q}$-rational if and only if $\mathbb{Q}(x_1, x_2, y_1, y_2)$ is a quadratic extension of $\mathbb{Q}$ and $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$ where σ denotes the generator of the Galois group of this extension. Moreover, $2D \sim D_3$ if and only if they have the same Mumford representations (as reduced divisors). Unfortunately, the system of equations $a_2 = 0$, $a_1 = -12$, ... is too complicated, and our computers are unable to solve it.

The last case is even worse. Note that all P_i are pairwise distinct (otherwise, $P_1, P_2, P_3 \in C_{-1728}(\mathbb{Q})$, and $2D \sim \mathcal{O}$). The numerators of appropriate functions $a_i, b_j \in \mathbb{Q}(x_1, x_2, x_3, y_1, y_2, y_3)$ have more terms and greater degrees than the ones in the second case.

4. The curves $y^2 = x^p + A$.

Consider the family of curves (over $\mathbb{Q}$) $C_{p,A} : y^2 = x^p + A$, where p is an odd prime and A is a nonzero rational. The curve $C_{p,A}$ is hyperelliptic of genus $(p-1)/2$. Without loss of generality we may assume that A is a $2p$-power free integer. Note that $\operatorname{disc}(x^p + A) = (-1)^{(p-1)/2}p^pA^{p-1}$, hence the curve $C_{p,A}$ has good reduction at a prime q if $q \nmid 2pA$. Let $J_{p,A}$ be the Jacobian variety of $C_{p,A}$. Note that the curve $C_{p,A}$ has the automorphism $(x,y) \mapsto (\zeta_p x, y)$ where ζ_p is a primitive pth root of unity. Hence the Jacobian $J_{p,A}$ has complex multiplication by ζ_p. In contrast to Section 3, no reduction to the elliptic curve case is possible for $C_{p,A}$. Set $p^* := (-1)^{(p-1)/2}p$.

The aim of this section is to prove the following:

THEOREM 4.1. *We have*

$$J_{p,A}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } A \neq \text{square and } A \neq p^* \times \text{square} \\ & \quad \text{and } A \neq p\text{th power}, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } A \neq \text{square and } A \neq p^* \times \text{square} \\ & \quad \text{and } A = p\text{th power}, \\ \mathbb{Z}/p\mathbb{Z} & \text{if } A = \text{square and } A \neq p\text{th power}, \\ \mathbb{Z}/2p\mathbb{Z} & \text{if } A = \text{square and } A = p\text{th power}, \\ \{0\} \text{ or } \mathbb{Z}/p\mathbb{Z} & \text{if } A = p^* \times \text{square and } A \neq p\text{th power}, \\ \mathbb{Z}/2\mathbb{Z} \text{ or } \mathbb{Z}/2p\mathbb{Z} & \text{if } A = p^* \times \text{square and } A = p\text{th power}. \end{cases}$$

Moreover, we know the following torsion points: $[(-\sqrt[p]{A}, 0) - \infty]$ *of order* 2, $[(0, \sqrt{A}) - \infty]$ *of order* p *and* $[(0, \sqrt{A}) + (-\sqrt[p]{A}, 0) - 2\infty]$ *of order* $2p$.

The proof of Theorem 4.1 breaks into three lemmas.

LEMMA 4.2. *We have* $\#J_{p,A}(\mathbb{Q})_{\mathrm{tors}} \in \{1, 2, p, 2p\}$.

Proof. We will show that $J_{p,A}(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/2p\mathbb{Z}$. Observe first that

$$\#C_{p,A}(\mathbb{F}_{l^n}) = l^n + 1 \quad \text{if } p \nmid l^n - 1. \tag{4.1}$$

Indeed, the map $x \mapsto x^p$ is an automorphism of $\mathbb{F}_{l^n}^{\times}$, hence $x \mapsto x^p + A$ is one-to-one on $\mathbb{F}_{l^n}$. If l is the primitive root modulo p then (4.1) holds for $n = 1, \ldots, (p-1)/2$. Hence, by Lemma 2.1, we obtain $\#J_{p,A}(\mathbb{F}_l) = l^{(p-1)/2} + 1$. For a prime $l \nmid 2pA$ reduction modulo l induces an embedding $J_{p,A}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow J_{p,A}(\mathbb{F}_l)$ (cf. [HS, Theorem C.1.4, p. 263]), therefore

$$\#J_{p,A}(\mathbb{Q})_{\mathrm{tors}} \mid \#J_{p,A}(\mathbb{F}_l). \tag{4.2}$$

Take a prime $q \nmid 2p$. We will show that $J_{p,A}(\mathbb{Q})$ has no q-torsion. Choose a prime $l \nmid 2pA$ such that l is a primitive root modulo p and $l \equiv 1 \pmod{q}$. Then $l^{(p-1)/2} + 1 \equiv 2 \pmod{q}$, hence $q \nmid \#J_{p,A}(\mathbb{F}_l)$. Now we can deduce bounds for 2- and p-torsion. Taking a prime $l \nmid 2pA$ such that l is a primitive root modulo p and $l \equiv 1 \pmod 4$ we have $4 \nmid \#J_{p,A}(\mathbb{F}_l)$. Similarly, taking a prime $l \nmid 2pA$ such that l is a primitive root modulo p and $p^2 \nmid l^{(p-1)/2} + 1$ we obtain $p^2 \nmid \#J_{p,A}(\mathbb{F}_l)$, and the assertion follows. ■

LEMMA 4.3. $J_{p,A}(\mathbb{Q})$ *has a point of order* 2 *if and only if* A *is a pth power.*

Proof. Suppose that $A = B^p$ with $B \in \mathbb{Z}$. Then the divisor $D = (-B, 0) - \infty$ is rational and represents a point of order two in $J_{p,A}(\mathbb{Q})$. Conversely, it is well known that every point in $J_{p,A}(\overline{\mathbb{Q}})[2]$ can be uniquely written as $D = \sum n_i P_i - (\sum n_i)\infty$, where $P_i = (x_i, 0)$ are pairwise distinct, $n_i \in \{0, 1\}$ and $\sum n_i \leq (p-1)/2$. Since the polynomial $x^p + A$ is either irreducible over $\mathbb{Q}$ or has a rational root, therefore $J_{p,A}(\mathbb{Q})[2] \neq \{\mathcal{O}\}$ implies that A is a pth power. ∎

LEMMA 4.4. *If A is a square then $J_{p,A}(\mathbb{Q})$ has a point of order p. Assume futhermore that $A \notin p^*\mathbb{N}^2$. Then the converse statement is true.*

Proof. If $A = B^2$ then the rational divisor $D = (0, B) - \infty$ is not principal but $pD = \operatorname{div}(B - y)$.

Now suppose that A is not a square. First, we show that there are infinitely many odd primes q such that $q \equiv 1 \pmod p$ and $\left(\frac{A}{q}\right) = -1$. If $A = \pm 2pa^2$ or $A = \pm 2a^2$ then we can take q such that $q \equiv 1 \pmod p$ and $q \equiv 5 \pmod 8$. If $A = -a^2$ or $A = -p^*a^2$ then we choose $q \equiv 1 \pmod p$, $q \equiv 3 \pmod 4$. In all other cases there exists an odd prime $l \neq p$ such that $\operatorname{ord}_l(A)$ is odd. By the Chinese Remainder Theorem and the Dirichlet Prime Number Theorem, there are infinitely many primes q such that q is congruent to 1 modulo 8, modulo p and modulo all primes dividing A except l and $q \equiv r \pmod l$, where $\left(\frac{r}{l}\right) = -1$. Such a q has the desired property.

Next, we consider the group homomorphism $h : \mathbb{F}_{q^n}^\times \to \mathbb{F}_{q^n}^\times$, $h(x) = x^p$. Observe that $\#\ker h = p$. Moreover, A is a square in $\mathbb{F}_{q^n}$ if and only if n is even. Hence

$$\#C_{p,A}(\mathbb{F}_{q^n}) \equiv \begin{cases} 1 \pmod p & \text{if } n \text{ is odd,} \\ 3 \pmod p & \text{if } n \text{ is even.} \end{cases}$$

Using Lemma 2.1 we find that $\#J_{p,A}(\mathbb{F}_q) \equiv 1 \pmod p$. By (4.2) we conclude that $J_{p,A}(\mathbb{Q})$ has no point of order p. ∎

REMARKS 4.5. (i) The excluded case C_{p,p^*a^2} is more difficult. For $p = 3$ these curves are elliptic and $E_{-3a^2} = C_{3,-3a^2} = J_{3,-3a^2}$. By Proposition 1.2, we have $E_{-3a^2}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/3\mathbb{Z}$ if and only if $a = 2^2 3$; in the remaining cases $E_{-3a^2}(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}\}$ except for $E_{-27}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. For $p = 5$ we have $J_{5,5a^2}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z}$ only when $a = 2^4 5^2$. For other values of a we have $J_{5,5a^2}(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}\}$ except for $J_{5,5^5}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, one can show that $p \mid \#J_{p,\pm pa^2}(\mathbb{F}_q)$ for any prime $q \nmid 2pA$. Hence the group $J_{p,\pm pa^2}(\mathbb{F}_q)$ always contains a point of order p.

(ii) The cases $p = 3$ and $p = 5$ suggest that $J_{p,(-1)^{(p-1)/2}2^{2(p-1)}p^p}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/p\mathbb{Z}$, but on the other hand $J_{7,-2^{12}7^7}(\mathbb{Q})_{\mathrm{tors}}$ is trivial. Indeed, one can easily check that $J_{7,-2^{12}7^7}(\mathbb{F}_{11})[7]$ has order 7, so the same is true for $J_{7,-2^{12}7^7}(\mathbb{Q}_{11})[7]$. Since -7 is a square mod 11, this group is generated by the class of the divisor $(0, 2^6 7^3\sqrt{-7}) - \infty$. But this divisor is not defined over $\mathbb{Q}$.

(iii) In general (for $p > 5$), if there is a p-torsion point in $J_{p,p^*a^2}(\mathbb{Q})$ then $J_{p,p^*a^2}(\mathbb{Q}(\sqrt{p^*}))[p] = (\mathbb{Z}/p\mathbb{Z})^2$, since the curve C_{p,p^*a^2} is isomorphic to C_{p,a'^2} (over $\mathbb{Q}(\sqrt{p^*})$), which also contributes p-torsion. If there is an odd prime q such that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = 1$, $q \nmid a$, $q \not\equiv 1 \pmod p$ and $p^2 \nmid \#J_{p,p^*a^2}(\mathbb{F}_q)$ then we get a contradiction.

Acknowledgements. I would like to thank the referee for carefully reading my manuscript and for giving constructive comments and suggestions which helped improve the quality of the paper. I also wish to express my thanks to Prof. Andrzej Dąbrowski for his active interest in this paper.

References

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

[BCP] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235—265.

[DJ] A. Dąbrowski and T. Jędrzejak, *Ranks in families of Jacobian varieties of twisted Fermat curves*, Canad. Math. Bull. 53 (2010), 58–63.

[G] D. Grant, *On an analogue of the Lutz–Nagell Theorem for hyperelliptic curves*, J. Number Theory 133 (2013), 963–969.

[HKT] M. Haneda, M. Kawazoe and T. Takahashi, *Formulae of the order of Jacobians for certain hyperelliptic curves*, SCIS (2004), 885–890.

[HS] M. Hindry and J. H. Silverman, *Diophantine Geometry*, Grad. Texts in Math. 201, Springer, 2000.

[JTU] T. Jędrzejak, J. Top and M. Ulas, *Tuples of hyperelliptic curves* $y^2 = x^n + a$, Acta Arith. 150 (2011), 105–113.

[JU] 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.

[KR1] S. A. Katre and A. R. Rajwade, *Jacobsthal sums of prime order*, Indian J. Pure Appl. Math. 17 (1986), 1345–1362.

[KR2] S. A. Katre and A. R. Rajwade, *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum*, Math. Scand. 60 (1987), 52–62.

[K] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

[KTW] T. Kodama, J. Top and T. Washio, *Maximal hyperelliptic curves of genus three*, Finite Fields Appl. 15 (2009) 392–403.

[L] F. Lemmermeyer, *Reciprocity Laws: from Euler to Eisenstein*, Springer Monogr. Math., Springer, Berlin 2000.

[MWZ] 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.

[SL] P. Stevenhagen and H. W. Lenstra, *Chebotarev and his Density Theorem*, Math. Intelligencer 18 (1996), no. 2, 26–37.

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

Received on 20.3.2012
and in revised form on 30.9.2013 (7009)