TORSION POINTS ON CURVES OF THE FORM $y^n = x^d + 1$

VISHAL ARUL

Abstract. In this paper we study torsion points on curves of the form $y^n = x^d + 1$. When $n$ and $d$ are coprime and neither is a power of 2, we show that the only torsion points on this curve are: (i) those whose $x$-coordinate is zero, (ii) those whose $y$-coordinate is zero, (iii) the point at infinity.

1. Introduction

Fix coprime integers $n, d \geq 1$, and assume neither is a power of 2. Let $C$ be the smooth projective model of the curve given by the equation

$$y^n = x^d + 1$$

in $\mathbb{A}^2_C$. Then $C$ has a unique point at infinity, denoted by $\infty$. The genus of $C$ is

$$g = \frac{1}{2}(n - 1)(d - 1).$$

Let $J$ be the Jacobian of $C$. Then $C$ naturally embeds into $J$ via the map $P \mapsto P - \infty$; that is, the point $P$ of $C$ goes to the divisor $P - \infty$.

A point $P$ of $C$ is called a torsion point if there exists an integer $k \geq 1$ such that

$$kP \sim k\infty.$$

We seek to classify the torsion points on $C$.

Let $\zeta_n, \zeta_{2d} \in K$ be primitive $n$th and $2d$th roots of unity, respectively. For odd $0 \leq i \leq 2d - 1$ and any $0 \leq j \leq n - 1$, we have

$$\text{div}(x - \zeta_{2d}^i) = n(\zeta_{2d}^i, 0) - n\infty$$

$$\text{div}(y - \zeta_n^j) = d(0, \zeta_n^j) - d\infty,$$

from which it follows that the points $(\zeta_{2d}^i, 0)$ and $(0, \zeta_n^j)$ are all torsion points of $C$. Of course, there is also the point $\infty$ of $C$, which also counts as a torsion point. We seek to show that these are the only torsion points on $C$. Indeed, this will be our main result as Corollary 4.15. We restate it here as Theorem 1.1.

Theorem 1.1. Suppose $n, d$ are coprime integers, neither of which is a power of 2. The only torsion points on the curve $y^n = x^d + 1$ are those whose $x$-coordinate or $y$-coordinate is zero, and also the point at $\infty$.

First we reduce to the case when $n, d$ are both primes. If $p, q$ are primes satisfying $p|n$ and $q|d$ and $C'$ is the projective normalization of the curve cut out by $y^p = x^q + 1$ in the affine plane, then there is a dominant map $C \to C'$ acting on points as $(x, y) \mapsto (x^{n/p}, x^{d/q})$ which must send torsion points to torsion points (as it also induces a map on their Jacobians).

This research was supported in part by Simons Foundation grant #550033.
So if we can show that the torsion points on $C'$ are precisely either (i) those whose $x$- or $y$-coordinates is zero or (ii) $\infty$, it follows that the same must be true for $C$.

So instead we now consider the curve $C$ which is the projective normalization of the affine plane $K$-curve $y^p = x^q + 1$, for distinct odd primes $p,q \geq 3$.

Similar results are proven for the Fermat curve $F_m$ given by the equation $X^n + Y^n + Z^n = 0$ in \cite{Col86}. A cusp is a point of $F_m(K)$ such that one of its coordinates is zero. In this paper, Coleman shows that whenever $P$ and $Q$ are points of $F_m(K)$ such that $P - Q$ is torsion and $P$ is a cusp, then $Q$ is also necessarily a cusp. Since our curve $y^m = x^q + 1$ is a quotient of the Fermat curve $F_{nd}$, we obtain a slightly stronger version of this result when $m$ is of the form $nd$.

In \cite{Jęd14} and \cite{Jęd16}, Jędrzejak considers a slightly more general variant given by $y^a = x^b + a$. Jędrzejak studies the rational torsion of the Jacobian. Letting the Jacobian of this curve be $J_{q,p,a}$, Jędrzejak shows that the group $J_{q,p,a}(Q)_{\text{tors}} \simeq (\mathbb{Z}/2\mathbb{Z})^{e_2} \times (\mathbb{Z}/p\mathbb{Z})^{e_p} \times (\mathbb{Z}/q\mathbb{Z})^{e_q}$ where $e_2, e_p, e_q \in \{0, 1\}$. Jędrzejak also shows that when $a$ is odd, that $e_2 = 0$. It follows easily that $J_{q,p,1}(Q)_{\text{tors}} \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$, generated by the points $(-1, 0)$ and $(0, 1)$. Moreover in the case $a = 1$ we work out explicitly the torsion fields $Q(J_{q,p,1}[p], \mu_{pq})$ and $Q(J_{q,p,1}[q], \mu_{pq})$ in Theorem 3.6 The key ingredient is an understanding of the $p$-adic and $q$-adic valuation of certain Jacobi sums; this analysis is performed in \cite{Aru19}.

2. THE STRUCTURE OF $T_{\ell}J$ AS A $Z$-REPRESENTATION

Let $J$ be the Jacobian of $C$. For any prime $\ell$, let $T_{\ell}J$ be the $\ell$-adic Tate module of $J$.

Now define $Z$ to be the subgroup of $\text{Aut}(C)$ generated by the automorphism sending $(x, y) \mapsto (\zeta x, \zeta y)$. Note that $Z$ is naturally isomorphic to $\mu_{pq}$. We will seek to understand $T_{\ell}J$ as a representation of $Z$.

For every positive integer $m$, define $H_{\infty,m}$ to be the following Galois group.

$$H_{\infty,m} := \text{Gal}(Q(\mu_{pq}, J[m^\infty])/Q(\mu_{pq})).$$

**Proposition 2.1.** Suppose $K_\ell$ is any extension of $Q_\ell$ containing a primitive $pq$-th root of unity. Let $O_\ell = O_{K_\ell}$. Let $J_\ell$ be the group of characters (group homomorphisms) $\chi: Z \to O_\ell^\times$ and $T_\chi \subseteq T_{\ell}J \otimes_{\mathbb{Z}_\ell} O_\ell$ be the eigenspace corresponding to $\chi$.

1. We have that

$$T_{\chi} \simeq \begin{cases} O_\ell & \text{if } \chi \text{ is injective}, \\ 0 & \text{otherwise}. \end{cases}$$

2. We have a decomposition

$$T_{\ell}J \otimes_{\mathbb{Z}_\ell} O_\ell \simeq \bigoplus_{\chi \in J_\ell} T_{\chi},$$

that respects the $H_{\infty,\ell}$ action; in particular, we get characters for $H_{\infty,\ell}$ indexed by $J_\ell$. For injective $\chi$, define

$$\xi_\chi: H_{\infty,\ell} \to \text{Aut}T_{\chi} \simeq O_\ell^\times$$

to be the action of $H_{\infty,\ell}$ on $T_{\chi}$.

3. The Weil pairing extends to a nondegenerate symplectic pairing on $T_{\ell}J \otimes_{\mathbb{Z}_\ell} O_\ell$ taking values in $T_{\ell}J \otimes_{\mathbb{Z}_\ell} O_\ell \simeq \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} O_\ell$. Furthermore, for the Weil pairing we have $\langle T_{\chi}, T_{\psi} \rangle = 0$ whenever $\psi \neq \chi^{-1}$. 

2
Proof.

(1) (a) (Case 1: $\chi$ is not injective)

Either $\chi^p = 1$ or $\chi^q = 1$. The two cases are similar so we handle the former. Then $Z^p$ must act trivially on $T \chi \subseteq T_\ell J \otimes_{\mathcal{O}_\ell} \mathcal{O}_\ell$, so in fact we must have the containment

$$T \chi \subseteq (T_\ell J \otimes_{\mathcal{O}_\ell} \mathcal{O}_\ell)^{Z^p} = (T_\ell J)^{Z^p} \otimes_{\mathcal{O}_\ell} \mathcal{O}_\ell.$$ 

Now note that under the quotient map $C \to C/Z^p$ we get an induced map $J \to \text{Jac}(C/Z^p)$ which induces $T_\ell J \to (T_\ell \text{Jac}(C/Z^p))$ and allows us to identify $T_\ell \text{Jac}(C/Z^p)$ with $(T_\ell J)^{Z^p}$. However $C/Z^p$ is isomorphic to $\mathbb{P}^1$, so

$$(T_\ell J)^{Z^p} \simeq T_\ell \text{Jac}(C/Z^p) \simeq T_\ell \mathbb{P}^1 = 0.$$  

(b) (Case 2: $\chi$ is injective)

Note that $\text{Gal}(\mathbb{Q}(\mu_{pq})/\mathbb{Q})$ acts on $\mu_{pq}$, which is naturally isomorphic to $Z$. Then this Galois group must also act on the group of characters $J_\ell$, and it acts on the injective characters transitively. Therefore $\dim T \chi$ is independent on $\chi$ for the injective $\chi$.

Then as

$$\dim_{\mathcal{O}_\ell} T_\ell J \otimes_{\mathcal{O}_\ell} \mathcal{O}_\ell = \dim_{\mathcal{O}_\ell} T_\ell J = 2g = (p - 1)(q - 1) = \# \{\text{injective characters } \chi \}.$$  

this shows that $\dim T \chi = 1$ for injective $\chi$.

(2) The previous argument shows that this decomposition exists. It respects the $H_{\infty, \ell}$ action since the actions of $H_{\infty, \ell}$ and $Z$ on $\mathcal{C}$ both commute with each other.

(3) The Weil pairing on $T_\ell J$ is $Z$-invariant (since $Z$ consists of automorphisms of the curve). It follows then that the dual of $\langle T\chi, T\psi \rangle = 0$ whenever $\chi \psi \neq 1$.

□

Definition 2.2. Since $H_{\infty, \ell}$ acts on $\mu_{l^\infty}$, it induces a map $H_{\infty, \ell} \to \text{Aut}(\mu_{l^\infty}) = Z_\ell^\times$. Let $\lambda$ be the map

$$\lambda: H_{\infty, \ell} \to Z_\ell^\times \hookrightarrow \mathcal{O}_\ell^\times.$$  

Since the Weil pairing is nondegenerate, we know that $\mathbb{Q}(J[l^\infty])$ contains $\mathbb{Q}(\mu_{l^\infty})$. Therefore,

Lemma 2.3. The image of $\lambda$ is the following.

$$\lambda(H_{\infty, \ell}) = \begin{cases} Z_\ell^\times & \text{for } \ell \notin \{p, q\} \\ \ker(Z_\ell^\times \to \mathbb{F}_\ell^\times) & \text{for } \ell \in \{p, q\}. \end{cases}$$  

Lemma 2.4. For every $\chi \in J_\ell$ we have

$$\xi_\chi \xi_{\chi^{-1}} = \lambda.$$  

Proof. From Galois-equivariance of the Weil pairing we have that if $v \in T\chi$, $w \in T\chi^{-1}$, and $h \in H_{\infty, \ell}$ then

$$h(\langle v, w \rangle) = \langle h(v), h(w) \rangle = \langle \xi_\chi(h)v, \xi_{\chi^{-1}}(h)w \rangle = (\xi_\chi \xi_{\chi^{-1}})(h)\langle v, w \rangle.$$  

If $\langle v, w \rangle$ is chosen to be a primitive element of $\mu_{l^\infty}$, the above shows that $\lambda(h) = \xi_\chi \xi_{\chi^{-1}}(h)$. □
Remark 2.5. By Proposition 2.1 (2), we have an embedding
\[ H_{\infty, \ell} \hookrightarrow \prod_{\chi: \mathbb{Z} \to \mathcal{O}_\ell^\times} \text{Aut } T_{\chi} \simeq (\mathcal{O}_\ell^\times)^{2g}. \]
In particular, \( H_{\infty, \ell} \) is abelian. Taking the direct sum over all \( \ell \), we see that the torsion field \( \mathbb{Q}(\mu_{pq}, J_{\text{tors}}) \) is abelian over \( \mathbb{Q}(\mu_{pq}) \).

In particular, the group \( \text{Gal}(\mathbb{Q}(\mu_{pq})/\mathbb{Q}) \) acts on \( H_{\infty, m} \) via conjugation in a well-defined way. This inspires the following definition

Definition 2.6. Let \( \sigma \in \text{Gal}(\mathbb{Q}(\mu_{pq})/\mathbb{Q}) \) be complex conjugation. For \( h \in H_{\infty, m} \), define \( \overline{h} = \sigma h \sigma^{-1} \in H_{\infty, m} \). (That is, lift \( \sigma \) arbitrarily to \( \bar{\sigma} \) and then define \( \overline{h} = \overline{\sigma h \bar{\sigma}^{-1}} \); this is well-defined since \( H_{\infty, m} \) is abelian.)

Lemma 2.7. Let \( h \in H_{\infty, \ell} \) and \( \chi \in \mathcal{J}_{\ell} \). The image of \( \overline{h} \) under \( \xi_{\chi} \) is
\[ \xi_{\chi}(\overline{h}) = \xi_{\chi^{-1}}(h). \]
Proof. Pick \( v \in T_{\chi} \), lift \( \sigma \in \text{Gal}(\mathbb{Q}(\mu_{pq})/\mathbb{Q}) \) arbitrarily to \( \bar{\sigma} \in \text{Gal}(\mathbb{Q}(\mu_{pq}, J[\ell^\infty])/\mathbb{Q}) \) and consider the action of \( \bar{\sigma} \) on \( T_{\chi} \). Let \( \sigma \) and \( \bar{\sigma} \) act on \( \mathcal{O}_{\ell} \) via conjugation in a well-defined way. Since \( \bar{\sigma} \) is linear and \( \bar{\sigma} v \in T_{\chi^{-1}} \), we see that
\[ \bar{\sigma} v = \bar{\sigma} h \bar{\sigma}^{-1} v = \bar{\sigma} (\xi_{\chi^{-1}}(h) \bar{\sigma}^{-1} v) = \xi_{\chi^{-1}}(h) \bar{\sigma} \bar{\sigma}^{-1} v = \xi_{\chi^{-1}}(h) v. \]
From this we conclude that \( \xi_{\chi}(\overline{h}) = \xi_{\chi^{-1}}(h) \).

Proposition 2.8. Let \( h \in H_{\infty, \ell} \). The element \( h \overline{h} \in H_{\infty, \ell} \) acts by \( \lambda(h) \) on all of \( T_{\ell} J \otimes \mathbb{Z}_{\ell} \mathcal{O}_{\ell} \).
Proof. Combining Lemmas 2.4 and 2.7 gives that \( \xi_{\chi}(h \overline{h}) = \xi_{\chi}(h) \xi_{\chi}(\overline{h}) = \xi_{\chi}(h) \xi_{\chi^{-1}}(h) = \lambda(h) \).
Hence \( h \overline{h} \) acts by multiplication by \( \lambda(h) \) on every \( T_{\chi} \), and hence on \( T_{\ell} J \otimes \mathbb{Z}_{\ell} \mathcal{O}_{\ell} \).

Lemma 2.9. Suppose \( \ell \notin \{ p, q \} \). Then the field \( \mathbb{Q}(J[\ell]) \) contains \( \mathbb{Q}(\mu_{pq}) \).
Proof. Define the homomorphism \( \nu \) as the following:
\[ \nu: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\mu_{pq})/\mathbb{Q}) \simeq (\mathbb{Z}/pq\mathbb{Z})^\times. \]
It suffices to show for every \( \tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) fixing \( J[\ell] \) that we have \( \nu(\tau) = 1 \).
Let \( D \) be any nonzero element of \( J[\ell] \). Then for every \( z \in \mathbb{Z} \), we have \( \tau z D = z \tau D \).
Therefore,
\[ D = z^{-1} z D = z^{-1} \tau z D = z^{\nu(\tau)-1} \tau D = z^{\nu(\tau)-1} D. \]
Therefore, \( z^{\nu(\tau)-1} \) must fix every element of \( J[\ell] \). If it were the case that \( \nu(\tau) \neq 1 \), then either \( Z^p \) or \( Z^q \) must act trivially on \( J[\ell] \), which forces \( \ell \) to be either \( p \) or \( q \).

Definition 2.10. For \( \ell \in \{ p, q \} \), let \( m_\ell \) be the maximal ideal of \( \mathcal{O}_{\ell} \).

Definition 2.11. Let \( \zeta_\ell \) be the automorphism given by \( (x, y) \mapsto (x, \zeta_\ell y) \).
Let \( \zeta_q \) be the automorphism given by \( (x, y) \mapsto (\zeta_q x, y) \).

Lemma 2.12. Suppose that \( \alpha \) is an endomorphism of \( T_{\ell} J \) that commutes with \( Z \) and that \( k \) is a nonnegative integer.

1. Note that \( \alpha \) induces an endomorphism of \( J[\ell^k] \). Then \( \alpha \) acts as the identity on \( J[\ell^k] \) if and only if \( \alpha \) acts on each \( T_{\chi} \) by multiplication by some element of \( 1 + \ell^k \mathcal{O}_{\ell} \) (i.e., if and only if \( \xi_{\chi}(\alpha) \in 1 + \ell^k \mathcal{O}_{\ell} \) for every \( \chi \)).
(2) Suppose \( \ell \in \{p, q\} \). Since \( \alpha \) commutes with \( \zeta_\ell \), it induces an endomorphism of \( J[(1 - \zeta_\ell)^k] \). Then \( \alpha \) acts as the identity on \( J[(1 - \zeta_\ell)^k] \) if and only if \( \alpha \) acts on each \( T_\chi \) by multiplication by some element of \( 1 + m_\ell^k \) (i.e., if and only if \( \xi_\chi(\alpha) \in 1 + m_\ell^k \) for every \( \chi \)).

**Proof.** By extending scalars, \( \alpha \) is also an endomorphism of \( T_\ell J \otimes \mathbb{Z}_\ell \mathcal{O}_\ell \).

(1) As
\[
J[\ell^k] = T_\ell J/\ell^k,
\]
we see that \( \alpha \) acts trivially on \( J[\ell^k] \) if and only if it acts trivially on \( T_\ell J/\ell^k \), if and only if (after extending scalars), it acts trivially on each \( T_\chi/\ell^k \).

Since \( \alpha \) commutes with \( Z \), it acts on each \( T_\chi \) by multiplication by an element of \( \mathcal{O}_\ell \). As \( T_\chi \simeq \mathcal{O}_\ell \) (as \( \mathcal{O}_\ell \)-modules) induces the isomorphism \( T_\chi/\ell^k \simeq \mathcal{O}_\ell/\ell^k \mathcal{O}_\ell \), the conclusion of the lemma follows.

(2) This proof is very similar to the previous part. Replace “\( \ell \)” with “\( 1 - \zeta_\ell \)” and \( \ell^k \mathcal{O}_\ell \) with \( \mathfrak{m}_\ell^k \).

\( \square \)

Using results of [Kat81], we can get an expression for \( \xi_\chi(g) \) when \( g \) is a Frobenius element, in terms of Jacobi sums. To do so, first select a prime \( r \not\in \{p, q, \ell\} \) and a prime \( \tau \) of \( \mathbb{Q}(\mu_{pq}) \) lying over \( r \) whose residue field is \( \mathbb{F}_r \). Since \( r \not\in \{p, q\} \), all the automorphisms in \( Z \) can be reduced to automorphisms over \( \mathbb{F}_r \). Moreover, if we let \( Z_r \) be the collection of these automorphisms defined over \( \mathbb{F}_r \), there is a natural isomorphism \( Z \simeq Z_r \) and also a natural isomorphism \( Z_\ell \simeq \mu_{pq}(\mathbb{F}_r) \).

The following lemma is essentially a reformulation of some of the results in the first three sections of [Kat81].

**Lemma 2.13.** Select a prime \( r \not\in \{p, q, \ell\} \), a prime \( \tau \) of \( \mathbb{Q}(\mu_{pq}) \) lying over \( r \) with residue field \( \mathbb{F}_r \), and a Frobenius element \( \text{Frob}_r \in H_{\infty, \ell} \) (note this is well-defined since \( \mathbb{Q}(\mu_{pq}, J[\ell^\infty]) \) is unramified over \( r \) by the criterion of Néron-Ogg-Shafarevich). Suppose that the size of \( \mathbb{F}_r \) is \( R \).

Suppose \( \chi : Z \rightarrow \mathcal{O}_\ell^\times \) is a character. Define \( \tilde{\chi} : \mathbb{F}_r^\times \rightarrow \mathcal{O}_\ell^\times \) as the composite of the “exponentiation by \( (R - 1)/(pq) \) map” \( \mathbb{F}_r^\times \rightarrow \mu_{pq}(\mathbb{F}_r) \) and the natural isomorphisms \( \mu_{pq}(\mathbb{F}_r) \simeq Z_r, Z_\ell \simeq Z \), and the character \( \hat{\chi} : Z \rightarrow \mathcal{O}_\ell^\times \).

Then
\[
\xi_\chi(\text{Frob}_r) = - \sum_{\alpha \in \mathbb{F}_r \setminus \{0, 1\}} \tilde{\chi}^p(\alpha) \hat{\chi}^q(1 - \alpha).
\]

**Proof.** From [Kat81] Lemma 1.1, we know that \( \text{Frob}_r \) operates on the \( \chi \)-isotypical part \( T_\chi \) of the Tate module \( T_\ell J \simeq H^1_{\text{et}}(\mathcal{C}, \mathbb{Q}_\ell) \) via multiplication by
\[
-S(\mathcal{C}/\mathbb{F}_r, \chi, 1) := -\frac{1}{|Z|} \sum_{z \in Z} \chi(z) \# \text{Fix}(\text{Frob}_r z^{-1})
\]
In this last expression, the quantity \( \# \text{Fix}(\text{Frob}_r z^{-1}) \) is the number of points of \( \mathcal{C}(\mathbb{F}_r) \) fixed by \( \text{Frob}_r z^{-1} \).

Now choose some \( z \in Z \). Write \( z = \bar{z}_p z_q \) where \( \bar{z}_p \) and \( z_q \) have order \( p \) and \( q \), respectively. Since \( Z \simeq Z_r \), we identify \( z, \bar{z}_p, z_q \) with automorphisms of \( \mathcal{C} \) defined over \( \mathbb{F}_r \). Let \( \zeta_p \) and \( \zeta_q \)
denote elements of $\mathbf{F}_r^\times$ such that (i) $\zeta_p$ is the scalar by which $z_p$ acts on the $y$-coordinate by multiplication, (ii) $\zeta_q$ is the scalar by which $z_q$ acts on the $x$-coordinate by multiplication.

Recall that $R$ is the size of $\mathbf{F}_r$. Note that $(x, y)$ is fixed by $\text{Frob}_r z^{-1}$ if and only if we have the following:

$$x^R = \zeta_q x$$
$$y^R = \zeta_q y.$$  

From these equations we see that $x^q$ and $y^p$ are both fixed by $\text{Frob}_r$, so $x^q, y^p \in \mathbf{F}_r$. We also have $y^p = x^q + 1$. Setting $\alpha = -x^q$ then, we have that $x^q = -\alpha$, $y^p = 1 - \alpha$ and that $\alpha \in \mathbf{F}_r$.

Suppose $x, y \neq 0$. Then from $\alpha$ we can recover $\zeta_p$ and $\zeta_q$ by $\zeta_q = x^{R-1} = (-\alpha)^{(R-1)/q}$ and $\zeta_p = y^{R-1} = (1 - \alpha)^{(R-1)/p}$. In particular, from our definition of $\chi$ we know that

$$\chi(z_q) = \tilde{\chi}^p(-\alpha)$$
$$\chi(z_p) = \tilde{\chi}^q(1 - \alpha)$$

When $R$ is odd, we know that $(R - 1)/q$ will be even, so $\tilde{\chi}^p(-\alpha) = \tilde{\chi}^p(-1)\chi^p(\alpha) = \tilde{\chi}^p(\alpha)$ as $(-1)^{(R-1)/q} = 1$. When $R$ is even, we know that $\alpha = -\alpha$ so in any case we can remove the minus sign to get

$$\chi(z_q) = \tilde{\chi}^p(\alpha)$$
$$\chi(z_p) = \tilde{\chi}^q(1 - \alpha).$$

Multiplying these two equations gives

$$\chi(z) = \tilde{\chi}^p(\alpha)\tilde{\chi}^q(1 - \alpha).$$

Since we made the assumption that $x, y \neq 0$, let $\mathcal{C}(\mathbf{F}_q)^*$ be the subset of $\mathcal{C}(\mathbf{F}_q)$ where neither the $x$- nor the $y$-coordinate is zero.

Going back to our sum, we then have

$$\sum_{z \in \mathbf{Z}} \chi(z) \# \text{Fix}(\text{Frob}_r z^{-1}) = \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathcal{C}(\mathbf{F}_r)^*} 1 \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathcal{C}(\mathbf{F}_r)^*} 1$$

$$= \sum_{(x, y) \in \mathcal{C}(\mathbf{F}_r)^*} \sum_{z \in \mathbf{Z}} \chi(z) \
= \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathcal{C}(\mathbf{F}_r)} 1 \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathcal{C}(\mathbf{F}_r)} 1$$

$$= \sum_{\alpha \in \mathbf{F}_r \setminus \{0, 1\}} \sum_{(x, y, z) \in \mathbf{F}_r^2 \times \mathbf{Z}} \chi^p(\alpha) \tilde{\chi}^q(1 - \alpha)$$

$$+ \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathbf{F}_r^2} 1 \sum_{z \in \mathbf{Z}} \chi(z) \sum_{(x, y) \in \mathbf{F}_r^2} 1.$$
Note that the last two sums are zero because for example, in the first sum the condition \( y^p = 1 \) immediately implies \( y^{R-1} = 1 \), so \( y^R = y \) and that forces \( z \) to fix the \( y \) coordinate. Hence this forces \( z \in \mathbb{Z}^p \) and the sum equals
\[
\sum_{z \in \mathbb{Z}} \chi(z) \sum_{y \in \mathbb{F}_r^{(0)}} 1 = \sum_{y \in \mu_p(\mathbb{F}_r)} \sum_{z \in \mathbb{Z}^p} \chi(z) = \sum_{y \in \mu_p(\mathbb{F}_r)} 0 = 0.
\]
Therefore, we have
\[
\sum_{z \in \mathbb{Z}} \chi(z) \# \text{Fix}(\text{Frob}_z z^{-1}) = \sum_{\alpha \in \mathbb{F}_r \setminus \{0,1\}} \sum_{(x,y) \in \mathbb{F}_r^2 \times \mathbb{Z}} \frac{\chi^p(\alpha) \chi^q(1-\alpha)}{x^q = \alpha, y^p = 1-\alpha}.
\]
In this final inner sum, we know that \( z \) is determined by \( \alpha \): the equations \( x^q = -\alpha \) and \( x^p = 1 - \alpha \) force \( x^R = (-\alpha)^{(R-1)/q} x \) and \( y^R = (1 - \alpha)^{(R-1)/p} y \), so that means that \( z \) must scale the \( x \)-coordinate by \( (-\alpha)^{(R-1)/q} \) and the \( y \)-coordinate by \( (1 - \alpha)^{(R-1)/p} \). So we may rewrite this as
\[
\sum_{z \in \mathbb{Z}} \chi(z) \# \text{Fix}(\text{Frob}_z z^{-1}) = \sum_{\alpha \in \mathbb{F}_r \setminus \{0,1\}} \sum_{(x,y) \in \mathbb{F}_r^2 \times \mathbb{Z}} \frac{\chi^p(\alpha) \chi^q(1-\alpha)}{x^q = -\alpha, y^p = 1-\alpha}.
\]
Since \( \alpha \notin \{0,1\} \), there are exactly \( pq = |\mathbb{Z}| \) such pairs \((x,y)\) satisfying \( x^q = -\alpha, y^p = 1-\alpha \). So this sum simplifies to
\[
\sum_{z \in \mathbb{Z}} \chi(z) \# \text{Fix}(\text{Frob}_z z^{-1}) = |\mathbb{Z}| \sum_{\alpha \in \mathbb{F}_r \setminus \{0,1\}} \chi^p(\alpha) \chi^q(1-\alpha).
\]
Dividing both sides by \(-|\mathbb{Z}|\) and recalling that \( \zeta(\text{Frob}_z) = -\frac{1}{|\mathbb{Z}|} \sum_{z \in \mathbb{Z}} \chi(z) \# \text{Fix}(\text{Frob}_z z^{-1}) \), we are done.

**Definition 2.14.** For two characters \( \psi, \psi' : \mathbb{F}_r^\times \to \mathcal{O}_r^\times \), define the Jacobi sum \( J(\psi, \psi') \) to be
\[
J(\psi, \psi') := \sum_{\alpha \in \mathbb{F}_r \setminus \{0,1\}} \psi(\alpha) \psi'(1-\alpha).
\]
That is, \( \zeta(\text{Frob}_z) = -J(\tilde{\chi}^p, \tilde{\chi}^q) \). Applying Lemma 2.12 to our situation with \( \alpha = \text{Frob}_z \), we obtain the following corollary.

**Corollary 2.15.** Suppose that \( \ell \) is a prime and \( k \) is a nonnegative integer.

1. Then \( \text{Frob}_z \) acts as the identity on \( J[\ell^k] \) if and only if for every character \( \tilde{\chi} : \mathbb{F}_r^\times \to \mathcal{O}_r^\times \), we have
\[
1 + J(\tilde{\chi}^p, \tilde{\chi}^q) \in \ell^k \mathcal{O}_r.
\]

2. Suppose \( \ell \in \{p,q\} \). Then \( \text{Frob}_z \) acts as the identity on \( J[(1 - \zeta(\ell))^k] \) if and only if for every character \( \tilde{\chi} : \mathbb{F}_r^\times \to \mathcal{O}_r^\times \), we have
\[
1 + J(\tilde{\chi}^p, \tilde{\chi}^q) \in \mathfrak{m}_r^k.
\]

**Lemma 2.16.** Fix a prime \( \ell \) and a nonnegative integer \( k \). Then

1. Suppose \( \ell \notin \{p,q\} \) and \( D \) is a divisor of exact order \( \ell^{k+1} \); that is, \( D \in J[\ell^{k+1}] \setminus J[\ell^k] \). Then \( Q(D, \mu_{pq}) = Q(J[\ell^{k+1}], \mu_{pq}) \).
(2) Suppose \( \ell \in \{p, q\} \) and \( D \) is a divisor of exact order \( (1 - \zeta_\ell)^{k+1} \); that is, \( D \in J[(1 - \zeta_\ell)^{k+1}] \setminus J[l(1 - \zeta_\ell)^k] \). Then \( Q(D, \mu_{pq}) = Q(J[(1 - \zeta_\ell)^{k+1}], \mu_{pq}) \).

**Proof.** The inclusions \( Q(D, \mu_{pq}) \subseteq Q(J[\ell^{k+1}], \mu_{pq}) \) and \( Q(D, \mu_{pq}) \subseteq Q(J[(1 - \zeta_\ell)^{k+1}], \mu_{pq}) \) are immediate.

(1) By Galois theory, it suffices to show that any \( h \in \text{Gal}(Q(J[\ell^{k+1}], \mu_{pq})/Q(\mu_{pq})) \) fixing \( D \) must be the identity. Suppose \( h \) is such an element. By the Chebotarev Density Theorem, we can assume \( h = \text{Frob}_l \). By Corollary \[2.15\] (1), we need to show that \( 1 + J(\overline{\chi^p}, \overline{\chi^q}) \in \ell^{k+1}O_\ell \) for every \( \overline{\chi} \). We see that \( J(\overline{\chi^p}, \overline{\chi^q}) \) is actually an element of \( Z[\zeta_{pq}] \), so we just need to show that \( 1 + J(\overline{\chi^p}, \overline{\chi^q}) \in \ell^{k+1}O_\ell \) for some \( \overline{\chi} \) (since the others are just Galois conjugates of our favorite one).

Consider the map \( T_\ell J \hookrightarrow T_\ell J \otimes_{\mathbb{Z}_l} O_\ell \simeq \bigoplus_{\chi} T_\chi \). Taking a quotient by \( \ell^{k+1} \), we get a map \[J[\ell^{k+1}] \leftrightarrow \bigoplus_{\chi} T_\chi/\ell^{k+1}T_\chi.\]

Note that the image of \( J[\ell^k] \) will be \( \bigoplus_{\chi} T_\chi/\ell^{k+1}T_\chi. \) Since \( D \in J[\ell^{k+1}] \setminus J[\ell^k] \), there will be some \( \chi \) such that the image of \( D \) in the projection to \( T_\chi/\ell^{k+1}T_\chi \) will land in \( \left(T_\chi/\ell^{k+1}T_\chi\right) \setminus \left(\ell T_\chi/\ell^{k+1}T_\chi\right). \)

For convenience, let \( D_\chi \) be the image of \( D \) in \( T_\chi/\ell^{k+1}T_\chi \). Since \( h \) fixes \( D \), we know that \( \xi_\chi(h) \) fixes \( D_\chi \). We also have \( D_\chi \in \left(T_\chi/\ell^{k+1}T_\chi\right) \setminus \left(\ell T_\chi/\ell^{k+1}T_\chi\right) \simeq \left(O_\ell/\ell^{k+1}O_\ell\right) \setminus \left(\ell O_\ell/\ell^{k+1}O_\ell\right). \)

Let \( R_\ell \) be the local ring \( O_\ell/\ell^{k+1}O_\ell \) with maximal ideal \( m_{R_\ell} = \ell R_\ell \). Then \( D_\chi \) is a unit of \( R_\ell \), so its annihilator must be zero. Hence the image of \( \xi_\chi(h) - 1 \) is zero in \( R_\ell \). In other words, we know that \( \xi_\chi(h) - 1 \in \ell^{k+1}O_\ell \). Hence by Lemma \[2.13\] we have \( 1 + J(\overline{\chi^p}, \overline{\chi^q}) = 1 - \xi_\chi(h) \in \ell^{k+1}O_\ell \), which completes the proof.

(2) The proof is very similar to the previous part. Replace “\( \ell \)” with \( 1 - \zeta_\ell \).

\[ \square \]

### 3. Computation of Some Torsion Fields

In this section, we use results of [Aru19] to compute some torsion fields.

**Definition 3.1.** Let \( \zeta_p \) be the automorphism given by \((x, y) \mapsto (x, \zeta_p y)\).

Let \( \zeta_q \) be the automorphism given by \((x, y) \mapsto (\zeta_q x, y)\).

For nonnegative \( i, j \) define

\[ L_{i,j} := Q(J[(1 - \zeta_p)^i(1 - \zeta_q)^j]) \]

Note that \( J[(1 - \zeta_p)^{p-1}(1 - \zeta_q)^{q-1}] = J[pq] \), so \( L_{p-1,q-1} = Q(J[pq]) \).

**Lemma 3.2.** We have the following facts about the fields \( L_{1,1}, L_{1,2}, L_{2,1} \):

1. The field \( L_{1,1} \) is \( Q(\mu_{pq}) \).
2. The field extension \( L_{2,1}/L_{1,1} \) is generated by the \( p \)-th roots of the numbers \( 1 - \zeta_p^i \).
3. The field extension \( L_{1,2}/L_{1,1} \) is generated by the \( q \)-th roots of the numbers \( 1 - \zeta_p^j \).
4. The field extensions \( L_{2,1}/L_{1,1} \) and \( L_{1,2}/L_{1,1} \) are nontrivial.
Proof.

(1) The field $L_{1,1}$ is generated by the points whose $x$-coordinates are zero and the points whose $y$-coordinates are zero, so it is exactly $\mathbb{Q} (\zeta_{pq})$.

(2) Let $L$ be a number field containing $L_{1,1} = \mathbb{Q} (\zeta_{pq})$ and $A = L[T]/(T^q + 1)$. Then we know that we have the “$x - T$” map

$$J(L)/(1 - \zeta_p)J(L) \hookrightarrow \ker(A^\times/(A^\times)^p) \overset{N}{\longrightarrow} L^\times/(L^\times)^p$$

which is essentially the Galois cohomology coboundary map

$$J(L)/(1 - \zeta_p)J(L) \hookrightarrow H^1(L, J[1 - \zeta_p])$$

arising from the short exact sequence

$$0 \rightarrow J[1 - \zeta_p] \rightarrow J \overset{1 - \zeta_p}{\longrightarrow} J \rightarrow 0.$$

The key point is that $H^1(L, J[1 - \zeta_p])$ is isomorphic to $\ker(A^\times/(A^\times)^p) \overset{N}{\longrightarrow} L^\times/(L^\times)^p)$ and that the image of a point $(a, b) \in C(L) \subseteq J(L)$ is $a - T$.

See [Poo06] Section 6.3 for more details of the “$x - T$” map; Poonen treats the hyperelliptic situation for the “multiplication by 2” isogeny, but this generalizes in a straightforward fashion in the superelliptic case and the “multiplication by (1 − $\zeta_p$)” isogeny.

In order for $L$ to contain the $(1 - \zeta_p)^2(1 - \zeta_q)$-torsion of $J$, it only needs to contain the $(1 - \zeta_p)^2$-torsion (since it already has the $(1 - \zeta_q)(1 - \zeta_q)$-torsion as it contains $\mu_{pq}$). Therefore it is sufficient for it to contain all divisors $D$ such that $(1 - \zeta_p)D \sim (-\zeta_q^i, 0) - \infty$ for $0 \leq i \leq q - 1$. That is, the points $(-\zeta_q^i, 0) - \infty$ need to be mapped to the identity in the above “$x - T$” map.

So we need $-\zeta_q^i - T$ to lie in $(A^\times)^p$. The Chinese remainder theorem gives that this is equivalent to $\zeta_q^j - \zeta_q^i$ being a $p$th-power for all $i, j$. Since $L$ already contains $\mu_{pq}$, this is equivalent to $1 - \zeta_q^k$ being a $p$th power for all $k$.

(3) Similar to the proof of part 2.

(4) We see that $L_{2,1}/L_{1,1}$ is nontrivial; the latter is similar. Consider the ramification of $L_{2,1}$ and $L_{1,1}$ above the prime $q$. Note that as $L_{2,1}$ contains $(1 - \zeta_q)^{1/p}$, we see that $e_q(L_{2,1}/\mathbb{Q}) \geq p(q - 1)$. However the degree of the extension $L_{1,1}/\mathbb{Q}$ is only $(p - 1)(q - 1)$, so $L_{2,1}$ has to strictly contain $L_{1,1}$.

Lemma 3.3. We have the following facts about the fields $L_{p-1,1}$, $L_{1,q-1}$, $L_{p-1,q-1}$.

(1) The extension $L_{p-1,1}/L_{1,1}$ is a $p$-Kummer extension; it is generated by $p$-th roots of elements of $L_{1,1} = \mathbb{Q} (\mu_{pq})$.

(2) The extension $L_{1,q-1}/L_{1,1}$ is a $q$-Kummer extension; it is generated by $q$-th roots of elements of $L_{1,1} = \mathbb{Q} (\mu_{pq})$.

Proof. Both parts are similar so we prove the first. From Remark 2.5 we know that the extension is abelian. Since $L_{1,1}$ already contains the $p$th roots of unity, it suffices to check that the exponent of $\text{Gal}(L_{p-1,1}/L_{1,1})$ divides $p$. To do so, we need to check that for every $h \in \text{Gal}(L_{p-1,1}/L_{1,1})$ that $h^p = 1$. From Lemma 2.12 we know that $\xi_\chi(h) \in 1 + m_p$ for all $\chi$. In particular,

$$\xi_\chi(h^p) = \xi_\chi(h)^p \in (1 + m_p)^p \subseteq 1 + pO_p,$$

so again by Lemma 2.12 we see that $h^p$ acts trivially on $J[p]$; hence, $h^p = 1$ as desired.
Using the main result in [Aru19], we can actually determine \( L_{p-1,1} \) and \( L_{1,q-1} \). Theorem 1.5 in [Aru19] states the following.

**Theorem 3.4.** Fix a prime \( r \) of \( \mathbb{Q}(\mu_{pq}) \) lying over a prime \( r \) of \( \mathbb{Q} \) such that \( r \not\in \{p,q\} \). Let \( \zeta_p \) and \( \zeta_q \) denote primitive \( p \)th and \( q \)th roots of unity in \( \mathbb{F}_r \). Take any Jacobi sum \( J = J(\overline{\chi}^p, \overline{\chi}^q) \) and an integer \( k \) in the range \( 2 \leq k \leq p - 1 \). Then

1. \( J + 1 \) always lies in \( \mathfrak{m}_p \).
2. \( J + 1 \) lies in \( \mathfrak{m}_p^k \) if and only if for each \( i \) in the range \( 0 \leq i \leq k - 2 \) and \( j \) in the range \( 1 \leq j \leq q - 1 \), we have

\[
\prod_{r=0}^{p-1} (1 - \zeta_q^r \zeta_p^r)^{(i)} \in (\mathbb{F}^\times_p)^j.
\]

Combining Theorem 3.4 and Corollary 2.15 we conclude that

**Corollary 3.5.** Fix a prime \( r \) of \( \mathbb{Q}(\mu_{pq}) \) lying over a prime \( r \) of \( \mathbb{Q} \) such that \( r \not\in \{p,q\} \). Let \( k \) be an integer in the range \( 2 \leq k \leq p - 1 \). Then

1. \( \text{Frob}_r \) always acts as the identity on \( J(1 - \zeta_p) \).
2. \( \text{Frob}_r \) acts as the identity on \( J(1 - \zeta_p^k) \) if and only if for each \( i \) in the range \( 0 \leq i \leq k - 2 \) and \( j \) in the range \( 1 \leq j \leq q - 1 \), we have

\[
\prod_{r=0}^{p-1} (1 - \zeta_q^r \zeta_p^r)^{(i)} \in (\mathbb{F}^\times_p)^j.
\]

Now applying the Chebotarev density theorem, Corollary 3.5 allows us to understand the field extension \( L_{1,k}/\mathbb{Q}(\mu_{pq}) \) for every \( k \) in the range \( 1 \leq k \leq p - 1 \). (Similarly, we also understand \( L_{1,k} \) for \( k \) in the range \( 1 \leq k \leq q - 1 \).) We get the following result.

**Theorem 3.6.** Let \( k \) be an integer in the range \( 2 \leq k \leq p - 1 \). Then

1. \( L_{1,1} = \mathbb{Q}(\mu_{pq}) \).
2. \( L_{k,1} = L_{k-1,1} \left( \sqrt[p]{\prod_{r=0}^{p-1} (1 - \zeta_q^r \zeta_p^r)^{(i)} : 1 \leq j \leq q - 1} \right) \).

Let us investigate the case \( k = 4 \) a bit more closely.

**Lemma 3.7.** Suppose \( p \geq 5 \) and that \( q^2 \not\equiv 1 \mod p \). Then the field \( L_{4,1} \) contains

\[
\mathbb{Q}(\mu_{pq}, \sqrt[q]{q}) \quad \text{and} \quad \mathbb{Q}(\mu_{pq}, \sqrt[p]{\prod_{s=0}^{p-1} (1 - \zeta_p^s)^{s^2}})
\]

The intersection of these subfields is \( \mathbb{Q}(\mu_{pq}) \).

**Proof.** We already get \( \sqrt[q]{q} \) in \( L_{2,1} \) because setting \( i = 0 \) and taking a product over the \( j \) gives

\[
\prod_{j=1}^{q-1} \prod_{s=0}^{p-1} \sqrt[p]{(1 - \zeta_q^j \zeta_p^s)^{(i)}} = \prod_{j=1}^{q-1} \sqrt[p]{1 - \zeta_p^{ps}} = \sqrt[q]{q}.
\]

Now do the same with \( i = 2 \) (we suppress the \( p \)-th root symbol for now):

\[
\prod_{j=1}^{q-1} \prod_{s=0}^{p-1} (1 - \zeta_q^j \zeta_p^s)^{(i)} = \prod_{s=0}^{p-1} \left( \frac{1 - \zeta_p^s}{1 - \zeta_p} \right)^{(i)}
\]
Up to an element of \((L_{1,1}^\times)^p\), we can simplify this expression further using the fact that 
\[\left(\begin{array}{c} a \\ 2 \end{array}\right) \equiv \left(\begin{array}{c} b \\ 2 \end{array}\right) \mod p \text{ whenever } a \equiv b \mod p.\] This gives

\[
\prod_{j=1}^{q-1} \prod_{s=0}^{p-1} (1 - \zeta_j^s \zeta_p^s) \left(\begin{array}{c} 2 \\ 2 \end{array}\right) = \prod_{s=0}^{p-1} \left(1 - \frac{\zeta_p^s}{1 - \zeta_p^s}\right) \left(\begin{array}{c} 2 \\ 2 \end{array}\right)
\]

\[
\equiv \prod_{s=1}^{p-1} (1 - \zeta_p^s)^{\left(\begin{array}{c} 2 \\ 2 \end{array}\right)} + \left(\begin{array}{c} 2 \\ 2 \end{array}\right) \mod (L_{1,1}^\times)^p
\]

\[
\equiv \prod_{s=1}^{p-1} (1 - \zeta_p^s)^{\frac{q^2-1}{2} s^2} \cdot \prod_{s=1}^{p-1} (1 - \zeta_p^s)^{\left(\begin{array}{c} 1-g \\ 2 \end{array}\right)} \mod (L_{1,1}^\times)^p
\]

\[
\equiv \left(\prod_{s=1}^{p-1} (1 - \zeta_p^s)^{s^2}\right)^{\frac{q^2-1}{2}} \cdot \left(\prod_{s=1}^{p-1} (1 - \zeta_p^s)^{\left(\begin{array}{c} 1-g \\ 2 \end{array}\right)}\right) \mod (L_{1,1}^\times)^p
\]

Note that the second product equals

\[
\prod_{s=1}^{p-1} (1 - \zeta_p^s)^s = \prod_{s=1}^{\frac{p-1}{2}} (1 - \zeta_p^s)^s \cdot \prod_{s=\frac{p+1}{2}}^{p-1} (1 - \zeta_p^s)^s
\]

\[
= \prod_{s=1}^{\frac{p-1}{2}} (1 - \zeta_p^s)^s \cdot \prod_{s=1}^{\frac{p-1}{2}} (1 - \zeta_p^{-s})^{p-s}
\]

\[
= \prod_{s=1}^{\frac{p-1}{2}} (-\zeta_p^{-s})^{p-s} (1 - \zeta_p)^p
\]

\[
= (-1)^{\sum_{s=1}^{\frac{p-1}{2}} s} \zeta_p^{\sum_{s=1}^{\frac{p-1}{2}} s^2} (1 - \zeta_p)^p \left(\begin{array}{c} \frac{p-1}{2} \\ 2 \end{array}\right).
\]

The first term is \((-1)^{q^2-1} = L_{4,1}^\times\), the second term is \(\zeta_p^{p(q^2-1)/24}\). Since \(p \geq 5\), the second term is just 1. In any case, this means that the entire expression is a \(p\)th power. So

\[
\prod_{j=1}^{q-1} \eta_{2,j} \equiv \left(\prod_{s=1}^{p-1} (1 - \zeta_p^s)^s\right)^{\frac{q^2-1}{2}} \mod (L_{1,1}^\times)^p.
\]

Since by assumption \(p\) is odd and \(q^2 \neq 1 \mod p\), it follows that \(\prod_{s=1}^{p-1} (1 - \zeta_p^s)^s\) has a \(p\)th root if and only if \(\prod_{j=1}^{q-1} \eta_{2,j}\) does. Since each \(\eta_{2,j}\) is a \(p\)th power in \(L_{4,1}\), it follows that so is

\[
\prod_{s=1}^{p-1} (1 - \zeta_p^s)^s^2.
\]

For the last part of the lemma, we will show that the intersection of \(Q(\mu_{pq}, \sqrt[p]{q})\) and \(Q(\mu_{pq}, \sqrt[p]{L_{1,1}^\times})\) is exactly \(Q(\mu_{pq})\). Note that both of these are Kummer extensions of \(Q(\mu_{pq})\) and their degrees divide \(p\), so we just need to show that they do not equal each other. Note that the extension \(Q(\mu_{pq}, \sqrt[p]{q})/Q(\mu_{pq})\) is totally ramified at \(q\), but the latter
extension $\mathbb{Q} \left( \mu_{pq}, \sqrt[p]{\prod_{s=0}^{p-1} (1 - \zeta_p^s)^2} \right) / \mathbb{Q}(\mu_{pq})$ is unramified at $q$. So the two fields are not equal, and hence their intersection must be $\mathbb{Q}(\mu_{pq})$. □

**Proposition 3.8.** Under the assumptions $p \geq 5$ and $q^2 \not\equiv 1 \mod p$, we have $[L_{4,1} : L_{1,1}] \geq p^2$.

**Proof.** By Lemma 3.7, we need only check that the subextensions $\mathbb{Q}(\mu_{pq}, \sqrt{q})/\mathbb{Q}(\mu_{pq})$ and $\mathbb{Q} \left( \mu_{pq}, \sqrt[p]{\prod_{s=0}^{p-1} (1 - \zeta_p^s)^2} \right) / \mathbb{Q}(\mu_{pq})$ are nontrivial. The former is nontrivial since it ramifies at $q$.

So we need only check that the latter is nontrivial. To do so, we need some notation for unit groups of cyclotomic fields. We follow [Was97] for this part. Let $E$ be the group of units of $\mathbb{Q}(\zeta_p)^+$, the totally real subfield of $\mathbb{Q}(\zeta_p)$. Let $C$ be the subgroup of cyclotomic units. The $p$-adic characters of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ are of the form $\omega^i$ for $0 \leq i \leq p - 2$, where $\omega$ is a Teichmüller character. The $p$-adic characters of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ are of the form $\omega^i$ where $i$ is even and in the range $0 \leq i \leq p - 2$. Let $\varepsilon_{\omega^i}(E/C)_p$ be the $\omega^i$-isotypic component of $E/C$. Let $A$ be the ideal class group of $\mathbb{Q}(\zeta_p)^+$ and $\varepsilon_{\omega^i}(A)$ be the $\omega^i$-isotypic component of $A$ (again, where $i$ is even). From [Was97] Theorem 15.7 we have

$$|\varepsilon_{\omega^i}A| = |\varepsilon_{\omega^i}(E/C)_p|$$

That is, the equality $|A| = |(E/C)_p|$ (that is, the class number of $\mathbb{Q}(\zeta_p)^+$ equals the index of the cyclotomic units inside the full unit group) holds component by component. Moreover, the $\omega^i$-isotypic component of $(E/C)_p$ is nontrivial if and only if the unit $E_i$ as defined in [Was97] (Section 8.3, page 155) is a $p$th power in $E$. From a calculation done on the same page, $E_i$ is a $p$th power if and only if the following is:

$$\prod_{a=1}^{p-1} \left( \zeta_p^{a(1-g)}/2 \frac{1 - \zeta_p^{ag}}{1 - \zeta_p^a} \right)^{a^{p-1}-i}$$

From a similar argument as in the proof of Lemma 3.7, this expression is a $p$th power in $\mathbb{Q}(\zeta_p)^+$ if and only if

$$\prod_{a=1}^{p-1} (1 - \zeta_p^a)^{a^{p-1}-i}$$

is a $p$th power in $\mathbb{Q}(\zeta_p)$. (The only difference between the unit group of $\mathbb{Q}(\zeta_p)^+$ and the unit group of $\mathbb{Q}(\zeta_p)$ is the torsion; i.e., the roots of unity.) So we conclude with $i = p - 3$ that the condition that $\prod_{s=0}^{p-1} (1 - \zeta_p^s)^2$ not being a $p$th power in $\mathbb{Q}(\zeta_p)$ is equivalent to $|\varepsilon_{\omega^{p-3}}| = 1$. From [Kur92] Corollary 3.8 we know that $|\varepsilon_{\omega^{p-3}}| = 1$, so indeed $\prod_{s=0}^{p-1} (1 - \zeta_p^s)^2$ is not a $p$th power in $\mathbb{Q}(\zeta_p)$.

A bit of Galois theory wraps up the rest: we have seen so far that the extension

$$\mathbb{Q} \left( \zeta_p, \sqrt[p]{\prod_{s=0}^{p-1} (1 - \zeta_p^s)^2} \right) / \mathbb{Q}(\zeta_p)$$
is nontrivial. Moreover the extension $\mathbb{Q}(\mu_{pq})/\mathbb{Q}(\zeta_p)$ is disjoint from this extension because the latter is totally ramified at $q$, while the former is unramified at $q$. So finally the extension

$$\mathbb{Q}\left(\mu_{pq}, \sqrt{\prod_{s=0}^{p-1}(1 - \zeta_p^s)^{s^2}}\right)/\mathbb{Q}(\mu_{pq})$$

is nontrivial.

\[\Box\]

4. Application to Torsion Points on $\mathcal{C}$

**Corollary 4.1.** Let $m$ be a positive integer. For each prime $\ell$ dividing $m$, choose an element $\lambda_\ell$ such that

$$\lambda_\ell \in \begin{cases} \mathbb{Z}_\ell & \text{if } \ell \not\in \{p, q\} \\ 1 + \ell \mathbb{Z}_\ell & \text{if } \ell \in \{p, q\} \end{cases}$$

Then there exists an element $\tau$ of $H_{\infty,m}$ such that for each $\ell$ dividing $m$, this element $\tau$ acts on $J[\ell^\infty]$ acts by multiplication as $\lambda_\ell$.

**Proof.** Let $h$ be any element of $H_{\infty,m}$ such that for each $\ell$ dividing $m$, the restriction of $h$ to $\text{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}(\mu_{pq}))$ is the one which raises each element of $\mu_{\ell^\infty}$ to the power of $\lambda_\ell$. Choosing $\tau = h\bar{h}$ then satisfies the desired property by Proposition 2.8.

We will also need a corollary of the Castelnuovo-Severi inequality. We state the Castelnuovo-Severi inequality here as it appears in [Poo07].

**Proposition 4.2** (Castelnuovo-Severi inequality). Let $F, F_1, F_2$ be function fields of curves over $k$, of genera $g, g_1, g_2$, respectively. Suppose that $F_i \subseteq F$ for $i = 1, 2$ and the compositum of $F_1$ and $F_2$ in $F$ equals $F$. Let $d_i = [F : F_i]$ for $i = 1, 2$. Then

$$g \leq d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1).$$

**Corollary 4.3.** Suppose that we have two maps $\mathcal{C} \to \mathbb{P}^1$ of degrees $d_1$ and $d_2$. If $d_1$ and $d_2$ are coprime, then

$$\text{genus}(\mathcal{C}) \leq (d_1 - 1)(d_2 - 1).$$

**Proof.** Let $F$ be the function field of $\mathcal{C}$. Each map gives an embedding of the function field of $\mathbb{P}^1$ into $F$; let their images be $F_1$ and $F_2$. Since $[F : F_i] = d_i$ and the $d_i$ are coprime, it follows that the compositum $F_1F_2$ equals $F$. We apply the Castelnuovo-Severi inequality in this situation with $g_1 = g_2 = 0$ to obtain the result.

The results up till now did not depend on $p, q \geq 3$, but we will certainly impose $p, q \geq 3$ from now on.

**Lemma 4.4.** Let $P_i, Q_i$ be points of $\mathcal{C}$ for $i \in \{1, 2, 3\}$.

1. If $P_1 + P_2 \sim Q_1 + Q_2$, then $\{P_1, P_2\} = \{Q_1, Q_2\}$.
2. Suppose $p, q \geq 5$. If $P_1 + P_2 + P_3 \sim Q_1 + Q_2 + Q_3$, then $\{P_1, P_2, P_3\} = \{Q_1, Q_2, Q_3\}$.

**Proof.** Let $f$ be a rational map $f : \mathcal{C} \to \mathbb{P}^1$ such that in case (1) we have $\text{div}(f) = P_1 + P_2 - Q_1 - Q_2$ and in case (2) we have $\text{div}(f) = P_1 + P_2 + P_3 - Q_1 - Q_2 - Q_3$.
(1) Suppose \( \{P_1, P_2\} \neq \{Q_1, Q_2\} \). Let \( f \) be a rational map \( f : C \to \mathbb{P}^1 \) such
\[
\text{div}(f) = P_1 + P_2 - Q_1 - Q_2
\]
Then \( f \) is either a degree 1 map or a degree 2 map to \( \mathbb{P}^1 \). We also have degree \( p \) and \( q \) maps to \( \mathbb{P}^1 \) via the \( x \)-map and \( y \)-map, respectively. By Corollary 4.3 this means that
\[
g \leq (2 - 1)(p - 1) \quad \text{and} \quad g \leq (2 - 1)(q - 1).
\]
Since \( g = (p - 1)(q - 1)/2 \), this would mean that \( q \leq 3 \) and \( p \leq 3 \), a contradiction since \( p, q \) are distinct odd primes.

(2) In the same way as the proof of the previous part, we assume \( \{P_1, P_2, P_3\} \neq \{Q_1, Q_2, Q_3\} \) to obtain a rational map \( f : C \to \mathbb{P}^1 \) such
\[
\text{div}(f) = P_1 + P_2 + P_3 - Q_1 - Q_2 - Q_3.
\]
Then the degree of \( f \) is at most 3, and since \( p, q \geq 5 \) we know that Corollary 4.3 gives
\[
g \leq (3 - 1)(p - 1) \quad \text{and} \quad g \leq (3 - 1)(q - 1)
\]
from which we get that \( p, q \leq 5 \) which contradicts our assumption that \( p, q \) are distinct primes that are at least 5.

\[\square\]

Using Corollary 4.1 and Lemma 4.4 we can bound the order of torsion points on \( C \).

**Proposition 4.5.** Suppose \( P \) is a torsion point of \( C \). Then \( 2pq(P - \infty) \sim 0 \).

**Proof.** Suppose \( m \) is a positive integer such that \( m(P - \infty) \sim 0 \). Without loss of generality, suppose \( m \) is divisible by \( 2pq \). Let \( \{r_1, \ldots, r_M\} \) be the set of primes that divide the prime-to-\( 2pq \)-part of \( m \).

Using Corollary 4.1 choose \( \tau_1, \tau_2, \tau_3 \in \text{Gal}(\mathbb{Q}(J[m])/\mathbb{Q}(\mu_{pq})) \) such that

- \( \tau_1 \) acts on \( J[2^\infty], J[p^\infty], J[q^\infty], J[r_i^\infty] \) as multiplication by \( 1 + 2 \), \( 1 + p \), \( 1 + q \), \( 2 \), respectively.
- \( \tau_2 \) acts on \( J[2^\infty], J[p^\infty], J[q^\infty], J[r_i^\infty] \) as multiplication by \( 1 - 2 \), \( 1 - p \), \( 1 - q \), \( -2 \), respectively.
- \( \tau_3 \) acts on \( J[2^\infty], J[p^\infty], J[q^\infty], J[r_i^\infty] \) as multiplication by 1.

Then by construction, we see that \( (\tau_1 + \tau_2) - (\tau_3 + 1) \) acts as the identity on \( J[m] \). In particular,
\[
\tau_1 P + \tau_2 P \sim \tau_3 P + P.
\]
Then by Lemma 4.4 (1) it follows that \( P \) is either \( \tau_1 P \) or \( \tau_2 P \).
If \( P = \tau_1 P \), then writing \( P - \infty = D_2 + D_p + D_q + \sum D_{ri} \) for divisors \( D_\ell \in J[[\ell]] \), we see that \( \tau_1 D_\ell = D_\ell \) for each \( \ell \). So in particular, \( 2D_2 \sim 0, pD_p \sim 0, qD_q \sim 0, \) and \( D_{ri} \sim 0 \) for each \( i \). Hence \( 2pq(P - \infty) \sim 0 \).

If \( P = \tau_2 P \), then a similar analysis shows that either (i) \( 2pq(P - \infty) \sim 0 \) or (ii) \( p, q \geq 5 \) and \( 6pq(P - \infty) \sim 0 \).

So the last case to consider is \( p, q \geq 5 \) and \( 6pq(P - \infty) \sim 0 \). In that case, find \( \tau_4 \in \text{Gal}(Q(J[m^\infty])/Q(\mu_{pq})) \) such that \( \tau_4 \) acts on \( J[3^\infty] \) as multiplication by \(-1\) and \( \tau_4 \) acts on \( J[(2pq)^\infty] \) as the identity. Then \( 3P \sim 3\tau_4 P \). Then by Lemma 4.6 (2) it follows that \( P = \tau_4 P \), so a similar analysis as before shows again that \( 2pq(P - \infty) \sim 0 \).

Next, we would like to remove the “2” in the statement of Proposition 4.5. To do so, we need to study ramification in torsion fields.

**Lemma 4.6.** We have the following.

1. The torsion field \( Q(J[2]) \) is ramified at 2.
2. Suppose \( D \) is a nonzero element of \( J[2] \). Then the field \( Q(D, \mu_{pq}) \) is ramified at 2.
3. The torsion field \( Q(J[pq]) \) is unramified at 2.

**Proof.**

1. From [Jęd16] applied with \( a = 1 \) we know that the reduction of the jacobian \( J \) at 2 is not ordinary. Applying Lemma 1.4 of [Gro78] now tells us that \( Q(J[2]) \) is ramified at 2.

2. From Lemma 2.16, we know that \( Q(D, \mu_{pq}) = Q(J[2]) \). So we are now done by the previous part and Lemma 2.9.

3. This follows from the criterion of Néron-Ogg-Shafarevich.

**Proposition 4.7.** If \( P \) is a torsion point on \( C \), then \( pq(P - \infty) \sim 0 \).

**Proof.** From Proposition 4.5 we know that \( P - \infty = D_2 + D_p + D_q \), where \( 2D_2, pD_p, qD_q \sim 0 \). Suppose \( D_2 \neq 0 \).

From Lemma 4.6, it follows that \( Q(J[pq]) \) cannot contain \( Q(D_2, \mu_{pq}) \). Hence we can find a \( \tau \in \text{Gal}(Q(J[2pq])/Q(J[pq])) \) which acts nontrivially on \( Q(D_2, \mu_{pq}) \). Since \( Q(\mu_{pq}) \subseteq Q(J[pq]) \) (due to the Weil pairing) it follows that \( \tau \) must act nontrivially on \( D_2 \).

Hence \( D_2 \neq \tau D_2 \) which implies \( P \neq \tau P \) and yet \( 2(P - \tau P) = 2(D_2 - \tau D_2) \sim 0 \), which violates Lemma 4.4. This contradiction implies \( D_2 = 0 \), as desired.

**Definition 4.8.** Choose \( a, b \) minimal such that

\[
(1 - \zeta_p)^a (1 - \zeta_q)^b P \sim 0.
\]

Define \( D_p, D_q \) such that \( P - \infty \sim D_p + D_q, pD_p \sim 0, \) and \( qD_q \sim 0 \).

In order to get a contradiction whenever \( a \) and \( b \) are large, we will use an argument with inflectionary weights of Weierstrass points. The following definitions can be found in an introductory book on Riemann surfaces, e.g. [Far92].

**Definition 4.9.** Given a point \( R \) on a nonsingular algebraic curve \( X \) of genus \( g \), an integer \( k \) is a gap of \( R \) if there is no rational function on \( X \) with a pole at \( R \) of exact order \( k \). By Riemann-Roch, there will be exactly \( g \) gaps and they will lie in the range \([1, 2g - 1]\). The set
of non-gaps forms a monoid, denoted by \( \text{WM}(R) \), the Weierstrass monoid of \( R \). If the gaps of \( R \) are \( k_1 < k_2 < \cdots < k_g \), then the inflectionary weight of \( R \) is

\[
\text{wt}(R) = \sum_{i=1}^{g} (k_i - i).
\]

The point \( R \) is called a Weierstrass point of \( X \) if \( \text{wt}(R) > 0 \).

We now use a basic result about Weierstrass points on a Riemann surface, found in [Mir95] as Corollary 4.17.

**Theorem 4.10.** The sum of the inflectionary weights of all the Weierstrass points on a Riemann surface \( X \) of genus \( g \) is \( g^3 - g \).

**Lemma 4.11.** Define

\[
S_P = \{hzP : h \in \text{Gal}(\mathbb{Q}(J[pq])/\mathbb{Q}(\mu_{pq})), z \in \mathbb{Z}\}
\]

1. If \( a \geq 2 \) and \( b \geq 1 \), then \( S_P \) has size at least \( pq[L_{a,1} : L_{1,1}] \) and for each \( Q \in S_P \) we have \( p - 1, p \in \text{WM}(Q) \).
2. If \( a \geq 1 \) and \( b \geq 2 \), then \( S_P \) has size at least \( pq[L_{1,b} : L_{1,1}] \) and for each \( Q \in S_P \) we have \( q - 1, q \in \text{WM}(Q) \).

**Proof.** Both parts are similar so we show the first.

Define

\[
E = D_p + (1 - \zeta_q)^b D_q
\]

Since \( a \geq 2, b \geq 1 \), we know that \( E \) is a divisor of exact order \( (1 - \zeta_p)^a(1 - \zeta_q) \). Therefore \( E \) is defined over \( L_{a,1} \).

To show that \(|S_P| \geq pq[L_{a,1} : L_{1,1}]\), we instead show the stronger statement that

\[
S_E = \{hzE : h \in \text{Gal}(\mathbb{Q}(D_p, \mu_{pq})/\mathbb{Q}(\mu_{pq})), z \in \mathbb{Z}\}
\]

already has size exactly equal to

\[
[\mathbb{Q}(D_p, \mu_{pq}) : \mathbb{Q}(\mu_{pq})] \cdot |\mathbb{Z}|.
\]

(By Lemma 2.16, we know that \( \mathbb{Q}(D_p, \mu_{pq}) = L_{a,1} \) so this latter number is exactly equal to \( [L_{a,1} : L_{1,1}]pq \).)

To do so, we need to check that all the elements \( hzE \) are distinct. Since \( \text{Gal}(\mathbb{Q}(D_p)/\mathbb{Q}(\mu_{pq})) \) is abelian and commutes with \( Z \), it suffices to check that if \( hE = zE \), then \( h = 1 \) and \( z = 1 \).

So assume now that \( hE = zE \). Since \( \zeta_p \) commutes with \( h, z \) we have that

\[
h(1 - \zeta_p)^{a-1}E = z(1 - \zeta_p)^{a-1}E.
\]

But \( (1 - \zeta_p)^{a-1}E \) is a \( (1 - \zeta_p)(1 - \zeta_q) \)-torsion divisor, and is hence defined over \( \mathbb{Q}(\mu_{pq}) \), so \( h \) is forced to fix it. Hence

\[
(1 - \zeta_p)^{a-1}E = z(1 - \zeta_p)^{a-1}E.
\]

But as \( (1 - \zeta_p)^{a-1}E \) has exact order \( (1 - \zeta_p)(1 - \zeta_q) \), the only element of \( Z \) that can fix it is 1; hence, \( z = 1 \).

As \( z = 1 \), we now assume \( hE = zE = E \). In particular, \( h \) also fixes \( D_p \). Hence \( h = 1 \) as well. We have now shown that

\[
|S_P| \geq |S_E| = [\mathbb{Q}(D_p, \mu_{pq}) : \mathbb{Q}(\mu_{pq})] \cdot |\mathbb{Z}| = pq[\mathbb{Q}(D_p, \mu_{pq}) : \mathbb{Q}(\mu_{pq})]
\]
It suffices to check that $p - 1, p \in \text{WM}(P)$. For this, let $h \in \text{Gal}(J[\mu_{pq}]/\mathbb{Q}(\mu_{pq}))$ be such that its restriction to $\text{Gal}(\mathbb{Q}(D_p, \mu_{pq})/\mathbb{Q}(\mu_{pq}))$ is nontrivial and its restriction to $\text{Gal}(\mathbb{Q}(J[q])/\mathbb{Q}(\mu_{pq}))$ is trivial. (This can be done since $a \geq 2$.) Then

$$h^iP \neq P \text{ for } 0 \leq i \leq p - 1. \quad (2)$$

(We know that $h^p = 1$ since the entire extension is $p$-Kummer.)

Since $h$ fixes the $q$-torsion, we know that $h(pP) \sim pP$. Therefore, $pP \sim p(hP)$ implies that $p \in \text{WM}(P)$. Moreover, we also see that $p \in \text{WM}(Q)$ for all $Q \in S_P$.

Moreover, note that $1 + h + h^2 + \cdots + h^{p-1}$ is an endomorphism of $J[\mu_{pq}]$. From Lemma 2.12 we know that for all $\chi$, $\xi_\chi(h) \in 1 + m_p$. Therefore,

$$1 + \xi_\chi(h) + \xi_\chi(h)^2 + \cdots + \xi_\chi(h)^{p-1} \in m_p^{p-1} = p\mathcal{O}_p.$$

So again by Lemma 2.12 we know that $1 + h + h^2 + \cdots + h^{p-1}$ acts trivially on $J[p]$. Since $h$ acts trivially on $J[q]$, we conclude that

$$(1 + h + h^2 + \cdots + h^{p-1}) - p \text{ acts trivially on } J[pq]$$

Therefore

$$hP + h^2P + \cdots + h^{p-1}P \sim (p - 1)P$$

and as $P \neq h^iP$ (by equation (2)) we see that $p - 1 \in \text{WM}(P)$ as well. Since this argument only used the fact that $P \in J[\mu_{pq}]$, we see it also applies to all $Q \in S_P$. \qed

**Proposition 4.12.**

1. If $a \geq 2$ and $b \geq 1$, then we must have $q = 3$ and $a \in \{2, 3\}$.
2. If $a \geq 1$ and $b \geq 2$, then we must have $p = 3$ and $b \in \{2, 3\}$.

**Proof.** Both parts are similar so we prove the first. By Lemma 4.11, there are at least $pq[L_{a,1} : L_{1,1}]$ points $P$ such that $p - 1, p \in \text{WM}(P)$.

We first obtain a lower bound on $\text{wt}(P)$ for such $P$. Since $p - 1, p \in \text{WM}(P)$, we know that $u(p - 1) + vp \in \text{WM}(P)$ for any $u, v \geq 0$. In particular, we know that

$$\{p - 1, p, 2p - 2, 2p - 1, 2p, 3p - 3, 3p - 2, 3p - 1, 3p, \cdots\} \subseteq \text{WM}(P).$$

\[\]
Therefore, a lower bound on the weight of $P$ is
\[
\text{wt}(P) = \sum_{i=1}^{g} (k_i - i) \\
\geq (1 - 1) + (2 - 2) + ((p - 2) - (p - 2)) \\
+ ((p + 1) - (p - 1)) + ((p + 2) - (p)) + \ldots + ((2p - 3) - (2p - 5)) \\
+ ((2p + 1) - (2p - 4)) + ((2p + 2) - (2p - 3)) + \ldots + ((3p - 4) - (3p - 9)) \\
+ \ldots \\
= 0 + \ldots + 0 + 2 + \ldots + 2 + 5 + \ldots + 5 + 9 + \ldots + 9 + \ldots \\
\text{p-2 times} \quad \text{p-3 times} \quad \text{p-4 times} \quad \text{p-5 times} \\
\geq 0 + \ldots + 0 + 2 + \ldots + 2 + 4 + \ldots + 4 + 6 + \ldots + 6 + \ldots \\
\text{p-1 times} \quad \text{p-1 times} \quad \text{p-1 times} \quad \text{p-1 times} \\
= (p - 1) \left( 0 + 2 + 4 + 6 + \ldots + 2 \left( \frac{q - 1}{2} \right) \right) \\
= (p - 1)(q - 3)(q - 1) \\
= \frac{g (q - 3)}{4}.
\]
By Lemma 3.3 (4) we know that $[L_{a,1} : L_{1,1}] \geq [L_{2,1} : L_{1,1}] \geq p$, so we have at least $p^2q$ of these points. Hence the total weight of all points on $C$ is at least
\[
g \left( \frac{q - 3}{2} \right) p^2q
\]
If $q \geq 5$, then we know that $q(q - 3) \geq \frac{5}{8}(q - 1)^2$ which means the total weight is at least
\[
g \left( \frac{q - 3}{2} \right) p^2q \geq g \left( \frac{5}{16} (q - 1)^2 \right) p^2 > \frac{5}{16} g ((p - 1)(q - 1))^2 = \frac{5}{4} g^3.
\]
This contradicts Theorem 4.10 which states that the total weight of all points on $C$ is $g^3 - g$.

Hence $q = 3$. If $a \geq 4$, then we know from Proposition 3.8 that $[L_{a,1} : L_{1,1}] \geq [L_{4,1} : L_{1,1}] \geq p^2$, so we have at least $p^3q$ of these points of weight at least
\[
\text{wt}(P) \geq (1 - 1) + (2 - 2) + \cdots + ((p - 2) - (p - 2)) + ((p + 1) - (p - 1)) = 2
\]
which means that the total weight is at least $2p^3q = 6p^3$. Since $g = (p - 1)(q - 1)/2 = p - 1$ and Theorem 4.10 states that the total weight of all points on $C$ is $g^3 - g = (p - 1)^3 - (p - 1) < p^3$, we have yet again a contradiction.

So the only remaining possibility is $q = 3$ and $a \in \{2, 3\}$. \hfill \Box

**Proposition 4.13.**

(1) It is impossible for $a = b = 1$.
(2) If $a = 0$, then $b \leq 1$.
(3) If $b = 0$, then $a \leq 1$.

**Proof.** (1) Suppose $a = b = 1$. Then
\[
(1 - \zeta_p)(1 - \zeta_q)P \sim 0
\]
which we rearrange to get
\[ P + \zeta_p \zeta_q P \sim \zeta_p P + \zeta_q P. \]
From Lemma 4.4 it follows that either \( P = \zeta_p P \) or \( P = \zeta_q P \), meaning that either \( a \) or \( b \) is 0.

(2) Suppose \( a = 0 \) and \( b \geq 1 \). We seek to show that \( b = 1 \).

Then \( qP \sim q\infty \). Let \( f \) be a function such that
\[ \text{div}(f) \sim qP - q\infty. \]
Since \( f \) only has poles at \( \infty \), it follows that \( f \) is a polynomial in \( x \) and \( y \). Since the pole order is \( q \), it follows that \( f(x, y) = y - g(x) \) where \( \deg(g) < q/p \). Let \( x_P \) be the \( x \)-coordinate of \( P \). From this it follows that
\[ \text{div} \left( \prod_{i=0}^{p-1} (\zeta_p^i y - g(x)) \right) = q \left( \sum_{i=0}^{p-1} \zeta_p^i P \right) - pq\infty. \]
Moreover we also have
\[ \text{div} \left( (x - x_P)^q \right) = q \left( \sum_{i=0}^{p-1} \zeta_p^i P \right) - pq\infty, \]
so it follows that \( \prod_{i=0}^{p-1} (\zeta_p^i y - g(x)) \) and \( (x - x_P)^q \) are the same up to a scalar. Simplifying the former expression, we see that
\[ \prod_{i=0}^{p-1} (\zeta_p^i y - g(x)) = y^p - g(x)^p = x^q + 1 - g(x)^p, \]
so we conclude
\[ (*) \quad x^q + 1 - g(x)^p = (x - x_P)^q. \]
Rewrite this as
\[ x^q + 1 - (x - x_P)^q = g(x)^p. \]
If \( g \) is nonconstant, then the right hand side has at least one root of order at least 3. However, this is not true of the left hand side: to see this, let \( L(x) = x^q + 1 - (x - x_P)^q \) and note
\[ L(x) = \frac{1}{q} (x - x_P) L'(x) = x_P x^{q-1} + 1 \]
has no double roots (hence \( L(x) \) has no triple roots).

This contradiction forces \( g \) to be a constant polynomial. Comparing the \( x^{q-1} \) coefficient of both sides of \( (*) \) then shows that \( x_P = 0 \). Hence \( P \) is a \( (1 - \zeta_q) \)-torsion point, forcing \( b = 1 \).

(3) Similar to the proof of the previous part.

\[ \square \]

Combining Propositions 4.12 and 4.13, the only cases we have left to consider are

(1) \( q = 3, a \in \{2, 3\}, b = 1 \)
(2) \( p = 3, a = 1, b \in \{2, 3\} \)
Both cases are similar so we handle the first. Hence from now on we suppose that $q = 3$, $b = 1$, $a \in \{2, 3\}$, and $p \geq 5$. We have that

$$(1 - \zeta_p^3)(1 - \zeta_3)P \sim 0,$$

which we rewrite as

$$(\zeta_p^3 \zeta_3 - \zeta_p^3 - 3\zeta_p^2 \zeta_3 + 3\zeta_p^2 + 3\zeta_p \zeta_3 - 3\zeta_p - \zeta_3 + 1)P \sim 0,$$

which we can rewrite as

$$\zeta_p^3 \zeta_3 P + 3\zeta_p^2 P + 3\zeta_p \zeta_3 P + P \sim \zeta_p^3 P + 3\zeta_p^2 \zeta_3 P + 3\zeta_p P + \zeta_3 P.$$

Since $p \geq 5$ and $q = 3$, the only way for any of these points $\{\zeta_p^i \zeta_3^j P\}$ to equal another is for $P$ to be in either $J[1 - \zeta_p]$ or $J[1 - \zeta_3]$. Therefore from this we get a degree 8 map to $\mathbb{P}^1$. Since we also have a degree 3 map to $\mathbb{P}^1$, we know from Corollary 4.3 that

$$g \leq (3 - 1)(8 - 1).$$

Since $g = (3 - 1)(p - 1)/2$, this means that

$$\frac{p - 1}{2} \leq 8 - 1,$$

so $p \leq 15$. Therefore we need only check that at the primes $p \in \{5, 7, 11, 13\}$ that there are no points $P \in J[(1 - \zeta_p)^3(1 - \zeta_3)] \setminus J[(1 - \zeta_p)(1 - \zeta_3)]$ in order to finish.

For the remaining three curves, the first step will be to compute explicitly the Galois action on $T_pJ$ to find that $L_{3,1}/L_{2,1}/L_{1,1}$ is a tower where each successive step is a nontrivial $p$-extension. The bottom extension $L_{2,1}/L_{1,1}$ is known to be nontrivial by Lemma 3.2 (4). So we need to show that the top extension is nontrivial.

The strategy will be to find primes $r$ such that for some prime $r$ of $\mathbb{Q}(\mu_{3p})$ lying above $r$, we have $\xi_r(Frob_r) - 1$ always has $\pi_p$-adic valuation 2. Then by Lemma 2.12, we will know that $Frob_r$ acts trivially on $J[(1 - \zeta_p)^2]$ but not on $J[(1 - \zeta_p)^3]$. In other words, $Frob_r$ will be a nontrivial element of $Gal(L_{3,1}/L_{2,1})$. By Theorem 3.4, we are searching for finite fields $F_R$ with $R \equiv 1 \mod 3p$ where

$$1 - \zeta_3, 1 - \zeta_3^2 \in F_R^p$$

$\eta_3, 1$ or $\eta_3, 2 \not\in F_R^p$.

With the help of a computer [Dev19], it does not take long to find such $R$. Here is a table with the smallest possible such $R$ satisfying these conditions for $p \in \{5, 7, 11, 13\}$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$2^4$</td>
</tr>
<tr>
<td>7</td>
<td>$13^2$</td>
</tr>
<tr>
<td>11</td>
<td>$43^2$</td>
</tr>
<tr>
<td>13</td>
<td>$547^2$</td>
</tr>
</tbody>
</table>

Now we can wrap up with one final lemma.

**Lemma 4.14.** The cases

1. $q = 3, p \in \{5, 7, 11, 13\}, a \in \{2, 3\}, b = 1$
2. $p = 3, q \in \{5, 7, 11, 13\}, a = 1, b \in \{2, 3\}$

are impossible.
Proof. Both cases are similar so we handle the first. Suppose \( a = 3 \). By our computation, there exists a nontrivial \( \gamma \in L_{3,1}/L_{2,1} \). By Lemma 2.16 we know that \( L_{3,1} = L_{2,1}(D_p) \), so \( \gamma \) must move \( D_p \) and hence it must move \( P \). Since 
\[
\xi_\chi(\gamma) \in 1 + m^3_p
\]
for every \( \chi \), we know that 
\[
\xi_\chi(\gamma) + \xi_\chi(\gamma^{-1}) - 1 \in 1 + m^6_p
\]
and hence \( \gamma + \gamma^{-1} - 1 \) must fix \( P \). (We are using Lemma 2.12 repeatedly.) So we can write 
\[
\gamma P + \gamma^{-1}P \sim P + P,
\]
and now by Lemma 4.4 we know that \( P \) must be either \( \gamma P \) or \( \gamma^{-1} P \), which is a contradiction.

If \( a = 2 \), we can do a very similar argument by picking \( \gamma \) to be a nontrivial element of \( \text{Gal}(L_{2,1}/L_{1,1}) \). \( \square \)

In summary, we have the following result.

**Corollary 4.15.** Suppose \( n, d \) are coprime integers, neither of which is a power of 2. The only torsion points on the curve \( y^n = x^d + 1 \) are those whose \( x \)-coordinate or \( y \)-coordinate is zero, and also the point at \( \infty \).

**Proof.** As done in the introduction, we reduce to the case where \( n, d \) are odd primes first. Pick an odd prime \( p \) dividing \( n \) and an odd prime \( q \) dividing \( d \). Then \( p \neq q \) since \( n \) and \( d \) are coprime. There is an the map from \( y^n = x^d + 1 \) to \( y^p = x^q + 1 \) given by \( (x, y) \mapsto (x^{d/q}, y^{n/p}) \) that sends torsion points to torsion points. By our work, we know that the only torsion points on the latter curve are those whose \( x \)- or \( y \)-coordinate is zero, and also the point at \( \infty \). The preimages of these points on the original curve are also points whose \( x \)-coordinate or \( y \)-coordinate is zero, and also the point at \( \infty \). \( \square \)

**References**
