NON-CYCLIC SUBGROUPS OF JACOBIANS OF GENUS TWO CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Let E be an elliptic curve defined over a finite field. Balasubramanian and Koblitz have proved that if the ℓ^{th} roots of unity μ_ℓ is not contained in the ground field, then a field extension of the ground field contains μ_ℓ if and only if the ℓ-torsion points of E are rational over the same field extension. We generalize this result to Jacobians of genus two curves. In particular, we show that the Weil- and the Tate-pairing are non-degenerate over the *same* field extension of the ground field.

From this generalization we get a complete description of the ℓ-torsion subgroups of Jacobians of supersingular genus two curves. In particular, we show that for $\ell > 3$, the ℓ-torsion points are rational over a field extension of degree at most 24.

1. Introduction

In [10], Koblitz described how to use elliptic curves to construct a public key cryptosystem. To get a more general class of curves, and possibly larger group orders, Koblitz [11] then proposed using Jacobians of hyperelliptic curves. After Boneh and Franklin [2] proposed an identity based cryptosystem by using the Weil-pairing on an elliptic curve, pairings have been of great interest to cryptography [6]. The next natural step was to consider pairings on Jacobians of hyperelliptic curves. Galbraith *et al* [7] survey the recent research on pairings on Jacobians of hyperelliptic curves.

The pairing in question is usually the Weil- or the Tate-pairing; both pairings can be computed with Miller's algorithm [14]. The Tate-pairing can be computed more efficiently than the Weil-pairing, cf. [5]. Let C be a smooth curve defined over a finite field $\mathbb{F}_q$, and let $\mathcal{J}_C$ be the Jacobian of C. Let ℓ be a prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian, and let k be the multiplicative order of q modulo ℓ. By [8], the Tate-pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. By [20, Proposition 8.1, p. 96], the Weil-pairing is non-degenerate on $\mathcal{J}_C[\ell]$. So if $\mathcal{J}_C[\ell]$ is not contained in $\mathcal{J}_C(\mathbb{F}_{q^k})$, then the Tate pairing is non-degenerate over a possible smaller field extension than the Weil-pairing. For elliptic curves, in most cases relevant to cryptography, the Weil-pairing and the Tate-pairing are non-degenerate over the same field: let E be an elliptic curve defined over $\mathbb{F}_p$, and consider a prime number ℓ dividing the number of $\mathbb{F}_p$-rational points on E. Balasubramanian and Koblitz [1] proved that

$$\text{(1)} \qquad \textit{if } \ell \nmid p-1, \textit{ then } E[\ell] \subseteq E(\mathbb{F}_{p^k}) \textit{ if and only if } \ell \mid p^k - 1.$$

2000 *Mathematics Subject Classification.* 11G20 (Primary) 11T71, 14G50, 14H45 (Secondary).

Key words and phrases. Jacobians, hyperelliptic genus two curves, pairings, embedding degree, supersingular curves.

Research supported in part by a PhD grant from CRYPTOMAThIC.

By Rubin and Silverberg [19], this result also holds for Jacobians of genus two curves in the following sense: *if $\ell \nmid p-1$, then the Weil-pairing is non-degenerate on $U \times V$, where $U = \mathfrak{J}_C(\mathbb{F}_p)[\ell]$, $V = \ker(\varphi - p) \cap \mathfrak{J}_C[\ell]$ and φ is the p-power Frobenius endomorphism on $\mathfrak{J}_C$.*

The result (1) can also be stated as: *if $\ell \nmid p-1$, then $E(\mathbb{F}_{p^k})[\ell]$ is bicyclic if and only if $\ell \mid p^k-1$.* In [17], the author generalized this result to certain CM reductions of Jacobians of genus two curves. In this paper, we show that in most cases, this result in fact holds for Jacobians of *any* genus two curves. More precisely, the following theorem is established.

Theorem 6. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism of the Jacobian $\mathfrak{J}_C$ as*

$$P_m(X) = X^4 + 2\sigma X^3 + (2q^m + \sigma^2 - \tau)X^2 + 2\sigma q^m X + q^{2m},$$

where $2\sigma, 4\tau \in \mathbb{Z}$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathfrak{J}_C$, and with $\ell \nmid q$ and $\ell \nmid q-1$. If $\ell \nmid 4\tau$, then

1. *$\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module, and*
2. *$\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic if and only if ℓ divides $q^m - 1$.*

If ℓ is a large prime number, then most likely $\ell \nmid 4\tau$, and Theorem 6 applies. In the special case $\ell \mid 4\tau$ we get the following result.

Theorem 7. *Let notation be as in Theorem 6. Furthermore, let ω_m be a q^m-Weil number of $\mathfrak{J}_C$ (cf. definition 4), and assume that ℓ is unramified in $K = \mathbb{Q}(\omega_m)$. Now assume that $\ell \mid 4\tau$. Then the following holds.*

1. *If $\omega_m \in \mathbb{Z}$, then $\ell \mid q^m - 1$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^m})$.*
2. *If $\omega_m \notin \mathbb{Z}$, then $\ell \nmid q^m - 1$, $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{mk}})$ if and only if $\ell \mid q^{mk} - 1$.*

By Theorem 6 and 7 we get the following corollary.

Corollary 10. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathfrak{J}_C$, and with $\ell \nmid q$. Let q be of multiplicative order k modulo ℓ. If $\ell \nmid q-1$, then the Weil-pairing is non-degenerate on $\mathfrak{J}_C(\mathbb{F}_{q^k})[\ell] \times \mathfrak{J}_C(\mathbb{F}_{q^k})[\ell]$.*

For the 2-torsion part, we prove the following theorem.

Theorem 11. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$ of odd characteristic. Let*

$$P_m(X) = X^4 + sX^3 + tX^2 + sq^m X + q^{2m}$$

be the characteristic polynomial of the q^m-power Frobenius endomorphism of the Jacobian $\mathfrak{J}_C$. Assume $|\mathfrak{J}_C(\mathbb{F}_{q^m})|$ is even. Then

$$\mathfrak{J}_C[2] \subseteq \begin{cases} \mathfrak{J}_C(\mathbb{F}_{q^{4m}}), & \text{if } s \text{ is even;} \\ \mathfrak{J}_C(\mathbb{F}_{q^{6m}}), & \text{if } s \text{ is odd.} \end{cases}$$

Now consider a supersingular genus two curve C defined over $\mathbb{F}_q$; cf. section 6. Again, let ℓ be a prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian and let k be the multiplicative order of q modulo ℓ. We know that $k \leq 12$, cf. Galbraith [5] and Rubin and Silverberg [18]. If $\ell^2 \nmid |\mathfrak{J}_C(\mathbb{F}_q)|$, then in many cases $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$, cf. Stichtenoth [21]. Zhu [23] gives a complete description of the subgroup of $\mathbb{F}_q$-rational points on the Jacobian. Using Theorem 6 we get the following explicit description of the ℓ-torsion subgroup of the Jacobian of a supersingular genus two curve.

Theorem 14. *Consider a supersingular genus two curve C defined over $\mathbb{F}_q$. Let ℓ be a prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, and with $\ell \nmid q$. Depending on the cases in table 1 we get the following properties of $\mathcal{J}_C$.*

Case I: $-q^2 \equiv q^4 \equiv 1 \pmod{\ell}$ *and* $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^4})$. *If* $\ell \neq 2$, *then* $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ *is cyclic.*

Case II: $q^3 \equiv 1 \pmod{\ell}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^6})$ *and* $\mathcal{J}_C(\mathbb{F}_q)$ *is cyclic. If* $\ell \neq 3$, *then* $q \not\equiv 1 \pmod{\ell}$.

Case III: $-q^3 \equiv q^6 \equiv 1 \pmod{\ell}$ *and* $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^6})$. *If* $\ell \neq 3$, *then* $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ *is cyclic.*

Case IV: $q \not\equiv q^5 \equiv 1 \pmod{\ell}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{10}})$ *and* $\mathcal{J}_C(\mathbb{F}_q)$ *is cyclic.*

Case V: $q \not\equiv q^5 \equiv 1 \pmod{\ell}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{10}})$ *and* $\mathcal{J}_C(\mathbb{F}_q)$ *is cyclic.*

Case VI: $-q^6 \equiv q^{12} \equiv 1 \pmod{\ell}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{24}})$ *and* $\mathcal{J}_C(\mathbb{F}_q)$ *is cyclic.*

Case VII: $q \equiv 1 \pmod{\ell}$ *and* $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^2})$. *If* $\ell \neq 2$, *then* $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*

Case VIII: $-q \equiv q^2 \equiv 1 \pmod{\ell}$ *and* $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^2})$. *If* $\ell \neq 2$, *then* $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*

Case IX: *If* $\ell \neq 3$, *then* $q \not\equiv q^3 \equiv 1 \pmod{\ell}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^3})$ *and* $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*

In particular, it follows from Theorem 14 that if $\ell > 3$, then the ℓ-torsion points on the Jacobian $\mathcal{J}_C$ of a supersingular genus two curve defined over $\mathbb{F}_q$ are rational over a field extension of $\mathbb{F}_q$ of degree at most 24, and $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module.

Assumption. In this paper, a *curve* is an irreducible nonsingular projective variety of dimension one.

2. Genus two curves

A hyperelliptic curve is a projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. It is well known, that any genus two curve is hyperelliptic. Throughout this paper, let C be a curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p. By the Riemann-Roch Theorem there exists a birational map $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

$$y^2 + g(x)y = h(x),$$

where $g, h \in \mathbb{F}_q[x]$ are of degree $\deg(g) \leq 3$ and $\deg(h) \leq 6$; cf. [3, chapter 1].

The set of principal divisors $\mathcal{P}(C)$ on C constitutes a subgroup of the degree zero divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

$$\mathcal{J}_C = \mathrm{Div}_0(C)/\mathcal{P}(C).$$

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_C[\ell^n] \subseteq \mathcal{J}_C$ of points of order dividing ℓ^n is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank four, i.e.

$$\mathcal{J}_C[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z};$$

cf. [12, Theorem 6, p. 109].

The multiplicative order k of q modulo ℓ plays an important role in cryptography, since the (reduced) Tate-pairing is non-degenerate over $\mathbb{F}_{q^k}$; cf. [8].

Definition 1 (Embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. The embedding degree of $\mathcal{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number k, such that $q^k \equiv 1 \pmod{\ell}$.

Closely related to the embedding degree, we have the *full* embedding degree.

Definition 2 (Full embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. The full embedding degree of $\mathcal{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number $\varkappa$, such that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\varkappa})$.

Remark 3. If $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\varkappa})$, then $\ell \mid q^\varkappa - 1$; cf. [4, Corollary 5.77, p. 111]. Hence, the full embedding degree is a multiple of the embedding degree.

A priori, the Weil-pairing is only non-degenerate over $\mathbb{F}_{q^\varkappa}$. But in fact, as we shall see, the Weil-pairing is also non-degenerate over $\mathbb{F}_{q^k}$.

3. The Weil- and the Tate-pairing

Let $\mathbb{F}$ be an algebraic extension of $\mathbb{F}_q$. Let $x \in \mathcal{J}_C(\mathbb{F})[\ell]$ and $y = \sum_i a_i P_i \in \mathcal{J}_C(\mathbb{F})$ be divisors with disjoint supports, and let $\bar{y} \in \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F})$ denote the divisor class containing the divisor y. Furthermore, let $f_x \in \mathbb{F}(C)$ be a rational function on C with divisor $\mathrm{div}(f_x) = \ell x$. Set $f_x(y) = \prod_i f(P_i)^{a_i}$. Then $e_\ell(x, \bar{y}) = f_x(y)$ is a well-defined pairing

$$e_\ell : \mathcal{J}_C(\mathbb{F})[\ell] \times \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F}) \longrightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^\ell,$$

it is called the *Tate-pairing*; cf. [6]. Raising the result to the power $\frac{|\mathbb{F}^\times|}{\ell}$ gives a well-defined element in the subgroup $\mu_\ell \subseteq \bar{\mathbb{F}}$ of the ℓ^{th} roots of unity. This pairing

$$\hat{e}_\ell : \mathcal{J}_C(\mathbb{F})[\ell] \times \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F}) \longrightarrow \mu_\ell$$

is called the *reduced* Tate-pairing. If the field $\mathbb{F}$ is finite and contains the ℓ^{th} roots of unity, then the Tate-pairing is bilinear and non-degenerate; cf. [8].

Now let $x, y \in \mathcal{J}_C[\ell]$ be divisors with disjoint support. The Weil-pairing

$$e_\ell : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell$$

is then defined by $e_\ell(x, y) = \frac{\hat{e}_\ell(x,\bar{y})}{\hat{e}_\ell(y,\bar{x})}$. The Weil-pairing is bilinear, anti-symmetric and non-degenerate on $\mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell]$; cf. [15].

4. Matrix representation of the endomorphism ring

An endomorphism $\psi : \mathcal{J}_C \to \mathcal{J}_C$ induces a linear map $\bar{\psi} : \mathcal{J}_C[\ell] \to \mathcal{J}_C[\ell]$ by restriction. Hence, ψ is represented by a matrix $M \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ on $\mathcal{J}_C[\ell]$. Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ (see [12, pp. 109–110]), and let $\bar{f} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of $\bar{\psi}$. Then f is a monic polynomial of degree four, and by [12, Theorem 3, p. 186],

$$f(X) \equiv \bar{f}(X) \pmod{\ell}.$$

Since C is defined over $\mathbb{F}_q$, the mapping $(x, y) \mapsto (x^q, y^q)$ is a morphism on C. This morphism induces the q-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. Let $P(X)$ be the characteristic polynomial of φ. $P(X)$ is called the *Weil polynomial* of $\mathcal{J}_C$, and

$$|\mathcal{J}_C(\mathbb{F}_q)| = P(1)$$

by the definition of $P(X)$ (see [12, pp. 109–110]); i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$.

Definition 4 (Weil number)**.** Let notation be as above. Let $P_m(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on $\mathcal{J}_C$. Consider a number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$. If $P_m(X)$ is reducible, assume furthermore that ω_m and φ_m are roots of the same irreducible factor of $P_m(X)$. We identify φ_m with ω_m, and we call ω_m a q^m*-Weil number* of $\mathcal{J}_C$.

Remark 5. A q^m-Weil number is not necessarily uniquely determined. In general, $P_m(X)$ is irreducible, in which case $\mathcal{J}_C$ has four q^m-Weil numbers.

Assume $P_m(X)$ is reducible. Write $P_m(X) = f(X)g(X)$, where $f, g \in \mathbb{Z}[X]$ are of degree at least one. Since $P_m(\varphi_m) = 0$, either $f(\varphi_m) = 0$ or $g(\varphi_m) = 0$; if not, then either $f(\varphi_m)$ or $g(\varphi_m)$ has infinite kernel, i.e. is not an endomorphism of $\mathcal{J}_C$. So a q^m-Weil number is well-defined.

5. Non-cyclic torsion

Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let $P_m(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m of the Jacobian $\mathcal{J}_C$. $P_m(X)$ is of the form $P_m(X) = X^4 + sX^3 + tX^2 + sq^m X + q^{2m}$, where $s, t \in \mathbb{Z}$. Let $\sigma = \frac{s}{2}$ and $\tau = 2q^m + \sigma^2 - t$. Then

$$P_m(X) = X^4 + 2\sigma X^3 + (2q^m + \sigma^2 - \tau)X^2 + 2\sigma q^m X + q^{2m},$$

and $2\sigma, 4\tau \in \mathbb{Z}$.

Theorem 6. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism of the Jacobian $\mathcal{J}_C$ as*

$$P_m(X) = X^4 + 2\sigma X^3 + (2q^m + \sigma^2 - \tau)X^2 + 2\sigma q^m X + q^{2m},$$

where $2\sigma, 4\tau \in \mathbb{Z}$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, and with $\ell \nmid q$ and $\ell \nmid q - 1$. If $\ell \nmid 4\tau$, then

(1) *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module, and*
(2) *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic if and only if ℓ divides $q^m - 1$.*

Proof. Let $\bar{P}_m \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ_m to $\mathcal{J}_C[\ell]$. Since ℓ divides $|\mathcal{J}_C(\mathbb{F}_q)|$, 1 is a root of $\bar{P}_m$. Assume that 1 is a root of $\bar{P}_m$ of multiplicity ν. Since the roots of $\bar{P}_m$ occur in pairs $(\alpha, q^m/\alpha)$, also q^m is a root of $\bar{P}_m$ of multiplicity ν.

If $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank three as a $\mathbb{Z}/\ell\mathbb{Z}$-module, then ℓ divides $q^m - 1$ by [4, Proposition 5.78, p. 111]. Choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$. With respect to $\mathcal{B}$, φ_m is represented by a matrix of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \\ 0 & 0 & 0 & m_4 \end{bmatrix}.$$

Now, $m_4 = \det M \equiv \deg \varphi_m = q^{2m} \equiv 1 \pmod{\ell}$. Hence, $\bar{P}_m(X) = (X-1)^4$. By comparison of coefficients it follows that $4\tau \equiv 0 \pmod{\ell}$, and we have a contradiction. So $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module.

Now assume that $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic. If $q^m \not\equiv 1 \pmod{\ell}$, then 1 is a root of $\bar{P}_m$ of multiplicity two, i.e. $\bar{P}_m(X) = (X-1)^2(X-q^m)^2$. But then it follows by comparison of coefficients that $4\tau \equiv 0 \pmod{\ell}$, and we have a contradiction. So $q^m \equiv 1 \pmod{\ell}$, i.e. ℓ divides $q^m - 1$. On the other hand, if ℓ divides $q^m - 1$, then the Tate-pairing is non-degenerate on $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$, i.e. $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ must be of rank at least two as a $\mathbb{Z}/\ell\mathbb{Z}$-module. So $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic. □

If ℓ is a large prime number, then most likely $\ell \nmid 4\tau$, and Theorem 6 applies. In the special case $\ell \mid 4\tau$ we get the following result.

Theorem 7. *Let notation be as in Theorem 6. Furthermore, let ω_m be a q^m-Weil number of $\mathfrak{J}_C$, and assume that ℓ is unramified in $K = \mathbb{Q}(\omega_m)$. Now assume that $\ell \mid 4\tau$. Then the following holds.*

1. *If $\omega_m \in \mathbb{Z}$, then $\ell \mid q^m - 1$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^m})$.*
2. *If $\omega_m \notin \mathbb{Z}$, then $\ell \nmid q^m - 1$, $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{mk}})$ if and only if $\ell \mid q^{mk} - 1$.*

Remark 8. A prime number ℓ is unramified in K if and only if ℓ divides the discriminant of the field extension $K/\mathbb{Q}$; see e.g. [16, Theorem 2.6, p. 199]. Hence, almost any prime number ℓ is unramified in K. In particular, if ℓ is large, then ℓ is unramified in K.

The special case of Theorem 7 *does* occur; cf. the following example 9.

Example 9. Consider the polynomial $P(X) = (X^2+X+3)^2 \in \mathbb{Q}[X]$. By [13] and [9] it follows that $P(X)$ is the Weil polynomial of the Jacobian of a genus two curve C defined over $\mathbb{F}_3$. The number of $\mathbb{F}_3$-rational points on the Jacobian is $P(1) = 25$, so $\ell = 5$ is an odd prime divisor of $|\mathfrak{J}_C(\mathbb{F}_3)|$ not dividing $q = p = 3$. Notice that $P(X) \equiv X^4 + 2\sigma X^3 + (2p+\sigma^2)X^2 + 2\sigma p X + p \pmod{\ell}$ with $\sigma = 1$. The complex roots of $P(X)$ are given by $\omega = \frac{-1+\sqrt{-11}}{2}$ and $\bar{\omega}$, and ℓ is unramified in $K = \mathbb{Q}(\omega)$. Since 3 is a generator of $(\mathbb{Z}/5\mathbb{Z})^\times$, it follows by Theorem 7 that $\mathfrak{J}_C(\mathbb{F}_3) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{81})$.

By Theorem 6 and 7 we get the following corollary.

Corollary 10. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathfrak{J}_C$, and with $\ell \nmid q$. Let q be of multiplicative order k modulo ℓ. If $\ell \nmid q-1$, then the Weil-pairing is non-degenerate on $\mathfrak{J}_C(\mathbb{F}_{q^k})[\ell] \times \mathfrak{J}_C(\mathbb{F}_{q^k})[\ell]$.*

Proof. Let

$$P_k(X) = X^4 + 2\sigma X^3 + (2q^k + \sigma^2 - \tau)X^2 + 2\sigma q^k X + q^{2k}$$

be the characteristic polynomial of the q^k-power endomorphism on the Jacobian $\mathfrak{J}_C$. If $\ell \mid 4\tau$, then $\mathfrak{J}_C[\ell] = \mathfrak{J}_C(\mathbb{F}_{q^k})[\ell]$ by Theorem 7, and the corollary follows.

Assume $\ell \nmid 4\tau$. Let $U = \mathfrak{J}_C(\mathbb{F}_q)[\ell]$ and $V = \ker(\varphi - q) \cap \mathfrak{J}_C[\ell]$, where φ is the q-power Frobenius endomorphism on $\mathfrak{J}_C$. Then the Weil-pairing e_W is non-degenerate on $U \times V$ by [19]. By Theorem 6, we know that $V = \mathfrak{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathfrak{J}_C(\mathbb{F}_q)[\ell]$ and that

$$\mathfrak{J}_C(\mathbb{F}_{q^k})[\ell] \simeq U \oplus V \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

Now let $x \in \mathfrak{J}_C(\mathbb{F}_{q^k})[\ell]$ be an arbitrary $\mathbb{F}_{q^k}$-rational point of order ℓ. Write $x = x_U + x_V$, where $x_U \in U$ and $x_V \in V$. Choose $y \in V$ and $z \in U$, such that $e_W(x_U, y) \neq 1$ and $e_W(x_V, z) \neq 1$. We may assume that $e_W(x_U, y)e_W(x_V, z) \neq 1$; if not, replace z with $2z$. Since the Weil-pairing is anti-symmetric, $e_W(x_U, z) = e_W(x_V, y) = 1$. Hence,

$$e_W(x, y+z) = e_W(x_U, y)e_W(x_V, z) \neq 1.$$

□

Proof of Theorem 7. We see that

$$P_m(X) \equiv (X^2 + \sigma X + q^m)^2 \pmod{\ell};$$

since $P_m(1) \equiv 0 \pmod{\ell}$, it follows that

$$P_m(X) \equiv (X-1)^2(X-q^m)^2 \pmod{\ell}.$$

Assume at first that $P_m(X)$ is irreducible in $\mathbb{Q}[X]$. Let $\mathfrak{O}_K$ denote the ring of integers of K. By [16, Proposition 8.3, p. 47], it follows that $\ell\mathfrak{O}_K = \mathfrak{L}_1^2\mathfrak{L}_2^2$, where $\mathfrak{L}_1 = (\ell, \omega_m - 1)\mathfrak{O}_K$ and $\mathfrak{L}_2 = (\ell, \omega_m - q)\mathfrak{O}_K$. In particular, ℓ ramifies in K, and we have a contradiction. So $P_m(X)$ is reducible in $\mathbb{Q}[X]$.

Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of ω_m. If $\deg f = 3$, then it follows as above that ℓ ramifies in K. So $\deg f < 3$. Assume that $\deg f = 1$, i.e. that $\omega_m \in \mathbb{Z}$. Since $\omega_m^2 = q^m$, we know that $\omega_m = \pm q^{m/2}$. So $f(X) = X \mp q^{m/2}$. Since $f(X)$ divides $P(X)$ in $\mathbb{Z}[X]$, either $f(X) \equiv X - 1 \pmod{\ell}$ or $f(X) \equiv X - q^m \pmod{\ell}$. It follows that $q^m \equiv 1 \pmod{\ell}$. Thus, $\omega_m \equiv \pm 1 \pmod{\ell}$. If $\omega_m \equiv -1 \pmod{\ell}$, then φ_m does not fix $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$. This is a contradiction. Hence, $\omega_m \equiv 1 \pmod{\ell}$. But then φ_m is the identity on $\mathfrak{J}_C[\ell]$. Thus, if $\omega_m \in \mathbb{Z}$, then $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^m})$.

Assume $\omega_m \notin \mathbb{Z}$. Then $\deg f = 2$. Since $f(X)$ divides $P(X)$ in $\mathbb{Z}[X]$, it follows that

$$f(X) \equiv (X-1)(X-q^m) \pmod{\ell};$$

to see this, we merely notice that if $f(X)$ is equivalent to the square of a polynomial modulo ℓ, then ℓ ramifies in K. Notice also that if $q^m \equiv 1 \pmod{\ell}$, then ℓ ramifies in K. So $q^m \not\equiv 1 \pmod{\ell}$.

Now let $U = \ker(\varphi_m - 1)^2 \cap \mathfrak{J}_C[\ell]$ and $V = \ker(\varphi_m - q^m)^2 \cap \mathfrak{J}_C[\ell]$. Then U and V are φ_m-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathfrak{J}_C[\ell]$ of rank two, and $\mathfrak{J}_C[\ell] \simeq U \oplus V$. Now choose $x_1 \in U$, such that $\varphi_m(x_1) = x_1$, and expand this to a basis (x_1, x_2) of U. Similarly, choose a basis (x_3, x_4) of V with $\varphi_m(x_3) = qx_3$. With respect to the basis (x_1, x_2, x_3, x_4), φ_m is represented by a matrix of the form

$$M = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q^m & \beta \\ 0 & 0 & 0 & q^m \end{bmatrix}.$$

Let q^m be of multiplicative order k modulo ℓ. Notice that

$$M^k = \begin{bmatrix} 1 & k\alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & kq^{m(k-1)}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Hence, the restriction of φ_m^k to $\mathfrak{J}_C[\ell]$ has the characteristic polynomial $(X-1)^4$. Let $P_{mk}(X)$ be the characteristic polynomial of the q^{mk}-power Frobenius endomorphism $\varphi_{mk} = \varphi_m^k$ of the Jacobian $\mathfrak{J}_C$. Then

$$P_{mk}(X) \equiv (X-1)^4 \pmod{\ell}.$$

Since ω_m is a q^m-Weil number of $\mathfrak{J}_C$, we know that ω_m^k is a q^{mk}-Weil number of $\mathfrak{J}_C$. Assume $\omega_m^k \notin \mathbb{Q}$. Then $K = \mathbb{Q}(\omega_m^k)$. Let $h \in \mathbb{Z}[X]$ be the minimal polynomial of ω_m^k. Then it follows that $h(X) \equiv (X-1)^2 \pmod{\ell}$, and ℓ ramifies in K. So $\omega_m^k \in \mathbb{Q}$, i.e. h is of degree one. But then $h(X) \equiv X - 1 \pmod{\ell}$, i.e. $\omega_m^k \equiv 1 \pmod{\ell}$. So φ_m^k is the identity map on $\mathfrak{J}_C[\ell]$. Hence, $M^k = I$, i.e. $\alpha \equiv \beta \equiv 0 \pmod{\ell}$. Thus, φ_m is represented by a diagonal matrix $\operatorname{diag}(1, 1, q^m, q^m)$ with respect to (x_1, x_2, x_3, x_4). The theorem follows. □

For the 2-torsion part, we get the following theorem.

Theorem 11. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$ of odd characteristic. Let $P_m(X) = X^4 + sX^3 + tX^2 + sq^mX + q^{2m}$ be the characteristic polynomial of the q^m-power Frobenius endomorphism of the Jacobian $\mathfrak{J}_C$. Assume $|\mathfrak{J}_C(\mathbb{F}_{q^m})|$ is even. Then*

$$\mathfrak{J}_C[2] \subseteq \begin{cases} \mathfrak{J}_C(\mathbb{F}_{q^{4m}}), & \text{if } s \text{ is even;} \\ \mathfrak{J}_C(\mathbb{F}_{q^{6m}}), & \text{if } s \text{ is odd.} \end{cases}$$

Proof. Since q is odd,

$$P_m(X) \equiv X^4 + sX^3 + tX^2 + sX + 1 \pmod{2}.$$

Assume at first that s is even. Since $P_m(1)$ is even, it follows that t is even; but then

$$P_m(X) \equiv (X-1)^4 \equiv X^4 - 1 \pmod{2}.$$

Hence, $\mathfrak{J}_C[2] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{4m}})$ in this case.

Now assume that s is odd. Again t must be even; but then

$$P_m(X) \equiv (X^2-1)(X^2+X+1) \pmod{2}.$$

Since $f(X) = X^2 + X + 1$ has the complex roots $\xi = -\frac{1}{2}(1 \pm i\sqrt{3})$, and $\xi^3 = 1$, it follows that $\mathfrak{J}_C[2] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{6m}})$ in this case. □

6. Supersingular curves

Consider a genus two curve C defined over a finite field $\mathbb{F}_q$ of characteristic p. C is called *supersingular*, if $\mathfrak{J}_C$ has no p-torsion. From [13] we have the following theorem.

Theorem 12. *Consider a polynomial $f \in \mathbb{Z}[X]$ of the form*

$$f(X) = f_{s,t}(X) = X^4 + sX^3 + tX^2 + sqX + q^2,$$

where $q = p^a$. If f is the Weil polynomial of the Jacobian of a supersingular genus two curve defined over the finite field $\mathbb{F}_q$, then (s,t) belongs to table 1.

Remark 13. By [9], in each of the cases in table 1 we can find a q such that $f_{s,t}(X)$ is the Weil polynomial of the Jacobian of a supersingular genus two curve defined over $\mathbb{F}_q$.

TABLE 1. Conditions for $f = X^4 + sX^3 + tX^2 + sqX + q^2$ to be the Weil polynomial of the Jacobian of a supersingular genus two curve defined over $\mathbb{F}_q$, where $q = p^a$.

Case	(s,t)	Condition
I	$(0,0)$	a odd, $p \neq 2$, or a even, $p \not\equiv 1 \pmod 8$.
II	$(0,q)$	a odd.
III	$(0,-q)$	a odd, $p \neq 3$, or a even, $p \not\equiv 1 \pmod{12}$.
IV	$(\pm\sqrt{q}, q)$	a even, $p \not\equiv 1 \pmod 5$.
V	$(\pm\sqrt{5q}, 3q)$	a odd, $p = 5$.
VI	$(\pm\sqrt{2q}, q)$,	a odd, $p = 2$.
VII	$(0,-2q)$	a odd.
VIII	$(0,2q)$	a even, $p \equiv 1 \pmod 4$.
IX	$(\pm 2\sqrt{q}, 3q)$	a even, $p \equiv 1 \pmod 3$.

Using Theorem 6, 7 and 12 we get the following explicit description of the ℓ-torsion subgroup of the Jacobian of a supersingular genus two curve.

Theorem 14. *Consider a supersingular genus two curve C defined over $\mathbb{F}_q$. Let ℓ be a prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathfrak{J}_C$, and with $\ell \nmid q$. Depending on the cases in table 1 we get the following properties of $\mathfrak{J}_C$.*

- **Case I:** $-q^2 \equiv q^4 \equiv 1 \pmod \ell$ *and* $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^4})$. *If* $\ell \neq 2$, *then* $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ *is cyclic.*
- **Case II:** $q^3 \equiv 1 \pmod \ell$, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^6})$ *and* $\mathfrak{J}_C(\mathbb{F}_q)$ *is cyclic. If* $\ell \neq 3$, *then* $q \not\equiv 1 \pmod \ell$.
- **Case III:** $-q^3 \equiv q^6 \equiv 1 \pmod \ell$ *and* $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^6})$. *If* $\ell \neq 3$, *then* $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ *is cyclic.*
- **Case IV:** $q \not\equiv q^5 \equiv 1 \pmod \ell$, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{10}})$ *and* $\mathfrak{J}_C(\mathbb{F}_q)$ *is cyclic.*
- **Case V:** $q \not\equiv q^5 \equiv 1 \pmod \ell$, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{10}})$ *and* $\mathfrak{J}_C(\mathbb{F}_q)$ *is cyclic.*
- **Case VI:** $-q^6 \equiv q^{12} \equiv 1 \pmod \ell$, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{24}})$ *and* $\mathfrak{J}_C(\mathbb{F}_q)$ *is cyclic.*
- **Case VII:** $q \equiv 1 \pmod \ell$ *and* $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^2})$. *If* $\ell \neq 2$, *then* $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*
- **Case VIII:** $-q \equiv q^2 \equiv 1 \pmod \ell$ *and* $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^2})$. *If* $\ell \neq 2$, *then* $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*
- **Case IX:** *If* $\ell \neq 3$, *then* $q \not\equiv q^3 \equiv 1 \pmod \ell$, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^3})$ *and* $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ *is bicyclic.*

Corollary 15. *If $\ell > 3$, then the full embedding degree with respect to ℓ of the Jacobian $\mathfrak{J}_C$ of a supersingular genus two curve defined over $\mathbb{F}_q$ is at most 24, and $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module.*

Proof of Theorem 14. In the following we consider each case in table 1 separately. Throughout this proof, assume that

$$f(X) = X^4 + sX^3 + tX^2 + sqX + q^2$$

is the Weil polynomial of the Jacobian $\mathfrak{J}_C$ of some supersingular genus two curve C defined over the finite field $\mathbb{F}_q$ of characteristic p, and let ℓ be a prime number dividing $f(1)$.

The case $s = 0$. First consider the cases I, II, III, VII and VIII of table 1.

Case I. If $(s, t) = (0, 0)$, then $f(1) = 1 + q^2 \equiv 0 \pmod{\ell}$, i.e. $q^2 \equiv -1 \pmod{\ell}$. So $f(X) \equiv X^4 - 1 \pmod{\ell}$, $q^4 \equiv 1 \pmod{\ell}$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^4})$. $\tau = 2q$ in Theorem 6, so if $\ell \neq 2$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic.

Case II. If $(s, t) = (0, q)$, then the roots of f modulo ℓ are given by ± 1 and $\pm q$. Since $f(1) = q^2 + q + 1 \equiv 0 \pmod{\ell}$, we know that $q \equiv \frac{1}{2}(-1 \pm \sqrt{-3}) \pmod{\ell}$. It follows that $q^3 \equiv 1 \pmod{\ell}$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^6})$. If $\ell = 2$, then $p \neq 2$, and $f(1)$ is odd. So $\ell \neq 2$. $\tau = q$ in Theorem 6, so $\mathcal{J}_C(\mathbb{F}_q)$ is cyclic.

Case III. If $(s, t) = (0, -q)$, then the roots of f modulo ℓ are given by ± 1 and $\pm q$. Since $f(1) = q^2 - q + 1 \equiv 0 \pmod{\ell}$, we know that $q \equiv \frac{1}{2}(1 \pm \sqrt{-3}) \pmod{\ell}$. It follows that $q^6 \equiv 1 \pmod{\ell}$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^6})$. As in case II, $\ell \neq 2$. Now $\tau = 3q$, so if $\ell \neq 3$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic.

Case VII. If $(s, t) = (0, -2q)$, then $q \equiv 1 \pmod{\ell}$ and $f(X) = (X^2 - q)^2$. Since q is an odd power of p, $X^2 - q$ is irreducible over $\mathbb{Q}$. So by [22, Theorem 2], $\mathcal{J}_C \simeq E \times E$ for some supersingular elliptic curve E. It follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^2})$. $\tau = 4q$, so if $\ell \neq 2$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bicyclic.

Case VIII. If $(s, t) = (0, 2q)$, then $q \equiv -1 \pmod{\ell}$ and $f(X) = (X^2 + q)^2$. Since $X^2 + q$ is irreducible over $\mathbb{Q}$, it follows that $\mathcal{J}_C \simeq E \times E$ for some supersingular elliptic curve E. So $q^2 \equiv 1 \pmod{\ell}$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^2})$. $\tau = 0$ and $\omega = i\sqrt{q}$ is a q-Weil number of $\mathcal{J}_C$. Since q is an even power of p, $K = \mathbb{Q}(\omega) = \mathbb{Q}(i)$ is of discriminant $d_K = -4$. Hence, if $\ell \neq 2$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bicyclic by Theorem 7.

Case IV–VI. Now we consider the cases IV, V and VI of table 1.

Case IV. If $(s, t) = (\sqrt{q}, q)$, then $4\tau = 5q$ in Theorem 6. Since $f(1)$ is odd, we know that $\ell \neq 2$. If ℓ divides 4τ, then $\ell = 5$; $\ell \nmid q$, since C is supersingular. But then $f(1) = q^2 + q\sqrt{q} + q + \sqrt{q} + 1 \equiv 0 \pmod{5}$, i.e. $q \equiv 2 \pmod{5}$. Since a is even and 2 is not a quadratic residue modulo 5, this is impossible. So $\ell \nmid 4\tau$. If $q \equiv 1 \pmod{\ell}$, then $f(1) \equiv 5 \pmod{\ell}$, i.e. $\ell = 5$. But then ℓ divides 4τ, a contradiction. So $\mathcal{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 6. From $f(1) \equiv 0 \pmod{\ell}$ it follows that $q^5 \equiv 1 \pmod{\ell}$. Since the complex roots of f are of the form $\sqrt{q}\xi$, where ξ is a primitive 5^{th} root of unity, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{10}})$. The case $(s, t) = (-\sqrt{q}, q)$ follows similarly.

Case V. If $(s, t) = (\sqrt{5q}, 3q)$ and $p = 5$, then 4τ is a power of 5 in Theorem 6. Since $f(1)$ is odd, we know that $\ell \neq 2$. If ℓ divides 4τ, then $\ell = 5$. Since C is supersingular and defined over a field of characteristic $p = 5$, this is a contradiction. So $\ell \nmid 4\tau$. If $q \equiv 1 \pmod{\ell}$, then $f(1) \equiv 5 + 2\sqrt{5} \equiv 0 \pmod{\ell}$, and it follows that $\ell = 5$. So $\mathcal{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 6. From $f(1) \equiv 0 \pmod{\ell}$ it follows that $q^5 \equiv 1 \pmod{\ell}$. Since the complex roots of f are of the form $\sqrt{q}\xi$, where ξ is a primitive 10^{th} root of unity, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{10}})$. The case $(s, t) = (-\sqrt{5q}, 3q)$ follows similarly.

Case VI. If $(s,t)=(\sqrt{2q},q)$ and $p=2$, then $4\tau=3\cdot 2^a$ for some number $a\in\mathbb{N}$. Hence, if ℓ divides 4τ, then $\ell=3$. But $3\nmid f(1)$; thus, $\ell\nmid 4\tau$. If $q\equiv 1 \pmod{\ell}$, then $f(1)\equiv 3+2\sqrt{2}\equiv 0 \pmod{\ell}$, and it follows that $\ell=1$. So $\mathcal{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 6. From $f(1)\equiv 0 \pmod{\ell}$ it follows that $q^6\equiv -1 \pmod{\ell}$. Since the complex roots of f are of the form $\sqrt{q}\xi$, where ξ is a primitive 24^{th} root of unity, it follows that $\mathcal{J}_C[\ell]\subseteq \mathcal{J}_C(\mathbb{F}_{q^{24}})$. The case $(s,t)=(-\sqrt{2q},q)$ follows similarly.

Case IX. Finally, consider the case IX. Assume that $(s,t)=(-2\sqrt{q},3q)$. We see that $f(X)=g(X)^2$, where $g(X)=X^2-\sqrt{q}X+q$. Since the complex roots of g are given by $\frac{1}{2}(1\pm\sqrt{-3})\sqrt{q}$, g is irreducible over $\mathbb{Q}$. So by [22, Theorem 2], $\mathcal{J}_C\simeq E\times E$ for some supersingular elliptic curve E. Hence, either $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bicyclic or equals the full ℓ-torsion subgroup of $\mathcal{J}_C$.

Assume $\mathcal{J}_C(\mathbb{F}_q)[\ell]=\mathcal{J}_C[\ell]$. Then $q\equiv 1 \pmod{\ell}$, i.e. $\sqrt{q}\equiv\pm 1 \pmod{\ell}$. But then $f(1)\equiv 9\equiv 0 \pmod{\ell}$ or $f(1)\equiv 1\equiv 0 \pmod{\ell}$, i.e. $\ell=3$.

Since $f(1)=(1-\sqrt{q}+q)^2\equiv 0 \pmod{\ell}$, we know that $q\equiv \frac{1}{2}(-1\pm\sqrt{-3}) \pmod{\ell}$. So $q^3\equiv 1 \pmod{\ell}$. Since $\ell\neq 3$, it follows that $q\not\equiv 1 \pmod{\ell}$. Hence, $\mathcal{J}_C[\ell]\subseteq\mathcal{J}_C(\mathbb{F}_{q^3})$ by the non-degeneracy of the Tate-pairing.

The case $(s,t)=(2\sqrt{q},3q)$ follows similarly. $\square$

References

[1] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm. *J. Cryptology*, 11:141–145, 1998.

[2] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Computing*, 32(3):586–615, 2003.

[3] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

[4] G. Frey and T. Lange. Varieties over special fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pages 87–113. Chapman & Hall/CRC, 2006.

[5] S.D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology – Asiacrypt 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer, 2001.

[6] S.D. Galbraith. Pairings. In I.F. Blake, G. Seroussi, and N.P. Smart, editors, *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, pages 183–213. Cambridge University Press, 2005.

[7] S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing 2007*, Lecture Notes in Computer Science, pages 108–131. Springer, 2007.

[8] F. Hess. A note on the tate pairing of curves over finite fields. *Arch. Math.*, 82:28–32, 2004.

[9] E.W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields, 2007. Preprint, available at `http://arxiv.org`.

[10] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[11] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.

[12] S. Lang. *Abelian Varieties*. Interscience, 1959.

[13] D. Maisner and E. Nart with an appendix by Everett W. Howe. Abelian surfaces over finite fields as jacobians. *Experimental Mathematics*, 11(3):321–337, 2002.

[14] V.S. Miller. Short programs for functions on curves, 1986. Unpublished manuscript, available at `http://crypto.stanford.edu/miller/miller.pdf`.

[15] V.S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17:235–261, 2004.

[16] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[17] C.R. Ravnshøj. Non-cyclic subgroups of Jacobians of genus two curves with complex multiplication, 2007. Preprint presented at AGCT 11, available at `http://arxiv.org`. Submitted to *Proceedings of AGCT 11*.

[18] K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In M. Yung, editor, *CRYPTO 2002*, Lecture Notes in Computer Science, pages 336–353. Springer, 2002.

[19] K. Rubin and A. Silverberg. Using abelian varieties to improve pairing-based cryptography, 2007. Preprint, available at `http://www.math.uci.edu/~asilverb/bibliography/`.
[20] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.
[21] H. Stichtenoth and C. Xing. On the structure of the divisor class group of a class of curves over finite fields. *Arch. Math.*, 65:141–150, 1995.
[22] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.
[23] H.J. Zhu. Group structures of elementary supersingular abelian varieties over finite fields. *J. Number Theory*, 81:292–309, 2000.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C
E-mail address: `cr@imf.au.dk`