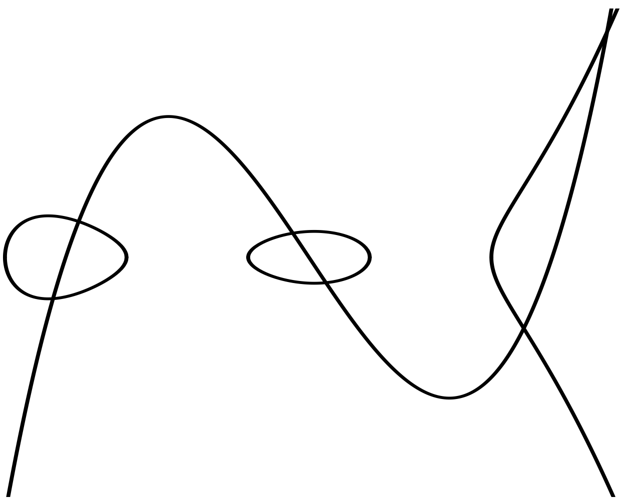
Aspects of Pairing Based Cryptography on Jacobians of

Genus Two Curves



PhD Thesis

Christian Robenhagen Ravnshøj

August 2008

Advisor: Johan Peder Hansen

Department of Mathematical Sciences

University of Aarhus

Introduction

The field of study

Koblitz (1987) 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 (1989) then proposed using Jacobians of hyperelliptic curves. After Boneh and Franklin (2001) proposed an identity based cryptosystem by using the Weil pairing on an elliptic curve, pairings have been of great interest to cryptography (see Galbraith, 2005). The next natural step was to consider pairings on Jacobians of hyperelliptic curves. Galbraith, Hess *et al.* (2007) survey the recent research on pairings on Jacobians of hyperelliptic curves. This thesis is on aspects of pairing based cryptography on Jacobians of genus two curves.

Consider the Jacobian $\mathcal{J}_C$ of a curve defined over a finite field $\mathbb{F}_q$. Let ℓ be a prime number dividing the number of rational points on $\mathcal{J}_C$, and let k be the multiplicative order of q modulo ℓ. The pairing in question is usually the Weil or the Tate pairing; both pairings can be computed with Miller's algorithm (Miller, 1986). The Tate pairing can be computed more efficiently than the Weil pairing (see Galbraith, 2001). The Tate pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ (see Hess, 2004) and the Weil pairing is non-degenerate on $\mathcal{J}_C[\ell]$ (see Silverman, 1986, Proposition 8.1, p. 96). 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 pairing based cryptography, the Weil pairing and the Tate pairing are non-degenerate over the same field. Let E be an elliptic curve defined over a finite field. Balasubramanian and Koblitz (1998) proved that if the group μ_ℓ of ℓ^{th} roots of unity 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 on E are rational over the same field extension. By Rubin and Silverberg (2007), this result also holds for Jacobians of genus two curves in the following sense: if μ_ℓ is not contained in the ground field, then the Weil pairing is non-degenerate on $U \times V$, where U is the rational ℓ-torsion subgroup and V is the p-eigenspace of the p-power Frobenius endomorphism of $\mathcal{J}_C$.

To use curves in (cryptographic) applications, we need a way to find the points on the curves. Miller (2004) uses the Weil pairing to find generators of the rational subgroup of an elliptic curve defined over a finite field $\mathbb{F}_q$. Frey and Rück (1994) claim that the non-degeneracy of the Tate pairing can be used to determine whether r random points of the rational m-torsion subgroup in fact is an independent set of generators of the rational m-torsion subgroup.

New results

The new results established and presented in this thesis are the following.

(a) A generalization of the result by Balasubramanian and Koblitz (1998) for elliptic curves to Jacobians of genus two curves (Theorem 2.1 and Theorem 2.2). This is the main result of the thesis.
(b) From this generalization it follows that if ℓ does not divide $q-1$, then the Weil pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \times \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ (Corollary 2.5).
(c) Moreover, we obtain an explicit description of the ℓ-torsion subgroup of the Jacobian of a supersingular genus two curve (Theorem 2.17). In particular, we see 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 (Corollary 2.18).

These results are presented in the preprint (Ravnshøj, 2008b).

(d) The q-power Frobenius endomorphism of $\mathcal{J}_C$ has either a diagonal representation on $\mathcal{J}_C[\ell]$ or a representation of a particular form (Theorem 2.11). The result is presented in the preprint (Ravnshøj, 2008c).
(e) If $2q^2$ divides the number of rational points on $\mathcal{J}_C$, then q is at most 16, and the Weil polynomial is on a very restricted list of polynomials (Theorem 2.19). The result is presented in the preprint (Ravnshøj, 2007c).
(f) A probabilistic algorithm to determine generators of $\mathcal{J}_C(\mathbb{F}_q)[m]$, where m is the largest divisor of the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, such that ℓ divides $q-1$ for every prime number ℓ dividing m (Algorithm 3.11). The result is presented in the preprint (Ravnshøj, 2007a).
(g) A probabilistic algorithm to determine generators of $\mathcal{J}_C[\ell]$, where ℓ does not divide $q-1$ (Algorithm 3.24). The algorithm is based on an explicit description of the representation of the q-power Frobenius endomorphism

and the Weil pairing on the ℓ-torsion subgroup $\mathcal{J}_C[\ell]$ (Theorem 2.11 and Theorem 3.19). The result is published in the paper (Ravnshøj, 2008c).

All of these results are established basically by using elementary methods from linear algebra and number theory.

The central idea is to consider the matrix representation of the q-power Frobenius endomorphism of the Jacobian on the ℓ-torsion subgroup. From this representation and the fact that the Weil polynomial $P(X)$ of the Jacobian is of a very specific form, we can deduce a lot of information about the Jacobian. The most important fact is that $P(X)$ and the characteristic polynomial of the representation of the Frobenius endomorphism on the ℓ-torsion subgroup are equivalent modulo ℓ. But also the fact that the number of rational points on the Jacobian is given by $P(1)$ is important; this reveals information on the coefficients of $P(X)$.

Another important idea is to use the non-degeneracy of the Weil pairing on the $\mathbb{F}_{q^k}$-rational ℓ-torsion subgroup $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Not only does this imply that $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is non-cyclic, if μ_ℓ is not contained in $\mathbb{F}_q$; also, it lets us determine if two $\mathbb{F}_{q^k}$-rational points are linearly dependent. In fact, we show that the Weil pairing can be used in this manner on the full ℓ-torsion subgroup, and not only on the $\mathbb{F}_{q^k}$-rational ℓ-torsion subgroup. This gives us a procedure to determine if four random ℓ-torsion points on the Jacobian generates the ℓ-torsion subgroup.

Structure of the thesis

The thesis is organized as follows.

Chapter 1 We define the objects of study: Jacobians of genus two curves. Basic definitions and facts about algebraic curves are recalled. Cryptographic protocols on Jacobians of curves are introduced; in particular, we introduce pairing based protocols. Finally, we recall the proof of the fact that any genus two curve is hyperelliptic and can be represented by a planar curve.

Chapter 2 In this chapter we establish and prove the new results (a)–(e) above on properties of Jacobians of genus two curves. The generalization of the result by Balasubramanian and Koblitz (1998) is the main result of the chapter. After proving the generalization, we treat the matrix representation of the Frobenius endomorphism and the supersingular case. The case where $2q^2$ divides the number of rational points on $\mathcal{J}_C$ is treated in the final section of the chapter.

Chapter 3 The algorithms (f) and (g) to determine generators of ℓ-torsion subgroups of the Jacobian of a genus two curve are established. The chapter is organized as follows. In the first section we recall some facts concerning finite abelian groups, and obtain an algorithm to choose an element of prime number order in a finite abelian group. In the second section we establish the algorithm (f), and in the last section we establish the algorithm (g).

Four appendices are included, containing the preprints by the author. To increase readability of the thesis, an index has been included after the bibliography.

Acknowledgements

The author wishes to thank his advisor Johan P. Hansen for his advice and encouragement. The author also wishes to thank the organizers of AGCT 11 for letting him present the preprint (Ravnshøj, 2008a) at the conference.

The research presented in the thesis is supported in part by a PhD grant from CRYPTOMAThIC.

Contents

Chapter 1

Jacobians of genus two curves

Since Jacobians of (genus two) curves naturally carry a group structure, they can be used in cryptographic applications. In particular, the existence of bilinear pairings on the Jacobians allows pairing based cryptography. The thesis is on aspects of pairing based cryptography on Jacobians of genus two curves.

In this chapter we define the objects we wish to study, that is Jacobians of genus two curves. Our intent is merely to present the properties that we need; thus facts will be stated but not proved. We will, though, prove the central results that any genus two curve is hyperelliptic and can be represented by a planar curve.

The chapter is organized as follows: In section 1.1 we recall basic definitions and facts about algebraic curves and fix the notation we will use throughout the thesis. In section 1.2 we recall how to construct cryptographic protocols on Jacobians of curves; in particular, we introduce pairing based protocols. Finally, in section 1.3 we define a hyperelliptic curve, and prove that any genus two curve is hyperelliptic and can be represented by a planar curve.

1.1 Algebraic curves

Throughout the thesis, a *curve* is an irreducible nonsingular projective variety of dimension one.

In the following, let C be curve of genus g defined over a field $\mathbb{F}$. Let $\bar{\mathbb{F}}$ denote the algebraic closure of $\mathbb{F}$. If $g > 1$, then we cannot define a group structure on the points on C. Instead, we consider the *divisor class group* of C.

1.1.1 The divisor class group

The divisor group $\mathrm{Div}(C)$ is the free, abelian group generated by the points on C; i.e. $\mathrm{Div}(C)$ is the set of formal sums

$$D = \sum_{P \in C(\bar{\mathbb{F}})} n_P (P)$$

of points on C, where $n_P = 0$ for all but a finite number of points $P \in C(\bar{\mathbb{F}})$. For a *divisor* $D = \sum_{P \in C(\bar{\mathbb{F}})} n_P(P)$, we define the *degree* of D by

$$\deg(D) = \sum_{P \in C(\bar{\mathbb{F}})} n_P \in \mathbb{Z},$$

and the *valuation* of D at P by $\nu_P(D) = n_P$. D is an *effective* divisor, if $\nu_P(D) \geq 0$ for all points $P \in C(\bar{\mathbb{F}})$. $\mathrm{Div}(C)$ is ordered by $D_1 > D_2$ if $D_1 - D_2$ is effective. The *support* of D is defined as

$$\mathrm{Supp}(D) = \{P \in C(\bar{\mathbb{F}}) | \, \nu_P(D) \neq 0\}.$$

Finally, let

$$\mathrm{Div}_0(C) = \{D \in \mathrm{Div}(C) | \deg D = 0\}$$

be the subgroup of degree zero divisors.

Denote the ring of polynomial functions $f : C \to \bar{\mathbb{F}}$ by $\bar{\mathbb{F}}[C]$, and let $\bar{\mathbb{F}}(C)$ denote the quotient field of $\bar{\mathbb{F}}[C]$. For every point $P \in C(\bar{\mathbb{F}})$ we define the ring

$$\mathcal{O}_P = \{g/h | g, h \in \bar{\mathbb{F}}[C], \; h(P) \neq 0\}.$$

$\mathcal{O}_P$ is a *local* ring, i.e. has a unique, maximal ideal $\mathfrak{m}_P$ (see Shafarevich, 1974, pp. 71–72). Since C is smooth, $\mathcal{O}_P$ is a principal ideal domain; this follows e.g. by (Shafarevich, 1974, Corollary 1, p. 75) and Nakayama's Lemma. A generator of $\mathfrak{m}_P$ is called a *local parameter* of C at P.

Let $f \in \bar{\mathbb{F}}(C)$ be a rational function. We define a valuation ν_P on $\bar{\mathbb{F}}(C)$ by

$$\nu_P(f) = n \iff f \in \mathfrak{m}_P^n \setminus \mathfrak{m}_P^{n+1},$$

if $f(P) = 0$, and $\nu_P(f) = -\nu_P(1/f)$ if $f(P) = \infty$. For $f(P) \notin \{0, \infty\}$, let $\nu_P(f) = 0$. If $\nu_P(f) = n > 0$, then we say that f has a *zero of order* n at P; if $n < 0$, then we say that f has a *pole of order* n at P.

The set of points on $C(\bar{\mathbb{F}})$ with $\nu_P(f) \neq 0$ is finite (see Shafarevich, 1974, p. 129). Thus we may associate a divisor $\mathrm{div}(f) = \sum_{P \in C(\bar{\mathbb{F}})} \nu_P(f)(P)$ to f. If a divisor $D \in \mathrm{Div}(C)$ is the divisor associated to a rational function, i.e. $D = \mathrm{div}(f)$ for some $f \in \bar{\mathbb{F}}(C)$, then D is called a *principal* divisor. The set of principal divisors on C is denoted $\mathrm{Prin}(C)$. A principal divisor is of degree zero (see Shafarevich, 1974, Theorem 1, p. 141). Hence, $\mathrm{Prin}(C)$ is a subgroup of the degree zero divisors $\mathrm{Div}_0(C)$.

1.1.2 Abelian varieties

A *group variety* is an algebraic variety G together with a group structure $\bullet$, such that the mappings

$$\begin{aligned} \iota : G \to G, &\quad g \mapsto g^{-1} \\ \kappa : G \times G \to G, &\quad (g, h) \mapsto g \bullet h \end{aligned}$$

are regular. Obviously, a group variety G is smooth: if $P \in G$ is a singular point, then *all* points on G are singular by translation of P. This is a contradiction.

Definition 1.1 (Abelian variety)**.** An abelian variety is a projective, irreducible group variety.

Example 1.2. An elliptic curve is the basic example of an abelian variety. Cf. section 1.2.1 on page 6.

An abelian variety is an abelian group (see Shafarevich, 1974, Theorem 3, p. 153). Thus we will write the group law additively. We denote the zero element by $\mathcal{O}$.

An *endomorphism* of an abelian variety A is a morphism $\phi : A \to A$, which is also a group homomorphism; i.e. $\phi(x + y) = \phi(x) + \phi(y)$ for any points $x, y \in A$. The set of endomorphisms on A constitutes a ring $\mathrm{End}(A)$ with composition as multiplicative structure and addition defined by

$$(\phi + \psi)(x) = \phi(x) + \psi(x).$$

The integers $\mathbb{Z}$ act on A in the obvious way, and the endomorphism of A induced by an integer $m \in \mathbb{Z}$ is denoted $[m]$.

Now, consider an abelian variety A defined over a field $\mathbb{F}$ and of dimension g. Let $\mathbb{F}$ be of characteristic $p > 0$. The *m-torsion subgroup* $A[m]$ of A is defined as the kernel of $[m]$,

$$A[m] = \ker[m] = \{P \in A | [m](P) = \mathcal{O}\}.$$

A point $P \in A[m]$ is called an *m-torsion point*. The m-torsion subgroup is a finite group, and if p does not divide m, then $A[m]$ is a $\mathbb{Z}/m\mathbb{Z}$-module of rank $2g$, i.e.

$$A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}. \tag{1.1}$$

(See Lang, 1959, Theorem 6, p. 109).

An endomorphism $\phi : A \to A$ induces a linear map $\bar{\phi} : A[m] \to A[m]$ by restriction. Hence, ϕ is represented by a matrix $M \in \mathrm{Mat}_{2g}(\mathbb{Z}/m\mathbb{Z})$ on $A[m]$.

If ϕ can be represented on $A[m]$ by a diagonal matrix with respect to an appropriate basis of $A[m]$, then we say that ϕ is *diagonalizable* or has a *diagonal representation* on $A[m]$.

Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ϕ (see Lang, 1959, pp. 109–110), and let $\bar{f} \in (\mathbb{Z}/m\mathbb{Z})[X]$ be the characteristic polynomial of $\bar{\phi}$. Then f is a monic polynomial of degree $2g$, and

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

(See Lang, 1959, Theorem 3, p. 186).

1.1.3 Jacobian varieties

Recall that C is a curve of genus g defined over a field $\mathbb{F}$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

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

The Jacobian is an abelian variety of dimension g, and the points on the Jacobian are divisor classes (see Lang, 1959, Theorem 8, p. 35).

Now, let $\mathbb{F} = \mathbb{F}_q$, the finite field of q elements. 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 $\mathcal{J}_C$ by

$$\varphi\left(\sum n_P(P)\right) = \sum n_P(\varphi(P)).$$

We say that a point $D \in \mathcal{J}_C$ is $\mathbb{F}_{q^m}$-rational, if $\varphi^m(D) = D$. The subgroup of $\mathbb{F}_{q^m}$-rational points on $\mathcal{J}_C$ is denoted $\mathcal{J}_C(\mathbb{F}_{q^m})$. This is a finite group, and

$$\mathcal{J}_C(\mathbb{F}_{q^m}) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_{2g}\mathbb{Z}, \tag{1.2}$$

where $n_i \mid n_{i+1}$ for $1 \leq i < 2g$ and n_g divides $q^m - 1$ (see Frey and Lange, 2006, Proposition 5.78, p. 111).

Let $P(X)$ be the characteristic polynomial of the q-power Frobenius endomorphism of $\mathcal{J}_C$. $P(X)$ is called the *Weil polynomial* of $\mathcal{J}_C$. It is of the form

$$P(X) = X^{2g} + a_1X^{2g-1} + \cdots + a_gX^g + \cdots + a_1q^{g-1}X + q^g. \tag{1.3}$$

(See Frey and Lange, 2006, Corollary 5.82, p. 112). By the definition of $P(X)$,

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

i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$. (See Lang, 1959, pp. 109–110).

In general, the q^m-power Frobenius endomorphism of $\mathfrak{J}_C$ is denoted φ_m; note that $\varphi_m = \varphi^m$. Denote the characteristic polynomial of φ_m by $P_m(X)$. A number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$ is called a q^m-*Weil number* of $\mathfrak{J}_C$. Note that $\mathfrak{J}_C$ has four q^m-Weil numbers. It follows by (Lang, 1959, Theorem 3, p. 186) that if $P_1(X) = \prod_i (X - \omega_i)$, then $P_m(X) = \prod_i (X - \omega_i^m)$. Hence, if ω is a q-Weil number of $\mathfrak{J}_C$, then ω^m is a q^m-Weil number of $\mathfrak{J}_C$.

1.1.4 The Weil and the Tate pairing

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

$$\varepsilon_t : \mathfrak{J}_C(\mathbb{F})[\ell] \times \mathfrak{J}_C(\mathbb{F})/\ell\mathfrak{J}_C(\mathbb{F}) \longrightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^\ell.$$

It is called the *Tate pairing* (see Galbraith, 2005). 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

$$\hat{\varepsilon}_t : \mathfrak{J}_C(\mathbb{F})[\ell] \times \mathfrak{J}_C(\mathbb{F})/\ell\mathfrak{J}_C(\mathbb{F}) \longrightarrow \mu_\ell$$

is called the *reduced* Tate pairing. The (reduced) Tate pairing is bilinear, and if the field $\mathbb{F}$ contains the ℓ^{th} roots of unity, then it is non-degenerate (see Hess, 2004). A fast algorithm for computing the Weil pairing is given by Duursma and Lee (2003).

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

$$\varepsilon_w : \mathfrak{J}_C[\ell] \times \mathfrak{J}_C[\ell] \to \mu_\ell$$

is then defined by $\varepsilon_w(x, y) = \frac{\hat{\varepsilon}_t(x,\bar{y})}{\hat{\varepsilon}_t(y,\bar{x})}$. The Weil pairing is bilinear, anti-symmetric and non-degenerate on $\mathfrak{J}_C[\ell] \times \mathfrak{J}_C[\ell]$ (see Miller, 2004).

Both the Weil and the Tate pairing can be computed with Miller's algorithm (Miller, 1986). The Tate pairing can be computed more efficiently than the Weil pairing (see Galbraith, 2001).

Since $\mathbb{F}_{q^m}$ contains the ℓ^{th} roots of unity if and only if ℓ divides $q^m - 1$, the multiplicative order of q modulo ℓ plays an important role in pairing based cryptography.

Definition 1.3 (Embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathfrak{J}_C$. The embedding degree of $\mathfrak{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number k, such that $q^k \equiv 1 \pmod{\ell}$.

Throughout the thesis, we will denote the embedding degree by k. Closely related to the embedding degree, we have the *full* embedding degree.

Definition 1.4 (Full embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathfrak{J}_C$. The full embedding degree of $\mathfrak{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number k_0, such that $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{k_0}})$.

Throughout the thesis we will denote the full embedding degree by k_0.

Remark 1.5. If $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{k_0}})$, then $\ell \mid q^{k_0} - 1$; cf. (1.1) on page 3 and (1.2) on page 4. Hence, the full embedding degree is a multiple of the embedding degree.

A priori, the Weil pairing is only non-degenerate over $\mathbb{F}_{q^{k_0}}$. But in fact, as we shall see in chapter 2, the Weil pairing is also non-degenerate over $\mathbb{F}_{q^k}$.

1.2 Cryptography on curves

Elliptic curve cryptography, ECC, is cryptography based on the group law on the points on an elliptic curve. In this section, we recall how the group structure on the Jacobian of an elliptic curve lets us define a group structure on the curve, and give examples of cryptographic protocols on elliptic curves. Finally, we review some aspects of the latest research on pairings on Jacobians of genus two curves.

We use elliptic curve as an example; but everywhere the elliptic curve can be replaced by the Jacobian of a curve.

1.2.1 Elliptic curves

An elliptic curve (E, P_∞) over the field $\mathbb{F}$ is a curve E of genus one defined over $\mathbb{F}$ with a selected point $P_\infty \in E(\mathbb{F})$. P_∞ is called the *point at infinity.* By the Riemann-Roch Theorem, E is isomorphic to a planar curve (see Silverman, 1986, Proposition 3.1 p. 63). The points on E and the points on the Jacobian $\mathfrak{J}_E$ of E are in bijective correspondance by the map $\sigma : E \to \mathfrak{J}_E$, $P \mapsto P - P_\infty$ (see Silverman, 1986, Proposition 3.4, p. 66). Define addition of points on E by

$$P_1 \oplus P_2 = P_3 \iff (P_1 - P_\infty) + (P_2 - P_\infty) = (P_3 - P_\infty);$$

here the last equation is in the Jacobian. Then σ is a group isomorphism. In particular, $(E, \oplus)$ is a group. The group law is illustrated on figure 1.1.

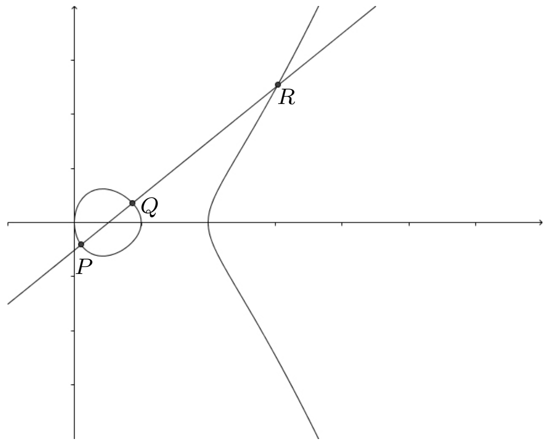


Figure 1.1: The group law on an elliptic curve over $\mathbb{R}$: $P \oplus Q \oplus R = \mathcal{O}$.

1.2.2 Classic cryptographic protocols

Consider an elliptic curve E defined over a field $\mathbb{F}$. The security of cryptographic protocols on elliptic curves is based on the *discrete logarithm problem*:

$$\text{Given } P, [n](P) \in E(\mathbb{F}), \text{ find } n. \tag{1.4}$$

In the following, we give instructive examples of classic cryptographic protocols on elliptic curves: (1) the Diffie-Hellman key exhange protocol and (2) the ElGamal protocol.

Example 1.6 (Diffie-Hellman key exchange)**.** The Diffie-Hellman protocol provides a key exchange between Alice and Bob. Choose an abelian group G and an element $P \in G$.

1. Alice chooses a secret number $a \in \mathbb{Z}$ and computes $Q_1 = [a](P)$. Similarly, Bob chooses a secret $b \in \mathbb{Z}$ and computes $Q_2 = [b](P)$.
2. Publicly, Alice and Bob exchange Q_1 and Q_2.
3. Alice and Bob computes $[a](Q_2)$ respectively $[b](Q_1)$.

Since $[a](Q_2) = [a][b](P) = [b][a](P) = [b](Q_1)$, Alice and Bob share the common secret $[ab](P)$ after using the protocol.

Example 1.7 (ElGamal encryption)**.** ElGamal is a *public key* protocol. The public parameters are an abelian group G, an element $P \in G$ and the order of P. Bob wishes to send a message $m \in G$ secretly to Alice. Alice has the secret key s_A and the public key $P_A = [s_A](P)$. The protocol consists of an encryption- and a decryption-part.

Encryption To send the message $m \in G$ secretly to Alice, Bob chooses a random number $a \in \mathbb{Z}$, and computes $R = [a](P)$ and $b = m + [a](P_A)$. Then Bob sends the pair (R, b) to Alice.

Decryption Alice has received a pair (R, b). She computes $S = [s_A](R)$, and reveals the message $m = b - S$. Since $S = [s_A](R) = [s_A][a](P) = [a][s_A](P) = [a](P_A)$, Alice now knows the original message $m \in G$.

1.2.3 Pairing based cryptographic protocols

The Diffie-Hellman key exchange protocol and the ElGamal protocol are both based on computations in an abelian group G; this group can e.g. be an elliptic curve or the multiplicative subgroup of a finite field. Hence, ECC with these protocols is essentially not a new cryptosystem; in ECC, the abelian group is merely represented in a clever way. In recent years, another cryptographic application of elliptic curves has been of increasing interest. This is the use of *pairings* on an elliptic curve (see Boneh and Franklin, 2001; Koblitz and Menezes, 2005). By using a pairing, not only the group structure on an elliptic curve is used; also the *representation* of the group is used. Hence, a *finer* structure is exploited, i.e. an essentially new cryptosystem is yielded.

Consider an elliptic curve E defined over a finite field $\mathbb{F}_q$. Let

$$\varepsilon : E[n] \times E[n] \to \mu_n \subseteq \mathbb{F}_{q^k}$$

be a bilinear and non-degenerate map. As ε we can choose e.g. the Weil or the Tate pairing; cf. section 1.1.4 on page 5.

Example 1.8 (Pairing based protocol)**.** By exploiting the bilinearity, Boneh and Franklin (2001) developed an *efficient identity based encryption.* The public parameters are an elliptic curve E and an n-torsion point $P \in E[n]$. Alice has the secret key $s_A \in \mathbb{Z}$ and the public key $P_A = [s_A](P)$. Alice is identified by the public n-torsion point $I_A \in E[n]$. Bob wishes to send a message $m \in \mathbb{F}_{q^k}$ secretly to Alice. This is done in the following way:

1. Bob chooses a random number $r \in \mathbb{Z}$ and computes the point $[r](P)$ and the pairing $\varepsilon(P_A, I_A)^r = \varepsilon([r](P_A), I_A)$.
2. Then Bob sends $[r](P)$ and $u = m + \varepsilon([r](P_A), I_A)$ to Alice.

Notice that

$$\varepsilon([r](P), D_A) = \varepsilon([r](P), [s_A](I_A)) = \varepsilon([r][s_A](P), I_A) = \varepsilon([r](P_A), I_A).$$

Since Alice knows $D_A = [s_A](I_A)$, she can compute $m = u - \varepsilon([r](P_A), I_A)$, i.e. decrypt the encrypted message.

Example 1.9 (Pairing based signature scheme)**.** With the bilinear map ε we can also construct a signature scheme. To do this, we exploit the fact that

$$\varepsilon(P, [a](Q)) = \varepsilon([b](P), Q) \iff a \equiv b \pmod{n}.$$

Still, the public parameters are the curve E and the n-torsion point $P \in E[n]$, and Alice has the secret key $s_A \in \mathbb{Z}$. To sign a message $Q \in E[n]$ with her secret key $s_A \in \mathbb{Z}$, Alice sends the tuple $(P, [s_A](P), Q, [s_A](Q))$. The point $[s_A](Q)$ is the *signature* on Q. The message is verified by the identity

$$\varepsilon(P, [s_A](Q)) = \varepsilon([s_A](P), Q).$$

Boneh, Lynn *et al.* (2004) describe the security of this kind of signature schemes.

These examples of exploiting pairings on elliptic curves are only instructive. A more thorough description is given in Paterson (2005).

1.2.4 Research on pairing based cryptography

Key distribution is perhaps *the* most basic problem in cryptography. For example, to maintain the security in a symmetric key protocol, new keys must be distributed frequently. The Diffie-Hellman key exchange protocol, Example 1.6 on page 7, partly solves this problem by providing an efficient key distribution system. But the Diffie-Hellman protocol requires the communicating parties Alice and Bob to exchange keys *before* they can communicate securely. Hence, the Diffie-Hellman is useless in situations where a pre-exchange of keys is either impossible or undesirable. Pairing based cryptography solves this problem: the public key of Alice can be derived from her social security number, say.

Consider the Jacobian $\mathfrak{J}_C$ of a genus two curve defined over a finite field $\mathbb{F}_q$. Let

$$\varepsilon : \mathfrak{J}_C(\mathbb{F}_{q^m})[n] \times \mathfrak{J}_C(\mathbb{F}_{q^m})[n] \to \mu_n \subseteq \mathbb{F}_{q^k}$$

be a pairing on the $\mathbb{F}_{q^m}$-rational n-torsion subgroup. A natural and central problem to consider is whether ε is non-degenerate, or how to ensure that ε is non-degenerate. Since the Tate pairing is non-degenerate if n divides $q^m - 1$

(see Hess, 2004), research is focused on the *embedding degree* k of the Jacobian, i.e. the multiplicative order of q modulo n.

In order to find curves with low embedding degree, supersingular curves are a natural first choice; these curves have embedding degree $k \leq 12$ (see Galbraith, 2001; Rubin and Silverberg, 2002). But furthermore, Jacobians of supersingular curves always have *distorsion maps* (Galbraith, Pujolàs *et al.*, 2006). A distortion map for a non-degenerate pairing ε and non-zero points $P_1, P_2 \in \mathcal{J}_C[n]$ is an endomorphism ψ on $\mathcal{J}_C$, such that $\varepsilon(P_1, \psi(P_2)) \neq 1$. When implementing pairing based cryptography on $\mathcal{J}_C(\mathbb{F}_q)[n]$, we might be facing the problem that $\varepsilon(P_1, P_2) = 1$ - this can happen, for example, if we use the Tate pairing and $k > 1$. In these situations, we need distortion maps. In other words, distortion maps ensure that pairing based cryptography can be implemented.

On the other hand, supersingular curves restrict us to embedding degrees $k \leq 12$. The next natural step is to consider non-supersingular curves. Galbraith, Mckee *et al.* (2007) gave a first step towards solving this problem by presenting some quadratic polynomial families of abelian varieties of dimension two with embedding degree $k = 5$ and $k = 10$. Hitt (2007) extended this result by presenting some quadratic polynomial families of Jacobians of genus two curves with larger embedding degrees. Unfortunately, neither Galbraith, Mckee *et al.* (2007) nor Hitt (2007) were able to generate any curves using the *complex multiplication method* (see Eisenträger and Lauter, 2007; Gaudry, Houtmann *et al.*, 2005; Weng, 2003). The first examples of non-supersingular genus two curves with "small" embedding degree (e.g., $k \leq 60$) were presented by Freeman (2007). But the Jacobians of these curves only have prime divisors $\ell \sim \sqrt[4]{q}$, and are therefore not attractive for cryptographic applications. Research in non-supersingular curves with low embedding degree is still needed.

Galbraith, Hess *et al.* (2007) list a number of open problems in pairing based cryptography. One open problem is to give *efficient methods to choose divisors in the particular subgroups.* In this thesis, this problem is adresses by (1) describing the rank of the $\mathbb{F}_{q^m}$-rational ℓ-torsion subgroup of the Jacobian of a genus two curve as a $\mathbb{Z}/\ell\mathbb{Z}$-module, and by (2) presenting a probabilistic algorithm to determine generators of the ℓ-torsion subgroup of the Jacobian of a genus two curve.

1.3 Genus two curves

In this final section we define a hyperelliptic curve, and prove that any genus two curve is hyperelliptic and can be represented by a planar curve.

1.3.1 Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable morphism $\phi : C \to \mathbb{P}^1$ of degree two.

Consider a hyperelliptic curve C of genus g defined over a (algebraically closed) field $\mathbb{F}$ of characteristic $p \neq 2$. Let $\phi : C \to \mathbb{P}^1$ be a separable morphism of degree two. Cf. (Silverman, 1986, p. 28), we define the *ramification index* of ϕ at a point $P \in C$ by

$$e_\phi(P) = \nu_P(\phi^* t_{\phi(P)}),$$

where ϕ^* is the pull-back of ϕ, and $t_{\phi(P)}$ is a local parameter at $\phi(P)$. So $e_\phi(P)$ is the order of P as a zero of the map $t_{\phi(P)} \circ \phi$. We note that since $t_{\phi(P)}(\phi(P)) = 0$, the ramification index $e_\phi(P) \geq 1$. By (Silverman, 1986, Proposition 2, p. 28),

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = 2. \tag{1.5}$$

Hence, $1 \leq e_\phi(P) \leq 2$ for any point $P \in C$. In particular, p does not divide $e_\phi(P)$. By Hurwitz' Theorem (see Silverman, 1986, Theorem 5.9, p. 41) it follows that

$$\sum_{P \in C(\bar{\mathbb{F}})} (e_\phi(P) - 1) = 2g + 2.$$

Hence,

Theorem 1.10. *A hyperelliptic curve C of genus g has exactly $2g+2$ points $P \in C$ with $e_\phi(P) = 2$.*

For any divisor $D \in \mathrm{Div}(C)$, let

$$\mathcal{L}(D) = \{f \in \mathbb{F}(C) | \operatorname{div}(f) + D > 0\} \cup \{0\}$$

be the space of functions with no poles outside the support of D. Denote the dimension of this space by $l(D) = \dim_{\mathbb{F}} \mathcal{L}(D)$. Let $P \in C(\mathbb{F})$ be a $\mathbb{F}$-rational point on C. A *gap value* in P is a number n with $\ell(nP) = \ell((n-1)P)$. By the Riemann-Roch Theorem,

$$1 = l(0) \leq \cdots \leq l((2g-1)P) = g,$$

and $l(nP) = n + 1 - g$ for $n \geq 2g - 1$. Since $l(nP) \leq l((n-1)P) + 1$, it follows that a curve of genus g has exactly g gap values

$$1 = n_1 < \cdots < n_g \leq 2g - 1.$$

The point P is called a *Weierstrass point*, if there exists a gap value $n_j \neq j$ in P.

Consider a genus two curve C defined over a field $\mathbb{F}$ of characteristic $p \neq 2$.

Theorem 1.11. *Any genus two curve C defined over a field $\mathbb{F}$ of characteristic $p \neq 2$ is hyperelliptic.*

Proof. Let $K > 0$ be a canonical divisor on C. By the Riemann-Roch Theorem we know that $\deg(K) = l(K) = 2$. Since $l(0) = 1$, it follows that any function $f \in \mathcal{L}(K) \setminus \mathcal{L}(0)$ will have two zeros, counted with multiplicity. Then the map $\phi : C \to \mathbb{P}^1$ given by $P \mapsto (1 : f(P))$ is a morphism of degree two. Since $p \neq 2$, it follows that ϕ is separable; cf. (Silverman, 1986, Corollary 2.12, p. 30). $\square$

1.3.2 Planar representation

Let $\phi : C \to \mathbb{P}^1$ be a separable morphism of degree two. Let $P_\infty \in C$ be a point with $e_\phi(P_\infty) = 2$. Since $\sum_{P \in \phi^{-1}(1:0)} e_\phi(P) = 2$ by (1.5) on the preceding page, composition of ϕ with the map $\mathbb{P}^1 \to \mathbb{F}$ given by $(1 : \xi) \mapsto \xi$ and $(0 : 1) \mapsto \infty$ defines a non-constant function $f \in \mathcal{L}(2P_\infty)$. Since $\deg(3P_\infty) = 3 = 2 \cdot 2 - 1$, it follows by the Riemann-Roch Theorem that $\ell(nP_\infty) = n - 1$ if $n \geq 3$. So $\ell(2P_\infty) = \ell(3P_\infty) = 2$. Hence, the gap values in P_∞ are $n_1 = 1$ and $n_2 = 3$, and P_∞ is a Weierstrass point on C. Let $\{1, x\}$ be a basis of $\mathcal{L}(2P_\infty)$, and $\{1, x, y\}$ a basis of $\mathcal{L}(4P_\infty)$, where y has a pole of order at most four in P_∞. Then

$$\{1, x, x^2, x^3, x^4, x^5, y, xy, x^2y, y^2\} \subseteq \mathcal{L}(10P_\infty).$$

Since $\ell(10P_\infty) = 9$, these functions are linearly dependent. So

$$y^2 + g(x)y = h(x), \tag{1.6}$$

for some polynomials $g, h \in \mathbb{F}[x]$ of degree $\deg g \leq 2$ and $\deg h \leq 5$. As in the proof of (Silverman, 1986, Theorem 3.1, p. 63), it follows that the map

$$\psi : C \to \mathbb{P}^2, \qquad P \mapsto (1 : x(P) : y(P))$$

is a birational map, mapping C to a variety $V \subseteq \mathbb{P}^2$ given on inhomogeneous form by (1.6), and that V is smooth. Hence, we may consider C as a smooth, plane curve. Every divisor class in the Jacobian is represented by a divisor of the form $P_1 + P_2 - 2P_\infty$ (see Duquesne and Lange, 2006, p. 305). The group law on the Jacobian of a genus two curve is illustrated on figure 1.2 on the next page. Duquesne and Lange (2006) gives explicit formulas for computing the group law.

Remark 1.12. By completing the square in (1.6) on this page, we see that any genus two curve C defined over a field of characteristic $p \neq 2$ can be given by an equation of the form

$$y^2 = f(x),$$

where $f \in \mathbb{F}[x]$ is a polynomial of degree $\deg f \leq 5$.

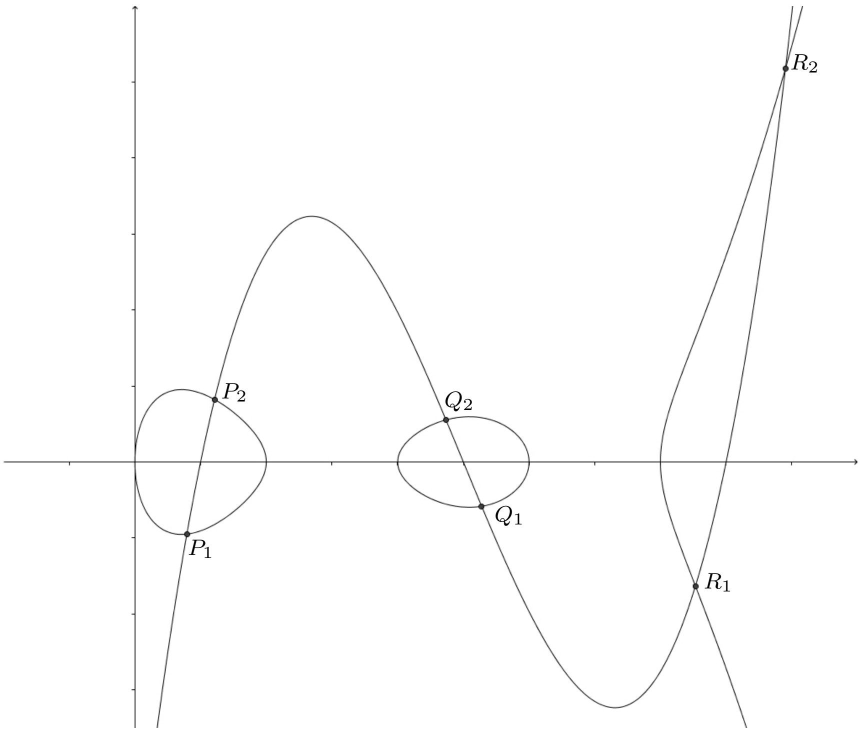


Figure 1.2: Group law on a genus two curve over $\mathbb{R}$: $(P_1+P_2)\oplus(Q_1+Q_2)\oplus(R_1+R_2) = \mathcal{O}$.

Chapter 2

Prime number torsion points

Consider the Jacobian $\mathcal{J}_C$ of a genus two curve 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, and let k be the multiplicative order of q modulo ℓ. The Tate pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$, and the Weil pairing is non-degenerate on $\mathcal{J}_C[\ell]$; cf. section 1.1.4 on page 5. 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 pairing based 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 (1998) proved that

$$\textit{if } \ell \nmid p-1, \textit{ then } E[\ell] \subseteq E(\mathbb{F}_{p^k}) \textit{ if and only if } \ell \mid p^k - 1. \tag{2.1}$$

By Rubin and Silverberg (2007), 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 $U = \mathcal{J}_C(\mathbb{F}_p)[\ell]$, $V = \ker(\varphi - p) \cap \mathcal{J}_C[\ell]$ and φ is the p-power Frobenius endomorphism of $\mathcal{J}_C$.*

The result (2.1) 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 (Ravnshøj, 2007b), the author generalized this result to certain CM reductions of Jacobians of genus two curves. In this chapter, we prove that in most cases this result in fact holds for Jacobians of *any* genus two curves, cf. Theorem 2.1 on page 17. With Theorem 2.2 on page 17 we describe the special case not included in Theorem 2.1, thus completing the description of the ℓ-torsion subgroup of the Jacobian.

By Theorem 2.1 and 2.2 it follows that if $k > 1$, then the Weil pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \times \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$; cf. Corollary 2.5 on page 18. For the

2-torsion part, we prove that if $|\mathcal{J}_C(\mathbb{F}_{q^m})|$ is even, then either $\mathcal{J}_C[2] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{4m}})$ or $\mathcal{J}_C[2] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{6m}})$; cf. Theorem 2.8 on page 20.

The matrix representation of the q-power Frobenius endomorphism on $\mathcal{J}_C[\ell]$ can be described explicitly. Actually, by Theorem 2.1 and 2.2 it follows that the matrix representation can be chosen either diagonal or of a particular form; cf. Theorem 2.12 on page 23.

Consider a supersingular genus two curve C defined over $\mathbb{F}_q$; cf. section 2.3. 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 $k \leq 12$ (see Galbraith, 2001; Rubin and Silverberg, 2002). If $\ell^2 \nmid |\mathcal{J}_C(\mathbb{F}_q)|$, then in many cases $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$ (see Stichtenoth and Xing, 1995). Zhu (2000) gives a complete description of the subgroup of $\mathbb{F}_q$-rational points on the Jacobian. Using Theorem 2.1, we obtain an explicit description of the ℓ-torsion subgroup of the Jacobian of a supersingular genus two curve; cf. Theorem 2.17 on page 24. In particular, it follows from Theorem 2.17 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.

Finally, we consider the case where q divides the number of $\mathbb{F}_q$-rational points $|\mathcal{J}_C(\mathbb{F}_q)|$ on the Jacobian. We prove that if $2q^2$ divides $|\mathcal{J}_C(\mathbb{F}_q)|$, then q is at most 16, and the Weil polynomial of $\mathcal{J}_C$ is on a very restricted list of polynomials; cf. Theorem 2.19 on page 28.

All results obtained and proved in this chapter are new. The result on $|\mathcal{J}_C(\mathbb{F}_q)|$ divisible by q is presented in (Ravnshøj, 2007c); the result on the matrix representation of the q-power Frobenius endomorphism is presented in (Ravnshøj, 2008c); all other results are presented in (Ravnshøj, 2008b).

The chapter is organized as follows: Section 2.1 is on the generalization of the result (2.1) on the previous page, and section 2.2 is on the diagonal representation of the Frobenius endomorphism. In section 2.3 we treat the supersingular case. The case where q divides $|\mathcal{J}_C(\mathbb{F}_q)|$ is treated in section 2.4.

2.1 Non-cyclic subgroups

Consider the Jacobian $\mathcal{J}_C$ of 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 of $\mathcal{J}_C$. $P_m(X)$ is of the form $P_m(X) = X^4+sX^3+tX^2+sq^mX+q^{2m}$, where $s,t \in \mathbb{Z}$; cf. (1.3) on page 4. Let $\tau = 8q^m + s^2 - 4t$. Then

$$P_m(X) = X^4 + sX^3 + (2q^m + (s^2 - \tau)/4)X^2 + sq^mX + q^{2m}.$$

We get the following description of the $\mathbb{F}_{q^m}$-rational ℓ-torsion subgroup.

Theorem 2.1. *Consider the Jacobian $\mathcal{J}_C$ of a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m of $\mathcal{J}_C$ as $P_m(X) = X^4 + sX^3 + (2q^m + (s^2 - \tau_m)/4)X^2 + sq^m X + q^{2m}$. 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 $\ell \nmid \tau_m$, 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 $(\alpha, q^m/\alpha)$, q^m is then also 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 (1.1) on page 3. Choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, such that φ_m is represented by a matrix of the form

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

with respect to $\mathcal{B}$. 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 $\tau_m \equiv 0 \pmod{\ell}$, and we have a contradiction. So $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module.

Now assume that $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ 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 $\tau_m \equiv 0 \pmod{\ell}$, 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 $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$, i.e. $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ must be of rank at least two as a $\mathbb{Z}/\ell\mathbb{Z}$-module. So $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic. ☐

If ℓ is a large prime number, then most likely $\ell \nmid \tau_m$, and Theorem 2.1 applies. In the special case where $\ell \mid \tau_m$, we get the following result.

Theorem 2.2. *Let the notation be as in Theorem 2.1. Furthermore, let ω_m be a q^m-Weil number of $\mathcal{J}_C$, and assume that ℓ is unramified in $K = \mathbb{Q}(\omega_m)$. Now assume that $\ell \mid \tau_m$. Then the following holds.*

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

Remark 2.3. A prime number ℓ is unramified in K if and only if ℓ divides the discriminant of the field extension $K/\mathbb{Q}$ (see Neukirch, 1999, 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 2.2 *does* occur; cf. the following example.

Example 2.4. Consider the polynomial $P(X) = (X^2 - 5X + 9)^2 \in \mathbb{Q}[X]$. By Maisner and Nart (2002) and Howe, Nart *et al.* (2007) it follows that $P(X)$ is the Weil polynomial of the Jacobian of a genus two curve C defined over $\mathbb{F}_9$. The number of $\mathbb{F}_9$-rational points on the Jacobian is $P(1) = 25$, so $\ell = 5$ is an odd prime divisor of $|\mathcal{J}_C(\mathbb{F}_9)|$ not dividing $q = 9$. Notice that $P(X) \equiv X^4 + 2qX^2 + q^2 \pmod 5$. The complex roots of $P(X)$ are given by $\omega = \frac{5+\sqrt{-11}}{2}$ and $\bar{\omega}$, and 5 is unramified in $\mathbb{Q}(\omega)$. Since $9^2 \equiv 1 \pmod 5$, it follows by Theorem 2.2 that $\mathcal{J}_C(\mathbb{F}_9)[5] \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathcal{J}_C[5] \subseteq \mathcal{J}_C(\mathbb{F}_{81})$.

By Theorem 2.1 and 2.2 we get the following corollary.

Corollary 2.5. *Consider the Jacobian $\mathcal{J}_C$ of 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 $\mathcal{J}_C$, 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 $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \times \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$.*

Proof. Let

$$P_k(X) = X^4 + sX^3 + (2q^m + (s^2 - \tau_k)/4)X^2 + sq^k X + q^{2k}$$

be the characteristic polynomial of the q^k-power endomorphism of the Jacobian $\mathcal{J}_C$. If $\ell \mid \tau_k$, then $\mathcal{J}_C[\ell] = \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ by Theorem 2.2, and the corollary follows.

Assume $\ell \nmid \tau_k$. Let $U = \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $V = \ker(\varphi - q) \cap \mathcal{J}_C[\ell]$, where φ is the q-power Frobenius endomorphism of $\mathcal{J}_C$. Then the Weil pairing ε_w is non-degenerate on $U \times V$ by Rubin and Silverberg (2007). By Theorem 2.1, we know that $V = \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and that

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

Now let $x \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ 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 points $y \in V$ and $z \in U$, such that $\varepsilon_w(x_U, y) \neq 1$ and $\varepsilon_w(x_V, z) \neq 1$. We may assume that $\varepsilon_w(x_U, y)\varepsilon_w(x_V, z) \neq 1$; if not, replace z with $2z$. Since the Weil pairing is anti-symmetric, $\varepsilon_w(x_U, z) = \varepsilon_w(x_V, y) = 1$. But then $\varepsilon_w(x, y + z) = \varepsilon_w(x_U, y)\varepsilon_w(x_V, z) \neq 1$. □

Proof of Theorem 2.2. 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 $K = \mathbb{Q}(\omega_m)$. By (Neukirch, 1999, 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 $\mathfrak{L}_2 = (\ell, \omega_m - q^m)\mathfrak{O}_K$. 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 $\{x_1\}$ 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

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

So the restriction of φ_m^k to $\mathcal{J}_C[\ell]$ 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 $\mathcal{J}_C$. Then

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

Since ω_m is a q^m-Weil number of $\mathcal{J}_C$, we know that ω_m^k is a q^{mk}-Weil number of $\mathcal{J}_C$. 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 $h(X) \equiv (X-1)^2 \pmod{\ell}$, and ℓ ramifies in K. So $\omega_m^k \in \mathbb{Q}$, i.e. h is of degree one. It follows that $h(X) \equiv X - 1 \pmod{\ell}$, i.e. $\omega_m^k \equiv 1 \pmod{\ell}$. So, φ_m^k is the identity map on $\mathcal{J}_C[\ell]$. 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. $\square$

Assume the Weil polynomial $P(X)$ splits in distinct linear factors modulo ℓ. Then

$$P_k(X) \equiv (X-1)^2(X-a)(X-1/a) \pmod{\ell}.$$

We see that $\tau_k = \frac{4(a-1)^4}{a^2}$. Hence, if ℓ divides τ_k, then $a \equiv 1 \pmod{\ell}$. But then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$, i.e. $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$. Hence, the following corollary holds.

Corollary 2.6. *If the Weil polynomial splits in distinct linear factors modulo ℓ, then*

$$\mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \simeq \begin{cases} \mathcal{J}_C[\ell], & \text{if } \tau_k \equiv 0 \pmod{\ell}, \\ \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}, & \text{if } \tau_k \not\equiv 0 \pmod{\ell}. \end{cases}$$

Remark 2.7. Assume the Weil polynomial $P(X)$ splits in linear factors modulo ℓ. Then $P(X)$ splits in *distinct* linear factors modulo ℓ if and only if ℓ does not divide the resultant $\operatorname{Res}(P, P', X)$. Hence, if $P(X)$ splits in linear factors modulo ℓ, then $P(X)$ splits in distinct linear factors modulo ℓ with probability $1 - 1/\ell$.

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

Theorem 2.8. *Consider the Jacobian $\mathcal{J}_C$ of 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 $\mathcal{J}_C$. Assume $|\mathcal{J}_C(\mathbb{F}_{q^m})|$ is even. Then*

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

Proof. Since q is odd,

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

Since $P_m(1)$ is even, it follows that t is even. Assume at first that s is even. 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. 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. $\square$

2.2 The matrix representation of the Frobenius endomorphism

Inspired by Theorem 2.1 and 2.2 on page 17 we introduce the following notation.

Definition 2.9. Consider the Jacobian $\mathfrak{J}_C$ of a genus two curve C defined over a finite field $\mathbb{F}_q$. We say that the Jacobian is a $\mathbb{J}(\ell, q, k, \tau_k)$-Jacobian or is of type $\mathbb{J}(\ell, q, k, \tau_k)$, and write $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, if the following holds.

1. The number ℓ is an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathfrak{J}_C$, ℓ divides neither q nor $q-1$, and $\mathfrak{J}_C(\mathbb{F}_q)$ is of embedding degree k with respect to ℓ.
2. The characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathfrak{J}_C$ is given by $P_k(X) = X^4 + sX^3 + (2q^k + (s^2 - \tau_k)/4)X^2 + sq^kX + q^{2k}$.
3. Let ω_k be a q^k-Weil number of $\mathfrak{J}_C$. If ℓ divides τ_k, then ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark 2.10. In most cases relevant to pairing based cryptography, ℓ is unramified in $\mathbb{Q}(\omega)$; cf. Remark 2.3 on page 18. But then $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$.

By Theorem 2.1 and 2.2, we get the following explicit description of the matrix representation of the Frobenius endomorphism of the Jacobian of a genus two curve.

Theorem 2.11. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$. If φ is not diagonalizable on $\mathcal{J}_C[\ell]$, then φ is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} \tag{2.2}$$

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. In particular, $c \not\equiv q+1 \pmod{\ell}$.

Proof. Assume at first that ℓ does not divide τ_k. Then we know that $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic and that $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 2.1. Choose points $x_1, x_2 \in \mathcal{J}_C[\ell]$, such that $\varphi(x_1) = x_1$ and $\varphi(x_2) = qx_2$. Then the set $\{x_1, x_2\}$ is a basis of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Now, extend $\{x_1, x_2\}$ to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. If x_3 and x_4 are eigenvectors of φ, then φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Assume x_3 is not an eigenvector of φ. Then the set $\mathcal{B}' = \{x_1, x_2, x_3, \varphi(x_3)\}$ is a basis of $\mathcal{J}_C[\ell]$, and φ is represented by a matrix of the form (2.2) with respect to $\mathcal{B}'$.

Now, assume ℓ divides τ_k. Since ℓ divides $q^k - 1$, it follows that the ℓ-torsion subgroup $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 2.2. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of the Weil polynomial $P(X)$ modulo ℓ. Assume that 1 is an root of $P(X)$ modulo ℓ of multiplicity ν. Since the roots of $P(X)$ occur in pairs $(\alpha, q/\alpha)$, it follows that

$$P(X) \equiv (X-1)^\nu (X-q)^\nu Q(X) \pmod{\ell},$$

where $Q \in \mathbb{Z}[X]$ is a polynomial of degree $4-2\nu$, $Q(1) \not\equiv 0 \pmod{\ell}$ and $Q(q) \not\equiv 0 \pmod{\ell}$. Let $U = \ker(\varphi - 1)^\nu$, $V = \ker(\varphi - q)^\nu$ and $W = \ker(Q(\varphi))$. Then U, V and W are φ-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U) = \operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(V) = \nu$, and $\mathcal{J}_C[\ell] \simeq U \oplus V \oplus W$. If $\nu = 1$, then it follows as above that φ is either diagonalizable on $\mathcal{J}_C[\ell]$ or represented by a matrix of the form (2.2) with respect to some basis of $\mathcal{J}_C[\ell]$. Hence, we may assume that $\nu = 2$. Now, choose $x_1 \in U$ such that $\varphi(x_1) = x_1$, and extend $\{x_1\}$ to a basis $\{x_1, x_2\}$ of U. Similarly, choose a basis $\{x_3, x_4\}$ of V with $\varphi(x_3) = qx_3$. With respect to the basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$, φ is represented by a matrix of the form

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

Notice that

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

Since $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$, we know that $\varphi^k = \varphi_k$ is the identity on $\mathcal{J}_C[\ell]$. Hence, $M^k = I$. So $\alpha \equiv \beta \equiv 0 \pmod{\ell}$, i.e. φ is represented by a diagonal matrix with respect to $\mathcal{B}$.

Finally, if $c \equiv q + 1 \pmod{\ell}$, then M is diagonalizable. The theorem is proved. □

Whether the Frobenius endomorphism is diagonalizable depends on the splitting behaviour of the Weil polynomial modulo ℓ.

Theorem 2.12. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let ω be a q-Weil number of $\mathcal{J}_C$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$. Then φ is diagonalizable on $\mathcal{J}_C[\ell]$ if and only if the Weil polynomial of $\mathcal{J}_C$ splits in linear factors modulo ℓ.*

Proof. "Only if" is obvious. We prove the "if" part. Write the Weil polynomial of $\mathcal{J}_C$ as

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}.$$

If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then the theorem follows. If $\alpha \equiv 1, q \pmod{\ell}$, then

$$\begin{aligned} P(X) &\equiv (X-1)^2(X-q)^2 \\ &\equiv X^4 + sX^3 + (2q + (s^2-\tau)/4)X^2 + sqX + q^2 \pmod{\ell}, \end{aligned}$$

where $s \equiv -(q+1) \pmod{\ell}$ and $\tau \equiv 0 \pmod{\ell}$. But then the theorem follows by the last part of the proof of Theorem 2.11. Finally, assume that $\alpha \equiv q/\alpha \pmod{\ell}$, i.e. that $\alpha^2 \equiv q \pmod{\ell}$. Then the q-power Frobenius endomorphism is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form

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

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. Notice that

$$M^{2k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2k\alpha^{2k-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, $P_{2k}(X) \equiv (X-1)^4 \pmod{\ell}$. By Theorem 2.2 on page 17 it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{2k}})$. But then $M^{2k} = I$, i.e. $\beta \equiv 0 \pmod{\ell}$. Hence, the q-power Frobenius endomorphism of $\mathcal{J}_C$ is diagonalizable on $\mathcal{J}_C[\ell]$ also in this case. The theorem is proved. □

Remark 2.13. Assume the Weil polynomial splits modulo ℓ. Then most likely, the Frobenius endomorphism is diagonalizable; cf. Remark 2.3 on page 18. But the Frobenius endomorphism is not *always* diagonalizable. Cf. Example 2.14.

Example 2.14. Consider the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by $y^2 = x^5 + 2x + 1$. The Weil polynomial of $\mathcal{J}_C$ is given by

$$P(X) = X^4 + 3X^3 - 2X^2 + 9X + 9.$$

Since $P(1) = 20$, $P(X) \equiv (X-1)(X-3)(X^2+2X+3) \pmod{5}$ and the polynomial X^2+2X+3 is irreducible over $\mathbb{F}_5$, the 3-power Frobenius endomorphism is not diagonalizable on $\mathcal{J}_C[5]$.

2.3 Supersingular curves

Consider a genus two curve C defined over a finite field $\mathbb{F}_q$ of characteristic p. The curve C is called *supersingular*, if $\mathcal{J}_C$ has no p-torsion. From Maisner and Nart (2002) we have the following theorem.

Theorem 2.15. *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 2.1 on the next page.

Remark 2.16. By Howe, Nart *et al.* (2007), in each of the cases in table 2.1 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 $\mathbb{F}_q$.

Using Theorem 2.1 on page 17, Theorem 2.2 on page 17 and Theorem 2.15 we get the following explicit description of the ℓ-torsion subgroup of the Jacobian of a supersingular genus two curve.

Theorem 2.17. *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 2.1 on the next page we get the following properties of $\mathcal{J}_C$.*

Table 2.1: 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, $p \equiv 1 \pmod 3$.

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 2.18. *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 2.17. In the following we consider each case in table 2.1 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 2.1.

Case i. If $(s,t) = (0,0)$, then $f(1) = 1 + q^2 \equiv 0 \pmod{\ell}$, and it follows that $q^2 \equiv -1 \pmod{\ell}$. So $f(X) \equiv X^4 - 1 \pmod{\ell}$, $q^4 \equiv 1 \pmod{\ell}$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^4})$. $\tau = 8q$ in Theorem 2.1, so if $\ell \neq 2$, then $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ 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 $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^6})$. If $\ell = 2$, then $p \neq 2$, and $f(1)$ is odd. So $\ell \neq 2$. $\tau = 4q$ in Theorem 2.1, so $\mathfrak{J}_C(\mathbb{F}_q)$ 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 $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^6})$. As in case ii, $\ell \neq 2$. Now $\tau = 12q$, so if $\ell \neq 3$, then $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ 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 (Tate, 1966, Theorem 2), $\mathfrak{J}_C \simeq E \times E$ for some supersingular elliptic curve E. It follows that $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^2})$. $\tau = 16q$, so if $\ell \neq 2$, then $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ 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 $\mathfrak{J}_C \simeq E \times E$ for some supersingular elliptic curve E. So $q^2 \equiv 1 \pmod{\ell}$ and $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^2})$. $\tau = 0$ and $\omega = i\sqrt{q}$ is a q-Weil number of $\mathfrak{J}_C$. 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 $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ is bicyclic by Theorem 2.2.

Case iv–vi

Now we consider the cases iv, v and vi of table 2.1.

Case iv. If $(s,t) = (\sqrt{q}, q)$, then $\tau = 5q$ in Theorem 2.1. Since $f(1)$ is odd, we know that $\ell \neq 2$. If ℓ divides τ, 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 $\ell \nmid \tau$. If $q \equiv 1 \pmod{\ell}$, then $f(1) \equiv 5 \pmod{\ell}$, i.e. $\ell = 5$. But then ℓ divides τ, a contradiction. So $\mathfrak{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 2.1. 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 $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{10}})$. The case $(s,t) = (-\sqrt{q}, q)$ follows similarly.

Case v. If $(s,t) = (\sqrt{5q}, 3q)$ and $p = 5$, then τ is a power of 5 in Theorem 2.1. Since $f(1)$ is odd, we know that $\ell \neq 2$. If ℓ divides τ, then $\ell = 5$. Since C is supersingular and defined over a field of characteristic $p = 5$, this is a contradiction. So $\ell \nmid \tau$. 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 $\mathfrak{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 2.1. 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 $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{10}})$. The case $(s,t) = (-\sqrt{5q}, 3q)$ follows similarly.

Case vi. If $(s,t) = (\sqrt{2q}, q)$ and $p = 2$, then $\tau = 3 \cdot 2^a$ for some $a \in \mathbb{N}$. Hence, if ℓ divides τ, then $\ell = 3$. But $3 \nmid f(1)$; thus, $\ell \nmid \tau$. 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 $\mathfrak{J}_C(\mathbb{F}_q)$ is cyclic by Theorem 2.1. 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 $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^{24}})$. 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 (Tate, 1966, Theorem 2), $\mathfrak{J}_C \simeq E \times E$ for some supersingular elliptic curve E. Hence, either $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ is bicyclic or equals the full ℓ-torsion subgroup of $\mathfrak{J}_C$.

Assume $\mathfrak{J}_C(\mathbb{F}_q)[\ell] = \mathfrak{J}_C[\ell]$. 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, $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^3})$ by the non-degeneracy of the Tate pairing.

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

2.4 q-subgroups of $\mathfrak{J}_C(\mathbb{F}_q)$

Consider the Jacobian of a genus two curve defined over a finite field $\mathbb{F}_q$. In most cases, q^2 does not divide the number of $\mathbb{F}_q$-rational points on the Jacobian.

Theorem 2.19. *Let $\mathcal{J}_C$ be the Jacobian of a genus two curve defined over $\mathbb{F}_q$. If $2q^2$ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, then the Weil polynomial of $\mathcal{J}_C$ is in the following list.*

1. $X^4 + 4X^3 + 16X^2 + 28X + 49$.
2. $X^4 + sX^3 + tX^2 + 3sX + 9$, *where* $(s,t) \in \{(1,4),(4,10)\}$.
3. $X^4 + sX^3 + tX^2 + 2^n sX + 2^{2n}$, *where either*
   a) $n = 1$ *and* $(s,t) = (1,0)$,
   b) $n = 2$ *and* $(s,t) \in \{(-2,9),(-1,4),(0,-1),(2,5)\}$,
   c) $n = 3$ *and* $(s,t) \in \{(-2,17),(-1,8),(0,-1)\}$, *or*
   d) $n = 4$ *and* $(s,t) \in \{(-2,33),(-1,16),(0,-1)\}$.

In particular, $q \in \{2,3,4,7,8,16\}$.

Proof. Assume q^2 divides $N = |\mathcal{J}_C(\mathbb{F}_q)|$. Let ω_i be the q-Weil numbers of $\mathcal{J}_C$. Since $|\omega_i| = \sqrt{q}$, we know that

$$N = P(1) = \prod_{i=1}^{4}(1-\omega_i) \leq (1+\sqrt{q})^4 = q^2 + 4q\sqrt{q} + 6q + 4\sqrt{q} + 1.$$

Hence, $\frac{N}{q^2} < 2$ for $q > 25$. So if $q > 25$, then 2 does not divide N. This is a contradiction. Thus, if $q > 25$, then q^2 does not divide N.

Assume $q \leq 25$. The Weil polynomial of $\mathcal{J}_C$ is of the form

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

where $|s| \leq 4\sqrt{q}$ and $2|s|\sqrt{q} - 2q \leq t \leq \frac{s^2}{4} + 2q$; cf. e.g. (Maisner and Nart, 2002, Lemma 2.1). Hence, there is only a small, finite number of candidates for $P(X)$. Let $\mathcal{C}$ be the set of candidates for P. Now, find the set of possibilities $\mathcal{P}$ for $P(X)$ by checking if $f(1)$ is even and divisible by q^2 for each $f \in \mathcal{C}$. The Theorem then follows by checking if each $f \in \mathcal{P}$ is the Weil polynomial of the Jacobian of some genus two curve by using (Howe, Nart *et al.*, 2007, Theorem 1.2). The details are left to the reader. □

Remark 2.20. Theorem 2.19 concerns Jacobians with an even number of rational points. By using results of Tate (1966) and Honda (1968), Zieve (2007) generalizes Theorem 2.19 to any Jacobian of a genus two curve.

Chapter 3

Finding generators

Consider the Jacobian $\mathcal{J}_C$ of a genus two curve defined over $\mathbb{F}_q$. Freeman and Lauter (2008) describes a probabilistic algorithm to determine generators of the subgroup $\mathcal{J}_C[\ell]$ of points of order ℓ, but the algorithm is incomplete in the sense that the output only *probably* is a generating set - it is not tested whether the output in fact *is* a generating set. Furthermore, if the output happens to be a generating set, it still may not be a *basis* of $\mathcal{J}_C[\ell]$. Miller (2004) uses the Weil pairing to find a basis of $E(\mathbb{F}_q)$, where E is an elliptic curve defined over a finite field $\mathbb{F}_q$. In this chapter we generalize this procedure to Jacobians of genus two curves. Freeman and Lauter (2008) use their algorithm to compute endomorphism rings of Jacobians of genus two curves, and this in turn has applications for generating Jacobians of genus two curves using the CRT version of the CM method (Eisenträger and Lauter, 2007). Hence, the algorithms presented in this chapter also has applications for generating Jacobians of genus two curves.

Consider the Jacobian $\mathcal{J}_C$ of a genus two curve defined over $\mathbb{F}_q$. Frey and Rück (1994) show that if m divides $q-1$, then the discrete logarithm problem (see (1.4) on page 7) in the rational m-torsion subgroup $\mathcal{J}_C(\mathbb{F}_q)[m]$ can be reduced to the corresponding problem in $\mathbb{F}_q^\times$ (Frey and Rück, 1994, Corollary 1). In the proof of this result it is claimed that the non-degeneracy of the Tate pairing can be used to determine whether r random points of the finite group $\mathcal{J}_C(\mathbb{F}_q)[m]$ in fact is an independent set of generators of $\mathcal{J}_C(\mathbb{F}_q)[m]$. In this chapter we obtain an explicit, probabilistic algorithm to determine generators of $\mathcal{J}_C(\mathbb{F}_q)[m]$, where m is the largest divisor of the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, such that ℓ divides $q-1$ for every prime number ℓ dividing m; cf. Algorithm 3.11 on page 35.

Algorithm 3.11 is based on solving the discrete logarithm problem in the group $\mathcal{J}_C(\mathbb{F}_q)[m]$. Contrary to the special case where the prime number divisors of m divide $q-1$, this is infeasible in general. Hence, in general this algorithm does not apply. But if the prime number divisors of m do not divide $q-1$, then the algorithm in (Miller, 2004) can be generalized to Jacobians of genus two curves; cf. Algorithm 3.24 on page 44. To obtain this generalization, we give an explicit description of the representation of the Weil pairing on the ℓ-torsion subgroup $\mathcal{J}_C[\ell]$; cf. Theorem 3.19 on page 40.

All results obtained and proved in this chapter are new. Algorithm 3.11 is presented in (Ravnshøj, 2007a), and Algorithm 3.24 is presented in (Ravnshøj, 2008c).

The chapter is organized as follows: In section 3.1 we recall some facts concerning finite abelian groups, and obtain an algorithm to choose an element of prime number order in a finite abelian group. In section 3.2 we obtain the explicit, probabilistic algorithm to determine generators of $\mathcal{J}_C(\mathbb{F}_q)[m]$, where m is the largest divisor of the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, such that ℓ divides $q-1$ for every prime number ℓ dividing m. In section 3.3 we generalize the algorithm in (Miller, 2004) to Jacobians of genus two curves. We will write $\langle P_i | i \in I\rangle = \langle P_i\rangle_i$ and $\bigoplus_{i\in I}\langle P_i\rangle = \bigoplus_i \langle P_i\rangle$ if the index set I is clear from the context.

3.1 Finite abelian groups

Miller (2004) shows the following theorem.

Theorem 3.1. *Let G be a finite abelian group of torsion rank r. Then for $s \geq r$ the probability that a random s-tuple of elements of G generates G is at least*

$$\frac{C_s}{\log\log|G|}$$

if $s = r$, and at least C_s if $s > r$, where $C_s > 0$ is a constant depending only on s (and not on $|G|$).

To determine whether a generating set $\{g_1, \ldots, g_s\} \subseteq G$ is independent, i.e. $\langle g_1, \ldots, g_s\rangle \simeq \bigoplus_i \langle g_i\rangle$, we need to know the subgroups of a cyclic ℓ-group G. These are determined uniquely by the order of G, since

$$\{0\} \subseteq \langle \ell^{n-1}g\rangle \subseteq \langle \ell^{n-2}g\rangle \subseteq \cdots \subseteq \langle \ell g\rangle \subseteq G$$

are the subgroups of the group $G = \langle g\rangle$ of prime power order ℓ^n. The following corollary is an immediate consequence of this observation.

Corollary 3.2. *Let U_1 and U_2 be cyclic subgroups of a finite group G. Assume U_1 and U_2 are ℓ-groups. Let $\langle u_i \rangle \subseteq U_i$ be the subgroups of order ℓ. Then $U_1 \cap U_2 = \{e\}$ if and only if $\langle u_1 \rangle \cap \langle u_2 \rangle = \{e\}$. Here, $e \in G$ is the neutral element.*

Consider a finite, abelian group G of order $|G| = N$. Let G_ℓ be the Sylow-ℓ subgroup of G. The following algorithm computes $N_\ell = |G_\ell|$.

Algorithm 3.3. *In the following steps, on input a number $N \in \mathbb{Z}$ and a prime divisor ℓ of N, the algorithm outputs ℓ^a, where $\frac{N}{\ell^a} \in \mathbb{Z}$ is not divisible by ℓ.*

1. *Let $N_\ell := 1$ and $M := N$. While ℓ divides M, do the following*
   a) *$N_\ell := \ell \cdot N_\ell$.*
   b) *$M := \frac{M}{\ell}$.*
2. *Output N_ℓ.*

Notice that $\frac{N}{N_\ell} g \in G_\ell$ for any element $g \in G$. Hence, the following algorithm outputs a non-trivial element $g \in G_\ell$.

Algorithm 3.4. *In the following steps, on input a finite, abelian group G of order N and a prime divisor ℓ of N, the algorithm outputs a non-trivial element $g \in G_\ell$.*

1. *Compute $N_\ell = |G_\ell|$ using e.g. Algorithm 3.3*
2. *Choose a random element $g \in G$. Compute $g := \frac{N}{N_\ell} g$.*
3. *If $g = 0$, then go to step 2.*
4. *Output g.*

3.2 The special case $\ell \mid q-1$

Let $\mathfrak{J}_C$ be the Jacobian of a genus two curve defined over a finite field $\mathbb{F}_q$. By (1.2) on page 4,

$$\mathfrak{J}_C(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}/n_3\mathbb{Z} \oplus \mathbb{Z}/n_4\mathbb{Z}, \tag{3.1}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid q-1$.

Frey and Rück (1994) show that if ℓ divides $q-1$, then the discrete logarithm problem in the rational ℓ-torsion subgroup $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ can be reduced to the corresponding problem in $\mathbb{F}_q^\times$ (Frey and Rück, 1994, Corollary 1). In the proof of this result, it is claimed that the non-degeneracy of the Tate pairing can be used to determine whether r random points of the finite group $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$

in fact is an independent set of generators of $\mathcal{J}_C(\mathbb{F}_q)[\ell]$. In this section, we describe an explicit, probabilistic algorithm to determine generators of

$$G = \mathcal{J}_C(\mathbb{F}_q)[m],$$

where m is the largest divisor of the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, such that ℓ divides $q-1$ for every prime number ℓ dividing m. The algorithm is given by Algorithm 3.11.

As an abelian group, G is isomorphic to the direct sum of its Sylow subgroups. Hence, to determine generators of G, we only need to determine generators of the Sylow-ℓ subgroups G_ℓ for every ℓ dividing both $q-1$ and the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. In the following steps we find points $P_i \in G_\ell$, such that $G_\ell \simeq \bigoplus_i \langle P_i \rangle$.

1. Choose random points $P_i \in G_\ell$ and $Q_j \in \mathcal{J}_C(\mathbb{F}_q)$, $i, j \in \{1, \dots, 4\}$.
2. Use the non-degeneracy of the reduced Tate pairing $\hat{\varepsilon}_t$ to *diagonalize* the sets $\{P_i\}_i$ and $\{Q_j\}_j$ with respect to $\hat{\varepsilon}_t$; i.e. modify the sets such that $\hat{\varepsilon}_t(P_i, Q_j) = 1$ if $i \neq j$ and $\hat{\varepsilon}_t(P_i, Q_i)$ is an ℓ^{th} root of unity.
3. If $\prod_i |P_i| < |G_\ell|$ then go to step 1.
4. Output the points P_1, P_2, P_3 and P_4.

Remark 3.5. Combining Theorem 3.1 on page 30 and (3.1) on the preceding page, we expect to find generators of G_ℓ by choosing four random points of G_ℓ in approximately $\frac{\log\log|G_\ell|}{C_4}$ attempts.

The key ingredient of the algorithm is the diagonalization in step 2; this process is explained in section 3.2.1.

3.2.1 Diagonalization

Consider a prime number ℓ dividing $N = |\mathcal{J}_C(\mathbb{F}_q)|$ and $q-1$. Choose four random points $\mathcal{O} \neq P_i \in \mathcal{J}_C(\mathbb{F}_q)_\ell$, using e.g. Algorithm 3.4 on the preceding page.

Let $|P_i| = \ell^{\nu_i}$, and re-enumerate the P_i's such that $\nu_i \leq \nu_{i+1}$. Since $P_i \neq \mathcal{O}$, we know that $\nu_i \neq 0$ for all i. Let $\zeta \in \mathbb{F}_q^\times$ be an element of order ℓ. Now, let $P_i' = [\ell^{\nu_i - 1}](P_i)$ for all i. Then $P_i' \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ for all i. Finally, choose four random points $Q_i \in \mathcal{J}_C(\mathbb{F}_q)$.

Since ℓ divides $q-1$, the reduced Tate pairing

$$\hat{\varepsilon}_t : \mathcal{J}_C(\mathbb{F}_q)[\ell] \times \mathcal{J}_C(\mathbb{F}_q)/\ell\mathcal{J}_C(\mathbb{F}_q) \to \langle\zeta\rangle \subseteq \mathbb{F}_q^\times$$

is non-degenerate; cf. section 1.1.4. Choose a point $Q \in \mathcal{J}_C(\mathbb{F}_q)$, such that $\hat{\varepsilon}_t(P_i', Q) \neq 1$. Write $\hat{\varepsilon}_t(P_i', Q_j) = \zeta^{\alpha_{ij}}$, where $\alpha_{ij} \in \mathbb{Z}$. Now, assume that the quotient $\mathcal{J}_C(\mathbb{F}_q)/\ell\mathcal{J}_C(\mathbb{F}_q)$ is generated by the classes $\overline{Q}_1$, $\overline{Q}_2$, $\overline{Q}_3$ and $\overline{Q}_4$. Then $\overline{Q} = \sum_i a_i\overline{Q}_i$, i.e.

$$\hat{\varepsilon}_t(P_i', Q) = \zeta^{\alpha_{i1}a_1+\alpha_{i2}a_2+\alpha_{i3}a_3+\alpha_{i4}a_4}.$$

If $\alpha_{ij} \equiv 0 \pmod{\ell}$ for $1 \le j \le 4$, then $\hat{\varepsilon}_t(P_i', Q) = 1$. Hence the following lemma.

Lemma 3.6. *Let the notation be as above. If the quotient $\mathcal{J}_C(\mathbb{F}_q)/\ell\mathcal{J}_C(\mathbb{F}_q)$ is generated by the classes $\overline{Q}_1$, $\overline{Q}_2$, $\overline{Q}_3$ and $\overline{Q}_4$, then for all i we may choose a j, such that $\alpha_{ij} \not\equiv 0 \pmod{\ell}$.*

Re-enumerate the Q_i's such that $\alpha_{44} \not\equiv 0 \pmod{\ell}$. Now, choose numbers $a_j \in \mathbb{Z}$ with $a_j \equiv \alpha_{44}^{-1}\alpha_{4j} \pmod{\ell}$ for $1 \le j \le 3$. Replacing Q_j by $Q_j - a_jQ_4$ then yields $\alpha_{4j} \equiv 0 \pmod{\ell}$ for $1 \le j \le 3$. Thus, we may assume that $\alpha_{41} \equiv \alpha_{42} \equiv \alpha_{43} \equiv 0 \pmod{\ell}$ and $\alpha_{44} \not\equiv 0 \pmod{\ell}$. Similarly, we may assume that $\alpha_{14} \equiv \alpha_{24} \equiv \alpha_{34} \equiv 0 \pmod{\ell}$. Repeating this procedure recursively, we may assume that $\alpha_{ij} \equiv 0 \pmod{\ell}$ if and only if $i \ne j$, and that $\alpha_{ii} \not\equiv 0 \pmod{\ell}$; here, $1 \le i, j \le 4$.

The discussion above is formalized in the following algorithm.

Algorithm 3.7. *The following algorithm takes as input the Jacobian $\mathcal{J}_C$ of a genus two curve C defined over a finite field $\mathbb{F}_q$, the number $N = |\mathcal{J}_C(\mathbb{F}_q)|$ of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, and a prime number ℓ dividing N and $q-1$. The algorithm outputs points $P_i \in \mathcal{J}_C(\mathbb{F}_q)_\ell$ of the Sylow-ℓ subgroup $\mathcal{J}_C(\mathbb{F}_q)_\ell$ of $\mathcal{J}_C(\mathbb{F}_q)$, such that $\langle P_i\rangle_i = \bigoplus_i \langle P_i\rangle$ in the following steps.*

1. *Choose points $\mathcal{O} \ne P_i \in \mathcal{J}_C(\mathbb{F}_q)_\ell$, $i \in I := \{1,2,3,4\}$, using e.g. Algorithm 3.4.*
2. *Choose points $Q_i \in \mathcal{J}_C(\mathbb{F}_q)$, $i \in I$.*
3. *Let $J := \{1,2,3,4\}$. For j_0 from 0 to 3 do the following:*
   a) *Let $j_{\max} := 4 - j_0$.*
   b) *Compute the orders $\ell^{\nu_j} := |P_j|$, $j \in J$. Re-enumerate the P_j's such that $\nu_j \le \nu_{j+1}$, $j \in J$. If $\nu_{j_{\max}} = 0$, then go to step 4.*
   c) *Compute $P_j' = [\ell^{\nu_j-1}](P_j)$ for $j \in J$. If $\hat{\varepsilon}_t(P_{j_{\max}}', Q_j) = 1$ for all $j \in J$, then go to step 2.*
   d) *Re-enumerate the Q_j's for $j \in J$, such that $\hat{\varepsilon}_t(P_{j_{\max}}', Q_{j_{\max}}) \ne 1$. Let $\zeta := \hat{\varepsilon}_t(P_{j_{\max}}', Q_{j_{\max}})$.*
   e) *For $1 \le j < j_{\max}$, compute numbers $\alpha_{j_{\max}j}, \alpha_{jj_{\max}} \in \mathbb{Z}$ such that $\hat{\varepsilon}_t(P_{j_{\max}}', Q_j) = \zeta^{\alpha_{j_{\max}j}}$ and $\hat{\varepsilon}_t(P_j', Q_{j_{\max}}) = \zeta^{\alpha_{jj_{\max}}}$.*
   f) *Let $Q_j := Q_j - [\alpha_{j_{\max}j}](Q_{j_{\max}})$, $P_j := P_j - [\alpha_{jj_{\max}}\ell^{\nu_{j_{\max}}-\nu_j}](P_{j_{\max}})$, and $J := J \setminus \{j_{\max}\}$.*
4. *Output $\{P_1, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4\}$.*

Remark 3.8. Algorithm 3.7 consists of a small number of (1) calculations of orders of points $P \in \mathcal{J}_C(\mathbb{F}_q)_\ell$, (2) multiplications of points $P \in \mathcal{J}_C(\mathbb{F}_q)$ with numbers $a \in \mathbb{Z}$, (3) additions of points $P_1, P_2 \in \mathcal{J}_C(\mathbb{F}_q)$, (4) evaluations of pairings of points $P_1, P_2 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and (5) solving the discrete logarithm problem in $\mathbb{F}_q^\times$, i.e. to determine α from ζ and $\xi = \zeta^\alpha$. Choosing a random point on $\mathcal{J}_C(\mathbb{F}_q)$ takes $O(\log q)$ field operations in $\mathbb{F}_q$, and computing a multiple $[m](P)$ or the sum $P + Q$ of points $P, Q \in \mathcal{J}_C(\mathbb{F}_q)$ also takes $O(\log q)$ field operations in $\mathbb{F}_q$ (see Freeman and Lauter, 2008, proof of Proposition 4.6). The order $|P|$ of a point $P \in \mathcal{J}_C(\mathbb{F}_q)_\ell$ can be calculated in $O(\log N_\ell)\mathcal{A}$ field operations in $\mathbb{F}_q$, where $\mathcal{A}$ is the number of field operations in $\mathbb{F}_q$ needed for adding two points on $\mathcal{J}_C(\mathbb{F}_q)$. By Frey and Rück (1994), evaluating the Tate pairing on two point of $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ takes $O(\log \ell)$ field operations in $\mathbb{F}_q$. The reduced Tate pairing is computed by raising the value of the Tate pairing to the power $\frac{q-1}{\ell}$. The exponentiation takes $O(\log \frac{q-1}{\ell})$ field operations in $\mathbb{F}_q$. Hence, evaluating the reduced Tate pairing on two point on $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ takes $O(\log \ell)O(\log \frac{q-1}{\ell})$ field operations in $\mathbb{F}_q$. Finally, by Pohlig and Hellman (1978) the discrete logarithm problem in $\mathbb{F}_q^\times$ can be solved in $O(\log q)$ field operations in $\mathbb{F}_q$. We see that the pairing computation is the most expensive step. Hence, we expect Algorithm 3.7 to run in $O(\log \ell \log \frac{q-1}{\ell})$ field operations in $\mathbb{F}_q$.

By carefully examining Algorithm 3.7, we see that the following lemma holds.

Lemma 3.9. *Let the notation be as above. Let $\mathcal{J}_C(\mathbb{F}_q)_\ell$ be the Sylow-ℓ subgroup of $\mathcal{J}_C(\mathbb{F}_q)$, and let $\{P_i, Q_j\}_{i,j}$ be the output of Algorithm 3.7. If $|P_i| = \ell^{\nu_i}$, then $\nu_i \leq \nu_{i+1}$. Let $P'_i = [\ell^{\nu_i - 1}](P_i)$, $1 \leq i \leq 4$. Define numbers $\alpha_{ij} \in \mathbb{Z}$ by $\hat{\varepsilon}_t(P'_i, Q_j) = \zeta^{\alpha_{ij}}$, where $\hat{\varepsilon}_t : \mathcal{J}_C(\mathbb{F}_q)[\ell] \times \mathcal{J}_C(\mathbb{F}_q)/\ell\mathcal{J}_C(\mathbb{F}_q) \to \mu_\ell = \langle \zeta \rangle$ is the reduced Tate pairing. Then one of the following cases holds.*

1. $\alpha_{11}\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\ell}$ *for* $i \neq j$.
2. $P_1 = \mathcal{O}$, $\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\ell}$ *for* $i \neq j$.
3. $P_1 = P_2 = \mathcal{O}$, $\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\ell}$ *for* $i \neq j$.
4. $P_1 = P_2 = P_3 = \mathcal{O}$.

Theorem 3.10. *Let the notation be as above. Algorithm 3.7 determines points P_1, P_2, P_3 and P_4 on $\mathcal{J}_C(\mathbb{F}_q)_\ell$, such that $\langle P_i \rangle_i = \bigoplus_i \langle P_i \rangle$.*

Proof. Let $P_i, Q_i \in \mathcal{J}_C(\mathbb{F}_q)$ be the output of Algorithm 3.7. Let $\ell^{\nu_i} = |P_i|$. Let $P'_i = [\ell^{\nu_i - 1}](P_i)$, $1 \leq i \leq 4$. Define numbers $\alpha_{ij} \in \mathbb{Z}$ by $\hat{\varepsilon}_t(P'_i, Q_j) = \zeta^{\alpha_{ij}}$. We only consider case 1 of Lemma 3.9, since the other cases follow similarly. We start by determining $\langle P_3 \rangle \cap \langle P_4 \rangle$. Assume that $P'_3 = [a](P'_4)$. Then

$$1 = \hat{\varepsilon}_t(P'_3, Q_4) = \hat{\varepsilon}_t([a](P'_4), Q_4) = \zeta^{a\alpha_{44}},$$

i.e. $a \equiv 0 \pmod{\ell}$. Hence, $\langle P_3 \rangle \cap \langle P_4 \rangle = \{\mathcal{O}\}$. Consider $\langle P_2 \rangle \cap \langle P_3, P_4 \rangle$. Assume $P_2' = [a](P_3') + [b](P_4')$. Then

$$1 = \hat{\varepsilon}_t(P_2', Q_3) = \hat{\varepsilon}_t([a](P_3'), Q_3) = \zeta^{a\alpha_{33}},$$

i.e. $a \equiv 0 \pmod{\ell}$. In the same way, $1 = \hat{\varepsilon}_t(P_2', Q_4) = \zeta^{b\alpha_{44}}$, i.e. also $b \equiv 0 \pmod{\ell}$. Hence, $\langle P_2 \rangle \cap \langle P_3, P_4 \rangle = \{\mathcal{O}\}$. Similarly, $\langle P_1 \rangle \cap \langle P_2, P_3, P_4 \rangle = \{\mathcal{O}\}$. Hence, $\langle P_i \rangle_i = \bigoplus_i \langle P_i \rangle$. □

3.2.2 Generators of $\mathfrak{J}_C(\mathbb{F}_q)[m]$

From Theorem 3.10 we get the following probabilistic algorithm to determine generators of the m-torsion subgroup $\mathfrak{J}_C(\mathbb{F}_q)[m]$, where m is the largest divisor of $|\mathfrak{J}_C(\mathbb{F}_q)|$ such that ℓ divides $q-1$ for every prime number ℓ dividing m.

Algorithm 3.11. *As input we are given the Jacobian $\mathfrak{J}_C$ of a genus two curve defined over a prime field $\mathbb{F}_q$, the number $N = |\mathfrak{J}_C(\mathbb{F}_q)|$ of $\mathbb{F}_q$-rational points on $\mathfrak{J}_C$, and the prime factors $\ell_1, \ldots, \ell_n$ of $\gcd(N, q-1)$. The algorithm outputs points $P_i \in \mathfrak{J}_C(\mathbb{F}_q)[m]$ such that $\mathfrak{J}_C(\mathbb{F}_q)[m] = \bigoplus_i \langle P_i \rangle$ in the following steps.*

1. *Set $P_i := \mathcal{O}$, $1 \le i \le 4$. For $\ell \in \{\ell_1, \ldots, \ell_n\}$ do the following:*
   a) *Use Algorithm 3.7 to determine points $\tilde{P}_i \in \mathfrak{J}_C(\mathbb{F}_q)_\ell$, $1 \le i \le 4$, such that $\langle \tilde{P}_i \rangle_i = \bigoplus_i \langle \tilde{P}_i \rangle$.*
   b) *If $\prod_i |\tilde{P}_i| < |\mathfrak{J}_C(\mathbb{F}_q)_\ell|$, then go to step 1a.*
   c) *Set $P_i := P_i + \tilde{P}_i$, $1 \le i \le 4$.*
2. *Output $\{P_1, P_2, P_3, P_4\}$.*

Remark 3.12. By remark 3.8, we expect Algorithm 3.7 to run in $O(\log \ell \log \frac{q-1}{\ell})$ field operations in $\mathbb{F}_q$. Hence, Algorithm 3.11 is an efficient, probabilistic algorithm to determine generators of the m-torsion subgroup $\mathfrak{J}_C(\mathbb{F}_q)[m]$, where m is the largest divisor of $|\mathfrak{J}_C(\mathbb{F}_q)|$ such that $\ell \mid q-1$ for every prime number $\ell \mid m$.

Remark 3.13. The strategy of Algorithm 3.7 can be applied to *any* finite, abelian group with a bilinear and non-degenerate pairing into a cyclic group. For the strategy to be efficient, the pairing must be efficiently computable, and the discrete logarithm problem in the cyclic group must be easy.

3.3 The general case $\ell \nmid q-1$

In section 3.2 we describe an algorithm based on the Tate pairing to determine generators of the subgroup $\mathfrak{J}_C(\mathbb{F}_q)[\ell]$ of points of order ℓ on the Jacobian, where ℓ is a number dividing $q-1$. The key ingredient of the algorithm is a "diagonalization" of a set of randomly chosen points $\{P_1,\dots,P_4,Q_1,\dots,Q_4\}$ on the Jacobian with respect to the reduced Tate pairing $\hat{\varepsilon}_t$; i.e. a modification of the set such that $\hat{\varepsilon}_t(P_i,Q_j)\neq 1$ if and only if $i=j$. This procedure is based on solving the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[\ell]$. Contrary to the special case where m divides $q-1$, it is in general infeasible to solve the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[m]$. Hence, in general the algorithm in section 3.2 does not apply.

In this section, we generalize the algorithm in section 3.2 to subgroups of points of prime order ℓ, where ℓ does not divide $q-1$. In order to do so, we must somehow alter the diagonalization step. We show and exploit the fact that the matrix representation on $\mathcal{J}_C[\ell]$ of the q-power Frobenius endomorphism on $\mathcal{J}_C$ can be described explicitly. This description enables us to describe the matrix representation of the Weil pairing on $\mathcal{J}_C[\ell]$ explicitly. Miller (2004) uses the Weil pairing to determine generators of $E(\mathbb{F}_{q^a})$, where E is an elliptic curve defined over a finite field $\mathbb{F}_q$ and $a\in\mathbb{N}$. The basic idea of his algorithm is to decide whether points on the curve are independent by means of calculating pairing values. The explicit description of the matrix representation of the Weil pairing lets us transfer this idea to Jacobians of genus two curves. Hereby, computations of discrete logarithms are avoided, yielding the desired altering of the diagonalization step.

If the Weil polynomial splits in distinct factors modulo ℓ, then the problem of determining a basis of the ℓ-torsion subgroup is trivially solved: the ℓ-torsion subgroup decomposes in four eigenspaces of the q-power Frobenius endomorphism, so to find a basis, simply choose an ℓ-torsion point and project it to the eigenspaces. A standard example is the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by $y^2=x^5+1$. The Weil polynomial of $\mathcal{J}_C$ is given by $P(X)=X^4+9$, the number of $\mathbb{F}_3$-rational points on $\mathcal{J}_C$ is $|\mathcal{J}_C(\mathbb{F}_3)|=P(1)=10$, and $P(X)$ factors modulo 5 as $P(X)\equiv(X-1)(X-2)(X-3)(X-4)\pmod 5$. But there *are* cases where the Weil polynomial does not split in distinct factors; cf. the following example.

Example 3.14. Consider the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by $y^2=x^5+2x^2+x+1$. The Weil polynomial of $\mathcal{J}_C$ is given by $P(X)=X^4+X^3-X^2+3X+9$, the number of $\mathbb{F}_3$-rational points on $\mathcal{J}_C$ is $|\mathcal{J}_C(\mathbb{F}_3)|=P(1)=13$, and $P(X)$ factors modulo 13 as $P(X)\equiv(X-1)(X-3)(X-4)^2\pmod{13}$.

3.3.1 Determining fields of definition

Freeman and Lauter (2008) consider the problem of determining the field of definition of the ℓ-torsion points on the Jacobian of a genus two curve, i.e. the problem of determining the full embedding degree k_0. They describe a probabilistic algorithm to determine if $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^\kappa})$ (see Freeman and Lauter, 2008, Algorithm 4.3). (Notice that Freeman and Lauter consider a Jacobian defined over a prime field $\mathbb{F}_p$, and (Freeman and Lauter, 2008, Algorithm 4.3) determines if $\mathfrak{J}_C[\ell^d] \subseteq \mathfrak{J}_C(\mathbb{F}_q)$, where $q = p^k$ and $d \in \mathbb{N}$. This algorithm is easily generalized to determine if $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^\kappa})$ for Jacobians defined over $\mathbb{F}_q$, $q = p^a$).

In most applications, a probabilistic algorithm to determine k_0 is sufficient. But we may have to compute k_0. To this end, consider a Jacobian $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$; cf. Definition 2.9 on page 21. Let ω be a q-Weil number of $\mathfrak{J}_C$. In cases relevant to pairing based cryptography, ℓ is most likely unramified in $\mathbb{Q}(\omega)$; cf. Remark 2.10 on page 21. But then the full embedding degree of $\mathfrak{J}_C$ with respect to ℓ can be computed directly by the following Algorithm 3.15 (obviously, in applications k_0 must be small enough for representation of and computations with points on $\mathfrak{J}_C(\mathbb{F}_{q^{k_0}})$ to be feasible. Hence, the algorithms presented are only relevant for applications if k_0 is "small").

Algorithm 3.15. *Consider a Jacobian $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let ω be a q-Weil number of $\mathfrak{J}_C$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$. Choose an upper bound $N \in \mathbb{N}$ of the full embedding degree k_0 of $\mathfrak{J}_C$ with respect to ℓ. If $k_0 \leq N$, then the following algorithm outputs k_0. If $k_0 > N$, then the algorithm outputs "$k_0 > N$".*

1. *Let $j = 1$.*
2. *If the Weil polynomial $P(X)$ of $\mathfrak{J}_C$ does not split in linear factors modulo ℓ, then φ is represented by a matrix M of the form* (2.2) *on $\mathfrak{J}_C[\ell]$. In this case, let $k_0 = \min\{\kappa \in k\mathbb{N}, \kappa \leq N, M^\kappa \equiv I \pmod{\ell}\}$, if the minimum exists. Else let $j = 0$.*
3. *If $P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}$, then do the following:*
   a) *If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then let $k_0 = \min\{\kappa \in k\mathbb{N}, \kappa \leq N, \alpha^\kappa \equiv 1 \pmod{\ell}\}$, if the minimum exists. Else let $j = 0$.*
   b) *If $\alpha \equiv 1, q \pmod{\ell}$, then let $k_0 = k$.*
   c) *If $\alpha \equiv q/\alpha \pmod{\ell}$, then let $k_0 = 2k$.*
4. *If $j = 0$ then output "$k_0 > N$". Else output k_0.*

Proof. First of all, recall that $k_0 \in k\mathbb{N}$; cf. Remark 1.5 on page 6. As usual, let φ be the q-power Frobenius endomorphism of $\mathfrak{J}_C$.

Assume at first that the Weil polynomial of $\mathfrak{J}_C$ does not split in linear factors modulo ℓ. Then φ is not diagonalizable on $\mathfrak{J}_C[\ell]$. Thus, φ is represented by a matrix M of the form (2.2) on $\mathfrak{J}_C[\ell]$. Since φ^{k_0} is the identity on $\mathfrak{J}_C[\ell]$, it is represented by the identity matrix I on $\mathfrak{J}_C[\ell]$. But φ^{k_0} is also represented by M^{k_0} on $\mathfrak{J}_C[\ell]$. So $M^{k_0} \equiv I \pmod{\ell}$. On the other hand, if $M^\kappa \equiv I \pmod{\ell}$ for some number $\kappa \leq k_0$, then φ^κ is the identity on $\mathfrak{J}_C[\ell]$, i.e. $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^\kappa})$. But then $\kappa = k_0$ by the definition of k_0. Hence, k_0 is the least number, such that $M^{k_0} \equiv I \pmod{\ell}$.

Now, assume the Weil polynomial splits in linear factors modulo ℓ. Then φ represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to an appropriate basis of $\mathfrak{J}_C[\ell]$; cf. Theorem 2.12 on page 23. The case $\alpha \not\equiv q/\alpha \pmod{\ell}$ is now obvious. If $\alpha \equiv q/\alpha \pmod{\ell}$, then $\alpha^2 \equiv q \pmod{\ell}$. So in this case, $k_0 = 2k$. □

Theorem 3.16. *Let the notation and assumptions be as in Algorithm 3.15. On input $\mathfrak{J}_C$, the Weil polynomial modulo ℓ and a number $N \in \mathbb{N}$, Algorithm 3.15 outputs either "$k_0 > N$" or the full embedding degree of $\mathfrak{J}_C$ with respect to ℓ in at most $O(N)$ number of operations in $\mathbb{F}_\ell$.*

Proof. If the Weil polynomial of $\mathfrak{J}_C$ does not split in linear factors modulo ℓ, then powers $\{M^k, (M^k)^2, \ldots, (M^k)^{\lfloor N/k \rfloor}\}$ of M modulo ℓ are computed; here, M is the matrix representation of the q-power Frobenius endomorphism on the ℓ-torsion subgroup $\mathfrak{J}_C[\ell]$. M is of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix}.$$

Hence, computing powers of M is equivalent to computing powers of $M' = \left[\begin{smallmatrix} 0 & -q \\ 1 & c \end{smallmatrix}\right]$ and powers of q. Computation of the product of two matrices $A, B \in \operatorname{Mat}_2(\mathbb{F}_\ell)$ takes 12 operations in $\mathbb{F}_\ell$, so computing the powers of M modulo ℓ takes $O(N)$ operations in $\mathbb{F}_\ell$.

Assume the Weil polynomial factors as $(X-1)(X-q)(X-\alpha)(X-q/\alpha)$ modulo ℓ. If $\alpha \equiv 1, q, q/\alpha \pmod{\ell}$, then no computations are needed. If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then powers $\{\alpha^k, (\alpha^k)^2, \ldots, (\alpha^k)^{\lfloor N/k \rfloor}\}$ of α modulo ℓ are computed; this takes $O(N)$ operations in $\mathbb{F}_\ell$. □

Remark 3.17. Recall that $q = p^a$ for some power $a \in \mathbb{N}$. Assume ℓ and p are of the same size. For small N (e.g. $N < 200$), a limit of $O(N)$ number of operations in $\mathbb{F}_\ell$ is a better result than the expected number of operations in $\mathbb{F}_p$ of (Freeman and Lauter, 2008, Algorithm 4.3) given by (Freeman and Lauter, 2008, Proposition 4.6). Furthermore, the algorithm of Freeman and Lauter (2008) only checks if a given number $\kappa \in \mathbb{N}$ is the full embedding degree k_0 of the Jacobian. Hence, to find k_0 using (Freeman and Lauter, 2008, Algorithm 4.3), we must apply it to every number in the set $\{\kappa \in k\mathbb{N} | \kappa \leq N\}$. Thus, we must multiply the number of expected operations in $\mathbb{F}_p$ with a factor $O(\lfloor N/k \rfloor)$. So if ℓ and p are of the same size, then Algorithm 3.15 is more efficient than (Freeman and Lauter, 2008, Algorithm 4.3). On the other hand, if $\ell \gg p$, then field operations in $\mathbb{F}_p$ is faster than field operations in $\mathbb{F}_\ell$, and (Freeman and Lauter, 2008, Algorithm 4.3) may be the more efficient one. Hence, the choice of algorithm to compute the full embedding degree depends strongly on the values of ℓ and p in the implementation.

3.3.2 Anti-symmetric pairings on the Jacobian

On $\mathcal{J}_C[\ell]$, a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times$$

exists, e.g. the Weil pairing; cf. Section 1.1.4 on page 5. Here, μ_ℓ is the group of ℓ^{th} roots of unity. Since ε is bilinear, it is given by

$$\varepsilon(x, y) = \zeta^{x^T \mathcal{E} y}, \tag{3.2}$$

for some matrix $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ with respect to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$.

Remark 3.18. To be more precise, the points x and y on the right hand of equation (3.2) should be replaced by their column vectors $[x]_\mathcal{B}$ and $[y]_\mathcal{B}$ with respect to $\mathcal{B}$. To ease notation, this has been omitted.

Let φ denote the q-power Frobenius endomorphism on $\mathcal{J}_C$. Since ε is Galois-invariant,

$$\forall x, y \in \mathcal{J}_C[\ell] : \varepsilon(x, y)^q = \varepsilon(\varphi(x), \varphi(y)).$$

This is equivalent to

$$\forall x, y \in \mathcal{J}_C[\ell] : q(x^T \mathcal{E} y) = (Mx)^T \mathcal{E}(My),$$

where M is the matrix representation of φ on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Since $(Mx)^T \mathcal{E}(My) = x^T M^T \mathcal{E} M y$, it follows that

$$\forall x, y \in \mathcal{J}_C[\ell] : x^T q\mathcal{E} y = x^T M^T \mathcal{E} M y,$$

or equivalently, that $q\mathcal{E} = M^T \mathcal{E} M$.

Now, let $\varepsilon(x_i, x_j) = \zeta^{a_{ij}}$. By anti-symmetry,

$$\mathcal{E} = \begin{bmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{bmatrix}.$$

At first, assume that φ is represented by a matrix of the form (2.2) with respect to $\mathcal{B}$. Since $M^T \mathcal{E} M = q\mathcal{E}$, it follows that

$$a_{14} - qa_{13} \equiv a_{23} - a_{24} \equiv a_{14}(c - (1+q)) \equiv a_{24}(c - (1+q)) \equiv 0 \pmod{\ell}.$$

Thus, $a_{13} \equiv a_{14} \equiv a_{23} \equiv a_{24} \equiv 0 \pmod{\ell}$, cf. Theorem 2.11 on page 22. So

$$\mathcal{E} = \begin{bmatrix} 0 & a_{12} & 0 & 0 \\ -a_{12} & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{34} \\ 0 & 0 & -a_{34} & 0 \end{bmatrix}.$$

Since ε is non-degenerate, $a_{12}^2 a_{34}^2 = \det \mathcal{E} \not\equiv 0 \pmod{\ell}$.

Finally, assume that φ is represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to $\mathcal{B}$. Then it follows from $M^T \mathcal{E} M = q\mathcal{E}$, that

$$a_{13}(\alpha - q) \equiv a_{14}(\alpha - 1) \equiv a_{23}(\alpha - 1) \equiv a_{24}(\alpha - q) \equiv 0 \pmod{\ell}.$$

If $\alpha \equiv 1, q \pmod{\ell}$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bi-cyclic. Hence the following theorem holds.

Theorem 3.19. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on $\mathcal{J}_C$. Choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by either a diagonal matrix* $\operatorname{diag}(1, q, \alpha, q/\alpha)$ *or a matrix of the form* (2.2) *with respect to $\mathcal{B}$. If the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of ℓ-torsion points on the Jacobian is cyclic, then all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices*

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$$

with respect to $\mathcal{B}$.

Remark 3.20. Let notation and assumptions be as in Theorem 3.19. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_C[\ell]$, and let ε be given by $\mathcal{E}_{a,b}$ with respect to a basis $\{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Then ε is given by $\mathcal{E}_{1,1}$ with respect to $\{a^{-1}x_1, x_2, b^{-1}x_3, x_4\}$.

Remark 3.21. In cases relevant to pairing based cryptography, we consider a prime divisor ℓ of size q^2. Assume ℓ is of size q^2. Then ℓ divides neither q nor $q - 1$. The number of $\mathbb{F}_q$-rational points on the Jacobian is approximately q^2. Thus, $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic in cases relevant to pairing based cryptography.

3.3.3 Generators of $\mathcal{J}_C[\ell]$

Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Assume the $\mathbb{F}_q$-rational subgroup of ℓ-torsion points $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic. Let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times.$$

In the following, frequently we will choose a random point $P \in \mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$ for some power $a \in \mathbb{N}$. This is done as follows: (1) Choose a random point $P \in \mathcal{J}_C(\mathbb{F}_{q^a})$. (2) Compute $P := [m](P)$, where $|\mathcal{J}_C(\mathbb{F}_{q^a})| = m\ell^s$ and $\ell \nmid m$. (3) Compute the order $|P| = \ell^{t(P)}$ of P. (4) If $t(P) > 0$, then let $P := [\ell^{t(P)-1}](P)$. Since the power $t(P)$ will be different for each point P, this procedure does not define a group homomorphism from $\mathcal{J}_C(\mathbb{F}_{q^a})$ to $\mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$. Thus, the image of points uniformly distributed in $\mathcal{J}_C(\mathbb{F}_{q^a})$ will not necessarily be uniformly distributed in $\mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$. A method of choosing points uniformly at random is given in (Freeman and Lauter, 2008, section 5.3), but it leads to a significant extra cost. In practice we believe it is better to not use the method in Freeman and Lauter (2008), even though this means one might need to sample a few extra points.

We consider the cases where $\ell \nmid \tau_k$ and where $\ell \mid \tau_k$ separately.

The case $\ell \nmid \tau_k$

If ℓ does not divide τ_k, then $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 2.1 on page 17. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and extend $\{x_1\}$ to a basis $\{x_1, y_2\}$ of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$, where $\varphi(y_2) = qy_2$. Let $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ be a random point. If $x_2' \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, then choose another random point $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. After two trials, $x_2' \notin \mathcal{J}_C(\mathbb{F}_q)[\ell]$ with probability $1 - 1/\ell^2$. Hence, we may ignore the case where $x_2' \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$. Write $x_2' = \alpha_1 x_1 + \alpha_2 y_2$. Then

$$\mathcal{O} \neq x_2 = x_2' - \varphi(x_2') = \alpha_2(1-q)y_2 \in \langle y_2 \rangle,$$

i.e. $\varphi(x_2) = qx_2$. Now, let $\mathcal{J}_C[\ell] \simeq \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \oplus W$, where W is a φ-invariant submodule of rank two. Choose a random point $x_3' \in \mathcal{J}_C[\ell]$. Since $x_3' - \varphi(x_3') \in \langle y_2 \rangle \oplus W$, we may assume that $x_3' \in \langle y_2 \rangle \oplus W$. But then

$$x_3 = qx_3' - \varphi(x_3') \in W$$

as above. If $\varphi(x_3') = qx_3'$, then $x_3' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. This will only happen with probability $1/\ell^2$. Hence, we may ignore this case. Notice that

$$\mathcal{J}_C[\ell] = \langle x_1, x_2, x_3, \varphi(x_3) \rangle \text{ if and only if } \varepsilon(x_3, \varphi(x_3)) \neq 1;$$

cf. Theorem 3.19 on the facing page.

Assume $\varepsilon(x_3, \varphi(x_3)) = 1$. Then x_3 is an eigenvector of φ. Let $\varphi(x_3) = \alpha x_3$. Then the Weil polynomial of $\mathcal{J}_C$ is given by

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}$$

modulo ℓ. Assume $\alpha \equiv q/\alpha \pmod{\ell}$. Then $\alpha^2 \equiv q \pmod{\ell}$, and it follows that the characteristic polynomial of φ^k is given by

$$P_k(X) \equiv (X-1)^2(X+1)^2 \equiv X^4 - 2q^k X^2 + q^{2k} \pmod{\ell}$$

modulo ℓ. But then $\ell \mid \tau_k$. This is a contradiction. So $\alpha \not\equiv q/\alpha \pmod{\ell}$. Therefore, we can extend $\{x_1, x_2, x_3\}$ to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 3.20 on page 40.

Now, choose a random point $x \in \mathcal{J}_C[\ell]$. Write $x = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4$. Then $\varepsilon(x_3, x) = \zeta^{\alpha_4}$. So $\varepsilon(x_3, x) \neq 1$ if and only if ℓ does not divide α_4. On the other hand, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only ℓ does not divide α_4. Thus, if ℓ does not divide τ_k, then the following Algorithm 3.22 outputs generators of $\mathcal{J}_C[\ell]$ with probability at least $1 - 1/\ell^n$.

Algorithm 3.22. *On input a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, the numbers ℓ, q, k and τ_k, the full embedding degree k_0 of $\mathcal{J}_C$ with respect to ℓ and a number $n \in \mathbb{N}$, if ℓ does not divide τ_k, then the following algorithm outputs a basis of $\mathcal{J}_C[\ell]$ or "failure".*

1. *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ and $x_3' \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$; compute $x_3 = q(x_3' - \varphi(x_3')) - \varphi(x_3' - \varphi(x_3'))$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
2. *Let $i = j = 0$. While $i < n$ do the following:*
   a) *Choose a random point $x_4 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
   b) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

The case $\ell \mid \tau_k$

Assume ℓ divides τ_k. Then $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 2.2 on page 17. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and let $y_2 \in \mathcal{J}_C[\ell]$ be a point with $\varphi(y_2) = qy_2$. Write $\mathcal{J}_C[\ell] = \langle x_1, y_2 \rangle \oplus W$, where W is a φ-invariant submodule of rank two; cf. the proof of Theorem 2.11 on page 22. Let $\{y_3, y_4\}$

be a basis of W, such that φ is represented on $\mathcal{J}_C[\ell]$ with respect to the basis $\mathcal{B} = \{x_1, y_2, y_3, y_4\}$ by either a diagonal matrix

$$M_1 = \operatorname{diag}(1, q, \alpha, q/\alpha),$$

or a matrix of the form

$$M_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix},$$

where $c \not\equiv q+1 \pmod{\ell}$; cf. Theorem 2.11 on page 22.

Now, choose a random point $z \in \mathcal{J}_C[\ell]$. Since $z - \varphi(z) \in \langle y_2, y_3, y_4\rangle$, we may assume that $z \in \langle y_2, y_3, y_4\rangle$. Write $z = \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Assume at first that φ is represented on $\mathcal{J}_C[\ell]$ by M_1 with respect to $\mathcal{B}$. Then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 \alpha y_3 + \alpha_4 (q/\alpha) y_4) \\ &= \alpha_3 (q-\alpha) y_3 + \alpha_4 (q - q/\alpha) y_4; \end{aligned}$$

so $qz - \varphi(z) \in \langle y_3, y_4\rangle$. If $qz - \varphi(z) = 0$, then it follows that $q \equiv 1 \pmod{\ell}$. This contradicts the choice of the Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$ in this case. Now assume that φ is represented on $\mathcal{J}_C[\ell]$ by M_2 with respect to $\mathcal{B}$. Then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 y_4 + \alpha_4(-q y_3 + c y_4)) \\ &= q(\alpha_3 + \alpha_4) y_3 + (\alpha_4 q - \alpha_3 - \alpha_4 c) y_4; \end{aligned}$$

so again $qz - \varphi(z) \in \langle y_3, y_4\rangle$. If $qz - \varphi(z) = 0$, then it follows that $c \equiv q+1 \pmod{\ell}$. This is a contradiction. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$ also in this case.

Choose random points $x_3, x_4 \in W$. Write $x_i = \alpha_{i3} y_3 + \alpha_{i4} y_4$ for $i = 3, 4$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 3.20 on page 40. But then $\varepsilon(x_3, x_4) = \zeta^{\alpha_{33}\alpha_{44} - \alpha_{34}\alpha_{43}}$. Hence, $\varepsilon(x_3, x_4) = 1$ if and only if $\alpha_{33}\alpha_{44} \equiv \alpha_{34}\alpha_{43} \pmod{\ell}$. So $\varepsilon(x_3, x_4) \neq 1$ with probability $1 - 1/\ell$. Hence, we have a procedure to find a basis of W.

Until now, we have found points $x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3, x_4 \in W$, such that $W = \langle x_3, x_4\rangle$. Now, choose a random point $x_2 \in \mathcal{J}_C[\ell]$. Write $x_2 = \alpha_1 x_1 + \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Then $\varepsilon(x_1, x_2) = \zeta^{\alpha_2}$, i.e. $\varepsilon(x_1, x_2) = 1$ if and only if $\alpha_2 \equiv 0 \pmod{\ell}$. Thus, with probability $1 - 1/\ell$, the set $\{x_1, x_2, x_3, x_4\}$ is a basis of $\mathcal{J}_C[\ell]$.

Summing up, if ℓ divides τ_k, then the following Algorithm 3.23 on the following page outputs generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$.

Algorithm 3.23. *On input a Jacobian $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, the numbers ℓ, q, k and τ_k, the full embedding degree k_0 of $\mathfrak{J}_C$ with respect to ℓ and a number $n \in \mathbb{N}$, if ℓ divides τ_k, then the following algorithm outputs a basis of $\mathfrak{J}_C[\ell]$ or "failure".*

1. *Choose a random point $\mathcal{O} \neq x_1 \in \mathfrak{J}_C(\mathbb{F}_q)[\ell]$.*
2. *Let $i = j = 0$. While $i < n$ do the following:*
   a) *Choose a random point $x_2 \in \mathfrak{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
   b) *If $\varepsilon(x_1, x_2) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$, then output "failure" and stop.*
4. *Let $i = j = 0$. While $i < n$ do the following:*
   a) *Choose random points $y_3, y_4 \in \mathfrak{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
   b) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
5. *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

The complete algorithm

Combining Algorithm 3.22 and 3.23, we obtain the desired algorithm to find generators of $\mathfrak{J}_C[\ell]$.

Algorithm 3.24. *On input a Jacobian $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, the numbers ℓ, q, k and τ_k, the full embedding degree k_0 of $\mathfrak{J}_C$ with respect to ℓ and a number $n \in \mathbb{N}$, the following algorithm outputs a basis of $\mathfrak{J}_C[\ell]$ or "failure".*

1. *If $\ell \nmid \tau_k$, run Algorithm 3.22 on input $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$.*
2. *If $\ell \mid \tau_k$, run Algorithm 3.23 on input $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$.*

Theorem 3.25. *Let $\mathfrak{J}_C$ be a $\mathbb{J}(\ell, q, k, \tau_k)$-Jacobian of full embedding degree k_0 with respect to ℓ. On input $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$, Algorithm 3.24 outputs generators of $\mathfrak{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$. We expect Algorithm 3.24 to run in*

$$O\left(\log \ell \log \frac{q^{k_0} - 1}{\ell} {k_0}^3 \log k_0 \log q\right)$$

field operations in $\mathbb{F}_q$ (ignoring $\log \log q$ factors).

Proof. We must compare the cost of the steps in Algorithm 3.24. From (Freeman and Lauter, 2008, proof of Proposition 4.6), (Frey and Rück, 1994, proof of Corollary 1) and Menezes, van Oorschot *et al.* (1997) we get the following estimates: (1) Choosing a random point on $\mathfrak{J}_C(\mathbb{F}_{q^a})$ for some power $a \in \mathbb{N}$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$, and computing a multiple $[m](P)$ of a point $P \in \mathcal{J}_C(\mathbb{F}_{q^a})$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$. (2) Evaluating the q^a-power Frobenius endomorphism of the Jacobian on a point $P \in \mathcal{J}_C[\ell]$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$. (3) Evaluating the Tate pairing on two point of $\mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$ takes $O(\log \ell)$ field operations in $\mathbb{F}_{q^{k_0}}$. The Weil pairing can be computed by computing two Tate pairings, raising the results to the power $\frac{q^{k_0}-1}{\ell}$ and finally computing the quotient of these numbers (see Galbraith, 2005). The exponentiation takes $O(\log \frac{q^{k_0}-1}{\ell})$ field operations in $\mathbb{F}_{q^{k_0}}$, and a division takes $O({k_0}^2)$ field operations in $\mathbb{F}_{q^{k_0}}$. Hence, evaluating the Weil pairing on two point on $\mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$ takes $O(\log \ell) O(\log \frac{q^{k_0}-1}{\ell}) O({k_0}^2)$ field operations in $\mathbb{F}_{q^{k_0}}$. (4) By using fast multiplication techniques, one field operation in $\mathbb{F}_{q^a}$ can be computed in $O(\log q^a \log\log q^a) = O(a \log a \log q)$ (ignoring $\log\log q$ factors).

We see that the pairing computation is the most expensive step in Algorithm 3.24. Thus, Algorithm 3.24 runs in $O(\log \ell \log \frac{q^{k_0}-1}{\ell} {k_0}^3 \log k_0 \log q)$ field operations in $\mathbb{F}_q$ (ignoring $\log\log q$ factors). $\square$

Freeman and Lauter (2008) gives an algorithm to determine *generators* for the ℓ-torsion subgroup (see Freeman and Lauter, 2008, Algorithm 4.3). This algorithm runs in expected time $O(k^2 \log k (\log p)^2 \ell^{s-4} \sqrt{-\log \varepsilon})$, where the number s is given by $|\mathcal{J}_C(\mathbb{F}_{q^{k_0}})| = m\ell^s$ and $\ell \nmid m$, and ε is the rate of failure. Hence, if $s > 4$, then Algorithm 3.24 is by far more efficient than (Freeman and Lauter, 2008, Algorithm 4.3).

3.3.4 A small example

To illustrate the steps of Algorithm 3.24 on the preceding page, we consider a small example. We will focus on the most common case where $\ell \nmid \tau_k$; i.e. we will compute the steps of Algorithm 3.22 on page 42 explicitly.

Consider the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by

$$y^2 = x^5 + 2x^2 + x + 1.$$

As usual, we let φ denote the 3-power Frobenius endomorphism on $\mathcal{J}_C$.

The Weil polynomial of $\mathcal{J}_C$ is given by

$$P(X) = X^4 + X^3 - X^2 + 3X + 9.$$

The number of $\mathbb{F}_3$-rational points on $\mathcal{J}_C$ is $|\mathcal{J}_C(\mathbb{F}_3)| = P(1) = 13$, and the embedding degree of $\mathcal{J}_C(\mathbb{F}_3)$ with respect to $\ell = 13$ is $k = 3$. We find that

$$P(X) \equiv (X-1)(X-3)(X-4)^2 \pmod{13}.$$

Hence, $\mathcal{J}_C(\mathbb{F}_{3^3})[13]$ is bicyclic, and the full embedding degree of $\mathcal{J}_C(\mathbb{F}_3)$ with respect to $\ell = 13$ is $k_0 = 6$. In particular, $\mathcal{J}_C[13] \subseteq \mathcal{J}_C(\mathbb{F}_{3^6})$.

The complex roots of $P(X)$ are given by ω_1, $\omega_2 = \bar{\omega}_1$, ω_3 and $\omega_4 = \bar{\omega}_3$, where

$$\omega_1 = -\frac{1}{4} + \frac{1}{4}\sqrt{29} + \frac{i}{4}\sqrt{18 + 2\sqrt{29}}$$

and

$$\omega_3 = -\frac{1}{4} - \frac{1}{4}\sqrt{29} + \frac{i}{4}\sqrt{18 - 2\sqrt{29}}.$$

Therefore, the characteristic polynomials $P_3(X)$ and $P_6(X)$ of the 3^3- and the 3^6-power Frobenius endomorphisms are given by

$$P_3(X) = \prod_i (X - \omega_i^3) = X^4 + 13X^3 + 89X^2 + 351X + 729$$

and

$$P_6(X) = \prod_i (X - \omega_i^6) = X^4 + 9X^3 + 253X^2 + 6561X + 531441.$$

In particular, the number of $\mathbb{F}_{3^3}$- and $\mathbb{F}_{3^6}$-rational points on the Jacobian $\mathcal{J}_C$ are $|\mathcal{J}_C(\mathbb{F}_{3^3})| = P_3(1) = 1183$ and $|\mathcal{J}_C(\mathbb{F}_{3^6})| = P_6(1) = 538265$.

Now, let $s = 13$ and $\tau_k = 29$. Then

$$P_3(X) = X^4 + sX^3 + (2 \cdot 3^3 + (s^2 - \tau_k)/4)X^2 + 3^3 \cdot sX + 3^6.$$

Thus, $\mathcal{J}_C$ is a $\mathbb{J}(13, 3, 3, 29)$-Jacobian. Since 13 does not divide $\tau_k = 29$, we use Algorithm 3.22 to find generators of $\mathcal{J}_C[13]$.

We start by choosing points $x_1 \in \mathcal{J}_C(\mathbb{F}_3)[13]$ and $x_2 \in \mathcal{J}_C(\mathbb{F}_{3^3})[13]$:

$$\begin{aligned} x_1 &= (0,1) + (-1,1) - 2P_\infty, \\ x_2 &= (\alpha + 2, \alpha^2 + 2\alpha + 1) + (2\alpha^2 + 2, 2\alpha^2 + \alpha + 1) - 2P_\infty. \end{aligned}$$

Here, α is a root of $X^3 + X^2 + X + 2$ modulo 3. Then we choose a point $x_3' \in \mathcal{J}_C(\mathbb{F}_{3^6})[13]$:

$$\begin{aligned} x_3' = (&\beta^4 + \beta^3 + 2\beta^2 + 2\beta + 2, \beta^5 + \beta^4 + \beta^2 + 2\beta) \\ &+ (2\beta^5 + 2\beta^2 + 2, \beta^5 + 2\beta^3 + \beta) - 2P_\infty. \end{aligned}$$

Here, β is a root of $X^6 + X^5 + 2X^4 + X^3 + X^2 + 2X + 2$ modulo 3. Finally, we compute $x_3 = x_3' - \varphi^3(x_3')$:

$$\begin{aligned} x_3 = (&2\beta^5 + 2\beta^4 + \beta^2 + \beta, \beta^5 + \beta^4 + \beta^3 + \beta + 2\beta^2) \\ &+ (2\beta^5 + 2\beta^4 + \beta^2 + \beta + 2, 2\beta^5 + 2\beta^3 + 2) - 2P_\infty. \end{aligned}$$

Now we compute $y = \varphi(x_3)$:

$$\begin{aligned} y = {} & (2\beta^5 + 2\beta^4 + \beta^2 + \beta, 2\beta^5 + 2\beta^4 + 2\beta + \beta^2 + 2\beta^3) \\ & (2\beta^5 + 2\beta^4 + \beta^2 + \beta + 2, \beta^5 + \beta^3 + 1) - 2P_\infty. \end{aligned}$$

Let $\varepsilon : \mathcal{J}_C[13] \times \mathcal{J}_C[13] \to \mu_{13}$ be the Weil pairing. Since $\varepsilon(x_3, y) = 1$, we know that $y \in \langle x_3 \rangle$. Hence, we must choose another point $x_4' \in \mathcal{J}_C(\mathbb{F}_{3^6})[13]$:

$$\begin{aligned} x_4' = {} & (\beta^2 + \beta + 1, 2\beta^5 + 2\beta^4 + 2\beta^2 + 2\beta + 2) \\ & (2\beta^5 + \beta^4 + 2\beta^3, 2\beta^5 + 2\beta^4 + 2\beta^3 + 2\beta^2 + \beta) - 2P_\infty. \end{aligned}$$

We compute $x_4 = x_4' - \varphi^3(x_4')$:

$$\begin{aligned} x_4 = {} & (2\beta^5 + 2\beta^4 + \beta^2 + \beta + 1, \beta^5 + \beta^3 + \beta^2 + 1) \\ & (2\beta^5 + 2\beta^4 + \beta^2 + \beta, \beta^5 + \beta^4 + \beta^3 + 2\beta^2 + \beta) - 2P_\infty. \end{aligned}$$

Since $\varepsilon(x_3, x_4) \neq 1$, $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ is a basis of $\mathcal{J}_C[13]$.

3.3.5 Implementation issues

To check if ℓ ramifies in $\mathbb{Q}(\omega_k)$ in the case where ℓ divides τ_k, a priori we need to find a q^k-Weil number ω_k of the Jacobian $\mathcal{J}_C$. On Jacobians generated by the *complex multiplication method* (Eisenträger and Lauter, 2007; Gaudry, Houtmann *et al.*, 2005; Weng, 2003), we know the Weil numbers in advance. Hence, Algorithm 3.24 on page 44 is particularly well suited for such Jacobians.

Fortunately, most likely ℓ does not divide τ_k, and then we do not have to find a q^k-Weil number (ℓ divides a random number $n \in \mathbb{Z}$ with vanishing probability $1/\ell$). And if the Weil polynomial splits in distinct linear factors modulo ℓ, then we do not even have to compute τ_k. To see this, assume that the Weil polynomial of $\mathcal{J}_C$ splits as

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell},$$

where $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$. Let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$, and let $P_k(X)$ be the characteristic polynomial of φ^k. Then

$$P_k(X) \equiv (X-1)^2(X-\alpha^k)(X-1/\alpha^k) \pmod{\ell}.$$

If ℓ divides τ_k, then $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 2.2 on page 17. But then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ divides } \tau_k \text{ if and only if } \alpha^k \equiv 1 \pmod{\ell}. \tag{3.3}$$

Assume $\alpha^k \equiv 1 \pmod{\ell}$. Then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ ramifies in } \mathbb{Q}(\omega^k) \text{ if and only if } \omega^k \notin \mathbb{Z}. \tag{3.4}$$

See (Neukirch, 1999, Proposition 8.3, p. 47). Here, ω is a q-Weil number of $\mathcal{J}_C$.

Consider the case where $\alpha^k \equiv 1 \pmod{\ell}$ and $\omega^k \in \mathbb{Z}$. Then $\omega = \sqrt{q}e^{in\pi/k}$ for some $n \in \mathbb{Z}$ with $0 < n < k$. Assume k divides mn for some $m < k$. Then $\omega^{2m} = q^m \in \mathbb{Z}$. Since the q-power Frobenius endomorphism is the identity on the $\mathbb{F}_q$-rational points on the Jacobian, it follows that $\omega^{2m} \equiv 1 \pmod{\ell}$. Hence, $q^m \equiv 1 \pmod{\ell}$, i.e. k divides m. This is a contradiction. So n and k has no common divisors. Let $\xi = \omega^2/q = e^{in2\pi/k}$. Then ξ is a primitive k^{th} root of unity, and $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\omega)$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] \leq 4$ and $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(k)$, where ϕ is the Euler phi function, it follows that $k \leq 12$. Hence,

$$\text{if } \alpha^k \equiv 1 \pmod{\ell}, \text{ then } \omega^k \in \mathbb{Z} \text{ if and only if } k \leq 12. \tag{3.5}$$

The criteria (3.3), (3.4) and (3.5) provides the following efficient algorithm to check whether a given Jacobian is of type $\mathbb{J}(\ell, q, k, \tau_k)$, and whether ℓ divides τ_k.

Algorithm 3.26. *Let $\mathcal{J}_C$ be the Jacobian of a genus two curve C. Assume that the odd prime number ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, and that ℓ divides neither q nor $q-1$. Let k be the multiplicative order of q modulo ℓ.*

1. *Compute the Weil polynomial $P(X)$ of $\mathcal{J}_C$. Let $P(X) \equiv \prod_{i=1}^{4}(X - \alpha_i) \pmod{\ell}$.*
2. *If $\alpha_i^k \not\equiv 1 \pmod{\ell}$ for an $i \in \{1,2,3,4\}$, then output "$\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$ and ℓ does not divide τ_k" and stop.*
3. *If $k > 12$ then output "$\mathcal{J}_C \notin \mathbb{J}(\ell, q, k, \tau_k)$" and stop.*
4. *Output "$\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$ and ℓ divides τ_k" and stop.*

Appendices

Appendix A

Generators of Jacobians of hyperelliptic curves

This appendix contains the preprint (Ravnshøj, 2007a).

GENERATORS OF JACOBIANS OF HYPERELLIPTIC CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. This paper provides a probabilistic algorithm to determine generators of the m-torsion subgroup of the Jacobian of a hyperelliptic curve of genus two.

1. Introduction

Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$, and $\mathcal{J}_C$ the Jacobian of C. Consider the rational subgroup $\mathcal{J}_C(\mathbb{F}_p)$. $\mathcal{J}_C(\mathbb{F}_p)$ is a finite abelian group, and

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}/n_3\mathbb{Z} \oplus \mathbb{Z}/n_4\mathbb{Z},$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p-1$. Frey and Rück (1994) shows that if $m \mid p-1$, then the discrete logarithm problem in the rational m-torsion subgroup $\mathcal{J}_C(\mathbb{F}_p)[m]$ of $\mathcal{J}_C(\mathbb{F}_p)$ can be reduced to the corresponding problem in $\mathbb{F}_p^\times$ (Frey and Rück, 1994, corollary 1). In the proof of this result it is claimed that the non-degeneracy of the Tate pairing can be used to determine whether r random elements of the finite group $\mathcal{J}_C(\mathbb{F}_p)[m]$ in fact is an independent set of generators of $\mathcal{J}_C(\mathbb{F}_p)[m]$. This paper provides an explicit, probabilistic algorithm to determine generators of $\mathcal{J}_C(\mathbb{F}_p)[m]$.

In short, the algorithm outputs elements γ_i of the Sylow-ℓ subgroup Γ_ℓ of the rational subgroup $\Gamma = \mathcal{J}_C(\mathbb{F}_p)$, such that $\Gamma_\ell = \bigoplus_i \langle\gamma_i\rangle$ in the following steps:

(1) Choose random elements $\gamma_i \in \Gamma_\ell$ and $h_j \in \mathcal{J}_C(\mathbb{F}_p)$, $i, j \in \{1, \dots, 4\}$.
(2) Use the non-degeneracy of the tame Tate pairing τ to *diagonalize* the sets $\{\gamma_i\}_i$ and $\{h_j\}_j$ with respect to τ; i.e. modify the sets such that $\tau(\gamma_i, h_j) = 1$ if $i \neq j$ and $\tau(\gamma_i, h_i)$ is an ℓ^{th} root of unity.
(3) If $\prod_i |\gamma_i| < |\Gamma_\ell|$ then go to step 1.
(4) Output the elements γ_1, γ_2, γ_3 and γ_4.

The key ingredient of the algorithm is the diagonalization in step 2; this process will be explained in section 5.

We will write $\langle\gamma_i | i \in I\rangle = \langle\gamma_i\rangle_i$ and $\bigoplus_{i\in I}\langle\gamma_i\rangle = \bigoplus_i\langle\gamma_i\rangle$ if the index set I is clear from the context.

2. Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. In the rest of this

Date: April 25, 2007. The author is a Ph.D.-student at the Department of Mathematical Sciences, Faculty of Science, University of Aarhus.

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 14Q05, 94A60.

Key words and phrases. Jacobians, hyperelliptic curves, complex multiplication, cryptography.

Research supported in part by a Ph.D. grant from CRYPTOMAThIC.

paper, let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p > 2$. By the Riemann-Roch theorem there exists an embedding $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

$$y^2 = f(x),$$

where $f \in \mathbb{F}_p[x]$ is of degree six and have no multiple roots (see Cassels and Flynn, 1996, 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

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

Consider the subgroup $\mathcal{J}_C(\mathbb{F}_p) < \mathcal{J}_C$ of $\mathbb{F}_p$-rational elements. There exist numbers n_i, such that

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}/n_3\mathbb{Z} \oplus \mathbb{Z}/n_4\mathbb{Z}, \tag{1}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p-1$ (see Frey and Lange, 2006, proposition 5.78, p. 111). We wish to determine generators of the m-torsion subgroup $\mathcal{J}_C(\mathbb{F}_p)[m] < \mathcal{J}_C(\mathbb{F}_p)$, where $m \mid |\mathcal{J}_C(\mathbb{F}_p)|$ is the largest number such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

3. Finite abelian groups

Miller (2004) shows the following theorem.

Theorem 1. *Let G be a finite abelian group of torsion rank r. Then for $s \geq r$ the probability that a random s-tuple of elements of G generates G is at least*

$$\frac{C_r}{\log\log|G|}$$

if $s = r$, and at least C_s if $s > r$, where $C_s > 0$ is a constant depending only on s (and not on $|G|$).

Proof. (Miller, 2004, theorem 3, p. 251) □

Combining theorem 1 and equation (1), we expect to find generators of $\Gamma[m]$ by choosing 4 random elements $\gamma_i \in \Gamma[m]$ in approximately $\frac{\log\log|\Gamma[m]|}{C_4}$ attempts.

To determine whether the generators are independent, i.e. if $\langle\gamma_i\rangle_i = \bigoplus_i\langle\gamma_i\rangle$, we need to know the subgroups of a cyclic ℓ-group G. These are determined uniquely by the order of G, since

$$\{0\} < \langle\ell^{n-1}g\rangle < \langle\ell^{n-2}g\rangle < \cdots < \langle\ell g\rangle < G$$

are the subgroups of the group $G = \langle g\rangle$ of order ℓ^n. The following corollary is an immediate consequence of this observation.

Corollary 2. *Let U_1 and U_2 be cyclic subgroups of a finite group G. Assume U_1 and U_2 are ℓ-groups. Let $\langle u_i\rangle < U_i$ be the subgroups of order ℓ. Then*

$$U_1 \cap U_2 = \{e\} \iff \langle u_1\rangle \cap \langle u_2\rangle = \{e\}.$$

Here $e \in G$ is the neutral element.

4. The tame Tate pairing

Let $\Gamma = \mathcal{J}_C(\mathbb{F}_p)$ be the rational subgroup of the Jacobian. Consider a number $\lambda \mid \gcd(|\Gamma|, p-1)$. Let $g \in \Gamma[\lambda]$ and $h = \sum_i a_i P_i \in \Gamma$ be divisors with no points in common, and let

$$\overline{h} \in \Gamma/\lambda\Gamma$$

denote the class containing the divisor h. Furthermore, let $f \in \mathbb{F}_p(C)$ be a rational function on C with divisor $\operatorname{div}(f) = \lambda g$. Set $f(h) = \prod_i f(P_i)^{a_i}$. Then

$$e_\lambda(g, \overline{h}) = f(h)$$

is a well-defined pairing $\Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^\lambda$, the *Tate pairing*; cf. Galbraith (2005). Raising to the power $\frac{p-1}{\lambda}$ gives a well-defined element in the subgroup $\mu_\lambda < \mathbb{F}_p^\times$ of the λ^{th} roots of unity. This pairing

$$\tau_\lambda : \Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \mu_\lambda$$

is called the *tame Tate pairing.*

Since the class $\overline{h}$ is represented by the element $h \in \Gamma$, we will write $\tau_\lambda(g, h)$ instead of $\tau_\lambda(g, \overline{h})$. Furthermore, we will omit the subscript λ and just write $\tau(g, h)$, since the value of λ will be clear from the context.

Hess (2004) gives a short and elementary proof of the following theorem.

Theorem 3. *The tame Tate pairing τ is bilinear and non-degenerate.*

Corollary 4. *For every element $g \in \Gamma$ of order λ an element $h \in \Gamma$ exists, such that $\mu_\lambda = \langle \tau(g, h) \rangle$.*

Proof. (Silverman, 1986, corollary 8.1.1., p. 98) gives a similar result for elliptic curves and the Weil pairing. The proof of this result only uses that the pairing is bilinear and non-degenerate. Hence it applies to corollary 4. □

Remark 5. In the following we only need the existence of the element $h \in \Gamma$, such that $\mu_\lambda = \langle \tau(g, h) \rangle$; we do not need to find it.

5. Generators of $\Gamma[m]$

As in the previous section, let $\Gamma = \mathcal{J}_C(\mathbb{F}_p)$ be the rational subgroup of the Jacobian. We are searching for elements $\gamma_i \in \Gamma[m]$ such that $\Gamma[m] = \bigoplus_i \langle \gamma_i \rangle$. As an abelian group, $\Gamma[m]$ is the direct sum of its Sylow subgroups. Hence, we only need to find generators of the Sylow subgroups of $\Gamma[m]$.

Set $N = |\Gamma|$ and let $\ell \mid \gcd(N, p-1)$ be a prime number. Choose four random elements $\gamma_i \in \Gamma$. Let $\Gamma_\ell < \Gamma$ be the Sylow-ℓ subgroup of Γ, and set $N_\ell = |\Gamma_\ell|$. Then $\frac{N}{N_\ell}\gamma_i \in \Gamma_\ell$. Hence, we may assume that $\gamma_i \in \Gamma_\ell$. If all the elements γ_i are equal to zero, then we choose other elements $\gamma_i \in \Gamma$. Hence, we may assume that some of the elements γ_i are non-zero.

Let $|\gamma_i| = \lambda_i$, and re-enumerate the γ_i's such that $\lambda_i \le \lambda_{i+1}$. Since some of the γ_i's are non-zero, we may choose an index $\nu \le 4$, such that $\lambda_\nu \ne 1$ and $\lambda_i = 1$ for $i < \nu$. Choose λ_0 minimal such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Then $\mathbb{F}_p$ contains an element ζ of order λ. Now set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$, $\nu \le i \le 4$. Then $g_i \in \Gamma[\lambda]$, $\nu \le i \le 4$. Finally, choose four random elements $h_i \in \Gamma$.

Let

$$\tau : \Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \langle \zeta \rangle$$

be the tame Tate pairing. Define remainders α_{ij} modulo λ by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}}.$$

By corollary 4, for any of the elements g_i we can choose an element $h \in \Gamma$, such that $|\tau(g_i, h)| = \lambda$. Assume that $\Gamma/\lambda\Gamma = \langle \overline{h}_1, \overline{h}_2, \overline{h}_3, \overline{h}_4 \rangle$. Then $\overline{h} = \sum_i q_i \overline{h}_i$, and so

$$\tau(g_i, h) = \zeta^{\alpha_{i1}q_1 + \alpha_{i2}q_2 + \alpha_{i3}q_3 + \alpha_{i4}q_4}.$$

If $\alpha_{ij} \equiv 0 \pmod{\ell}$, $1 \le j \le 4$, then $|\tau(g_i, h)| < \lambda$. Hence, if $\Gamma/\lambda\Gamma = \langle \overline{h}_1, \overline{h}_2, \overline{h}_3, \overline{h}_4 \rangle$, then for all $i \in \{\nu, \dots, 4\}$ we can choose a $j \in \{1, \dots, 4\}$, such that $\alpha_{ij} \not\equiv 0 \pmod{\ell}$.

Enumerate the h_i such that $\alpha_{44} \not\equiv 0 \pmod{\ell}$. Now assume a number $j < 4$ exists, such that $\alpha_{4j} \not\equiv 0 \pmod{\lambda}$. Then $\zeta^{\alpha_{4j}} = \zeta^{\beta_1 \alpha_{44}}$, and replacing h_j with $h_j - \beta_1 h_4$ gives $\alpha_{4j} \equiv 0 \pmod{\lambda}$. So we may assume that

$$\alpha_{41} \equiv \alpha_{42} \equiv \alpha_{43} \equiv 0 \pmod{\lambda} \qquad \text{and} \qquad \alpha_{44} \not\equiv 0 \pmod{\ell}.$$

Assume similarly that a number $j < 4$ exists, such that $\alpha_{j4} \not\equiv 0 \pmod{\lambda}$. Now set $\beta_2 \equiv \alpha_{44}^{-1}\alpha_{j4} \pmod{\lambda}$. Then $\tau(g_j - \beta_2 g_4, h_4) = 1$. So we may also assume that

$$\alpha_{14} \equiv \alpha_{24} \equiv \alpha_{34} \equiv 0 \pmod{\lambda}.$$

Repeating this process recursively, we may assume that

$$\alpha_{ij} \equiv 0 \pmod{\lambda} \qquad \text{and} \qquad \alpha_{44} \not\equiv 0 \pmod{\ell}.$$

Again $\nu \le i \le 4$ and $1 \le j \le 4$.

The discussion above is formalized in the following algorithm.

Algorithm 1. As input we are given a hyperelliptic curve C of genus two defined over a prime field $\mathbb{F}_p$, the number $N = |\Gamma|$ of $\mathbb{F}_p$-rational elements of the Jacobian, and a prime factor $\ell \mid \gcd(N, p-1)$. The algorithm outputs elements $\gamma_i \in \Gamma_\ell$ of the Sylow-ℓ subgroup Γ_ℓ of Γ, such that $\langle \gamma_i \rangle_i = \bigoplus_i \langle \gamma_i \rangle$ in the following steps.

(1) Compute the order N_ℓ of the Sylow-ℓ subgroup of Γ.
(2) Choose elements $\gamma_i \in \Gamma$, $i \in I := \{1, 2, 3, 4\}$. Set $\gamma_i := \frac{N}{N_\ell}\gamma_i$.
(3) Choose elements $h_j \in \Gamma$, $j \in J := \{1, 2, 3, 4\}$.
(4) Set $K := \{1, 2, 3, 4\}$.
(5) For k' from 0 to 3 do the following:
  (a) Set $k := 4 - k'$.
  (b) If $\gamma_i = 0$, then set $I := I \setminus \{i\}$. If $|I| = 0$, then go to step 2.
  (c) Compute the orders $\lambda_\kappa := |\gamma_\kappa|$, $\kappa \in K$. Re-enumerate the γ_κ's such that $\lambda_\kappa \le \lambda_{\kappa+1}$, $\kappa \in K$. Set $I := \{5 - |I|, 6 - |I|, \dots, 4\}$.
  (d) Set $\nu := \min(I)$, and choose λ_0 minimal such that $\lambda := \frac{\lambda_\nu}{\lambda_0} \mid p - 1$. Set $g_\kappa := \frac{\lambda_\kappa}{\lambda}\gamma_\kappa$, $\kappa \in I \cap K$.
    (i) If $g_k = 0$, then go to step 6.
    (ii) If $\tau(g_k, h_j)^{\lambda/\ell} = 1$ for all $j \le k$, then go to step 3.
  (e) Choose a primitive λ^{th} root of unity $\zeta \in \mathbb{F}_p$. Compute α_{kj} and $\alpha_{\kappa k}$ from $\tau(g_k, h_j) = \zeta^{\alpha_{kj}}$ and $\tau(g_\kappa, h_k) = \zeta^{\alpha_{\kappa k}}$, $1 \le j < k$, $\kappa \in I \cap K$. Re-enumerate $h_1, \dots, h_k$ such that $\alpha_{kk} \not\equiv 0 \pmod{\ell}$.
  (f) For $1 \le j < k$, set $\beta \equiv \alpha_{kk}^{-1}\alpha_{kj} \pmod{\lambda}$ and $h_j := h_j - \beta h_k$.
  (g) For $\kappa \in I \cap K \setminus \{k\}$, set $\beta \equiv \alpha_{kk}^{-1}\alpha_{\kappa k} \pmod{\lambda}$ and $\gamma_\kappa := \gamma_\kappa - \beta\frac{\lambda_k}{\lambda_\kappa}\gamma_k$.
  (h) Set $K := K \setminus \{k\}$.
(6) Output γ_1, γ_2, γ_3 and γ_4.

Remark 6. Algorithm 1 consists of a small number of

(1) calculations of orders of elements $\gamma \in \Gamma_\ell$,
(2) multiplications of elements $\gamma \in \Gamma$ with numbers $a \in \mathbb{Z}$,
(3) additions of elements $\gamma_1, \gamma_2 \in \Gamma$,
(4) evaluations of pairings of elements $\gamma_1, \gamma_2 \in \Gamma$ and
(5) solving the discrete logarithm problem in $\mathbb{F}_p$, i.e. to determine α from ζ and $\xi = \zeta^\alpha$.

By (Miller, 2004, proposition 9), the order $|\gamma|$ of an element $\gamma \in \Gamma_\ell$ can be calculated in time $O(\log^3 N_\ell)\mathcal{A}_\Gamma$, where $\mathcal{A}_\Gamma$ is the time for adding two elements of Γ. A multiple $a\gamma$ or a sum $\gamma_1 + \gamma_2$ is computed in time $O(\mathcal{A}_\Gamma)$. By Frey and Rück (1994), the pairing $\tau(\gamma_1, \gamma_2)$ of two elements $\gamma_1, \gamma_2 \in \Gamma$ can be evaluated in time $O(\log N_\ell)$. Finally, by Pohlig and Hellmann (1978) the discrete logarithm problem in $\mathbb{F}_p$ can be solved in time $O(\log p)$. We may assume that addition in Γ is easy, i.e. that $\mathcal{A}_\Gamma < O(\log p)$. Hence algorithm 1 runs in expected time $O(\log p)$.

Careful examination of algorithm 1 gives the following lemma.

Lemma 7. *Let Γ_ℓ be the Sylow-ℓ subgroup of Γ, $\ell \mid p-1$. Algorithm 1 determines elements $\gamma_i \in \Gamma_\ell$ and $h_i \in \Gamma$, $1 \le i \le 4$, such that one of the following cases holds.*

(1) $\alpha_{11}\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{1, 2, 3, 4\}$.
(2) $\gamma_1 = 0$, $\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{2, 3, 4\}$.
(3) $\gamma_1 = \gamma_2 = 0$, $\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{3, 4\}$.
(4) $\gamma_1 = \gamma_2 = \gamma_3 = 0$.

If $|\gamma_i| = \lambda_i$, then $\lambda_i \le \lambda_{i+1}$. Set $\nu = \min\{i|\lambda_i \ne 1\}$, and define λ_0 as the least number, such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$, $\nu \le i \le 4$. Then the numbers α_{ij} above are determined by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}},$$

where τ is the tame Tate pairing $\Gamma[\lambda] \times \Gamma/\lambda\Gamma \to \mu_\lambda = \langle\zeta\rangle$.

Theorem 8. *Algorithm 1 determines elements γ_1, γ_2, γ_3 and γ_4 of the Sylow-ℓ subgroup of Γ, $\ell \mid p-1$, such that $\langle\gamma_i\rangle_i = \bigoplus_i \langle\gamma_i\rangle$.*

Proof. Choose elements $\gamma_i, h_i \in \Gamma$ such that the conditions of lemma 7 are fulfilled. Set $\lambda_i = |\gamma_i|$, and let $\nu = \min\{i|\lambda_i \ne 1\}$. Define λ_0 as the least number, such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$. Then the α_{ij}'s from lemma 7 are determined by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}}.$$

We only consider case 1 of lemma 7, since the other cases follow similarly. We start by determining $\langle\gamma_3\rangle \cap \langle\gamma_4\rangle$. Assume that $g_3 = ag_4$. Then

$$1 = \tau(g_3, h_4) = \tau(ag_4, h_4) = \zeta^{a\alpha_{44}},$$

i.e. $a \equiv 0 \pmod{\lambda}$. Hence $\langle\gamma_3\rangle \cap \langle\gamma_4\rangle = \{0\}$. Then we determine $\langle\gamma_2\rangle \cap \langle\gamma_3, \gamma_4\rangle$. Assume $g_2 = ag_3 + bg_4$. Then

$$1 = \tau(g_2, h_3) = \tau(ag_3, h_3) = \zeta^{a\alpha_{33}},$$

i.e. $a \equiv 0 \pmod{\lambda}$. In the same way,

$$1 = \tau(g_2, h_4) = \zeta^{b\alpha_{44}},$$

i.e. $b \equiv 0 \pmod{\lambda}$. Hence $\langle\gamma_2\rangle \cap \langle\gamma_3, \gamma_4\rangle = \{0\}$. Similarly $\langle\gamma_1\rangle \cap \langle\gamma_2, \gamma_3, \gamma_4\rangle = \{0\}$. Hence $\langle\gamma_i\rangle_i = \bigoplus_i \langle\gamma_i\rangle$. □

From theorem 8 we get the following probabilistic algorithm to determine generators of the m-torsion subgroup $\Gamma[m] < \Gamma$, where $m \mid |\Gamma|$ is the largest divisor of $|\Gamma|$ such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

Algorithm 2. As input we are given a hyperelliptic curve C of genus two defined over a prime field $\mathbb{F}_p$, the number $N = |\Gamma|$ of $\mathbb{F}_p$-rational elements of the Jacobian, and the prime factors $p_1, \dots, p_n$ of $\gcd(N, p-1)$. The algorithm outputs elements $\gamma_i \in \Gamma[m]$ such that $\Gamma[m] = \bigoplus_i \langle \gamma_i \rangle$ in the following steps.

(1) Set $\gamma_i := 0$, $1 \le i \le 4$. For $\ell \in \{p_1, \dots, p_n\}$ do the following:
   (a) Use algorithm 1 to determine elements $\tilde{\gamma}_i \in \Gamma_\ell$, $1 \le i \le 4$, such that $\langle \tilde{\gamma}_i \rangle_i = \bigoplus_i \langle \tilde{\gamma}_i \rangle$.
   (b) If $\prod_i |\tilde{\gamma}_i| < |\Gamma_\ell|$, then go to step 1a.
   (c) Set $\gamma_i := \gamma_i + \tilde{\gamma}_i$, $1 \le i \le 4$.
(2) Output γ_1, γ_2, γ_3 and γ_4.

Remark 9. By remark 6, algorithm 2 has expected running time $O(\log p)$. Hence algorithm 2 is an efficient, probabilistic algorithm to determine generators of the m-torsion subgroup $\Gamma[m] < \Gamma$, where $m \mid |\Gamma|$ is the largest divisor of $|\Gamma|$ such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

Remark 10. The strategy of algorithm 1 can be applied to *any* finite, abelian group Γ with bilinear, non-degenerate pairings into cyclic groups. For the strategy to be efficient, the pairings must be efficiently computable, and the discrete logarithm problem in the cyclic groups must be easy.

References

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.

G. Frey and T. Lange. Varieties over Special Fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 87–113. Chapman & Hall/CRC, 2006.

G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, vol. 62, pp. 865–874, 1994.

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

F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, no. 82, pp. 28–32, 2004.

V.S. Miller. The Weil Pairing and Its Efficient Calculation. *J. Cryptology*, no. 17, pp. 235–261, 2004.

S. Pohlig and M. Hellmann. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory*, vol. 24, pp. 106–110, 1978.

J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

E-mail address: cr@imf.au.dk

Appendix B

p-torsion of genus two curves over prime fields of characteristic p

This appendix contains the preprint (Ravnshøj, 2007c).

p-TORSION OF GENUS TWO CURVES OVER PRIME FIELDS OF CHARACTERISTIC p

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Consider the Jacobian of a hyperelliptic genus two curve defined over a prime field of characteristic p and with complex multiplication. In this paper we show that the p-Sylow subgroup of the Jacobian is either trivial or of order p.

1. Introduction

In elliptic curve cryptography it is essential to know the number of points on the curve. Cryptographically we are interested in elliptic curves with large cyclic subgroups. Such elliptic curves can be constructed. The construction is based on the theory of complex multiplication, studied in detail by Atkin and Morain (1993). It is referred to as the *CM method*.

Koblitz (1989) suggested the use of hyperelliptic curves to provide larger group orders. Therefore constructions of hyperelliptic curves are interesting. The CM method for elliptic curves has been generalized to hyperelliptic curves of genus two by Spallek (1994), and efficient algorithms have been proposed by Weng (2003) and Gaudry *et al* (2005).

Both algorithms take as input a primitive, quartic CM field K (see section 3 for the definition of a CM field), and give as output a hyperelliptic genus two curve C defined over a prime field $\mathbb{F}_p$. A prime number p is chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$, where $\mathfrak{O}_K$ is the ring of integers of K. We have $K = \mathbb{Q}(\eta)$ and $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{D})$, where $\eta = i\sqrt{a + b\xi}$ and

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

In this paper, the following theorem is established.

Theorem 1. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$. Assume that $\mathrm{End}(C) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field as defined in definition 5, and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as above. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

2. Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. Let C be a hyperelliptic

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 11G15, 14Q05, 94A60.
Key words and phrases. Jacobians, hyperelliptic curves, complex multiplication, cryptography.
Research supported in part by a PhD grant from CRYPTOMAThIC.

curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p > 2$. By the Riemann-Roch theorem there exists an embedding $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

$$y^2 = f(x),$$

where $f \in \mathbb{F}_p[x]$ is of degree six and have no multiple roots (see Cassels and Flynn, 1996, chapter 1).

The set of principal divisors $\mathcal{P}(C)$ on C constitutes a subgroup of the degree 0 divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

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

Since C is defined over $\mathbb{F}_p$, the mapping $(x, y) \mapsto (x^p, y^p)$ is a morphism on C. This morphism induces the p-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. The characteristic polynomial $P(X)$ of φ is of degree four (Tate, 1966, Theorem 2, p. 140), and by the definition of $P(X)$ (see Lang, 1959, pp. 109–110),

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

i.e. the number of $\mathbb{F}_p$-rational points on the Jacobian is determined by $P(X)$.

3. CM fields

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *complex multiplication*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field*, and if $\mathrm{End}(E) \simeq \mathfrak{O}_K$, then E is said to have *CM by $\mathfrak{O}_K$*. More generally a CM field is defined as follows.

Definition 2 (CM field)**.** A number field K is a CM field, if K is a totally imaginary, quadratic extension of a totally real number field K_0.

In this paper only CM fields of degree $[K : \mathbb{Q}] = 4$ are considered. Such a field is called a *quartic* CM field.

Remark 3. Consider a quartic CM field K. Let $K_0 = K \cap \mathbb{R}$ be the real subfield of K. Then K_0 is a real, quadratic number field, $K_0 = \mathbb{Q}(\sqrt{D})$. By a basic result on quadratic number fields, the ring of integers of K_0 is given by $\mathfrak{O}_{K_0} = \mathbb{Z} + \xi\mathbb{Z}$, where

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

Since K is a totally imaginary, quadratic extension of K_0, a number $\eta \in K$ exists, such that $K = K_0(\eta)$, $\eta^2 \in K_0$. The number η is totally imaginary, and we may assume that $\eta = i\eta_0$, $\eta_0 \in \mathbb{R}$. Furthermore we may assume that $\eta^2 \in \mathfrak{O}_{K_0}$; so $\eta = i\sqrt{a + b\xi}$, where $a, b \in \mathbb{Z}$.

Let C be a hyperelliptic curve of genus two. Then C is said to have CM by $\mathfrak{O}_K$, if $\mathrm{End}(C) \simeq \mathfrak{O}_K$. The structure of K determines whether C is irreducible. More precisely, the following theorem holds.

Theorem 4. *Let C be a hyperelliptic curve of genus two with* $\mathrm{End}(C) \simeq \mathfrak{O}_K$*, where K is a quartic CM field. Then C is reducible if, and only if, $K/\mathbb{Q}$ is Galois with Galois group* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. (Shimura, 1998, Proposition 26, p. 61). □

Theorem 4 motivates the following definition.

Definition 5 (Primitive, quartic CM field)**.** A quartic CM field K is called primitive if either $K/\mathbb{Q}$ is not Galois, or $K/\mathbb{Q}$ is Galois with cyclic Galois group.

The CM method for constructing curves of genus two with prescribed endomorphism ring is described in detail by Weng (2003) and Gaudry *et al* (2005). In short, the CM method is based on the construction of the class polynomials of a primitive, quartic CM field K with real subfield K_0 of class number $h(K_0) = 1$. The prime number p has to be chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$. By Weng (2003) we may assume that $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$.

4. The p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$

Let K be a primitive, quartic CM field with real subfield $K_0 = \mathbb{Q}(\sqrt{D})$ of class number $h(K_0) = 1$. Cf. Remark 3 we may write $K = \mathbb{Q}(\eta)$, where $\eta = i\sqrt{a+b\xi}$ and

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2,3 \mod 4. \end{cases}$$

Let p be a prime number such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$. Let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. Assume that the p-power Frobenius under this isomorphism is given by the number

$$\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta, \quad c_i \in \mathbb{Z}. \tag{1}$$

Since the p-power Frobenius is of degree p, we know that $\omega\overline{\omega} = p$.

Remark 6. If $c_2 = 0$ in (1), then $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and K is not primitive. So $c_2 \neq 0$.

The characteristic polynomial $P(X)$ of the Frobenius is given by

$$P(X) = \prod_{i=1}^{4}(X - \omega_i),$$

where ω_i are the conjugates of ω. Since the conjugates of ω are given by $\omega_1 = \omega$, $\omega_2 = \overline{\omega}_1$, ω_3 and $\omega_4 = \overline{\omega}_3$, where $\omega_3 = c_1 + c_2\xi' + (c_3 + c_4\xi')\eta'$, $\eta' = i\sqrt{a+b\xi'}$ and

$$\xi' = \begin{cases} -\sqrt{D}, & \text{if } D \equiv 2,3 \mod 4 \\ \frac{1-\sqrt{D}}{2}, & \text{if } D \equiv 2,3 \mod 4 \end{cases}$$

it follows that

$$P(X) = X^4 - 4c_1X^3 + (2p + 4(c_1^2 - c_2^2D))X^2 - 4c_1pX + p^2,$$

if $D \equiv 2,3 \mod 4$, and

$$P(X) = X^4 - 2cX^3 + (2p + c^2 - c_2^2D)X^2 - 2cpX + p^2,$$

if $D \equiv 1 \mod 4$. Here, $c = 2c_1 + c_2$. We notice that $4 \mid P(1) = |\mathfrak{J}_C(\mathbb{F}_p)|$. This observation leads to the following lemma.

Lemma 7. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p > 5$. Assume that $\mathrm{End}(C) \simeq \mathfrak{O}_K$ and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

Proof. Assume $p^2 \mid N = |\mathfrak{J}_C(\mathbb{F}_p)|$. Since $|\omega_i| = \sqrt{p}$, we know that

$$N = P(1) = \prod_{i=1}^{4}(1-\omega_i) \leq (1+\sqrt{p})^4 = p^2 + 4p\sqrt{p} + 6p + 4\sqrt{p} + 1.$$

Hence, $\frac{N}{p^2} < 4$ for $p > 5$. But then $4 \nmid N$, a contradiction. So $p^2 \nmid N$, i.e. the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is of order at most p. □

Now consider the case $p \leq 5$. Assume at first that $D \equiv 2, 3 \mod 4$. Since $\omega_1\overline{\omega}_1 = \omega_2\overline{\omega}_2 = p$, we know that $|c_1 \pm c_2\sqrt{D}| \leq \sqrt{p}$. Thus,

$$\begin{aligned} |c_2\sqrt{D}| &= \frac{1}{2}\left|c_1 + c_2\sqrt{D} - \left(c_1 - c_2\sqrt{D}\right)\right| \\ &\leq \frac{1}{2}\left(\left|c_1 + c_2\sqrt{D}\right| + \left|c_1 - c_2\sqrt{D}\right|\right) \\ &\leq \sqrt{p}. \end{aligned}$$

Similarly we see that $|c_1| \leq \sqrt{p}$. Assume that $D > 5$. Then $|c_2| \leq \sqrt{\frac{p}{D}} < 1$. So $c_2 = 0$, since $c_2 \in \mathbb{Z}$. This contradicts remark 6, i.e. $D \leq 5$. Now assume that $D = 2$. Then $c_2 \leq \sqrt{\frac{p}{2}} \leq \sqrt{\frac{5}{2}}$, i.e. $c_2 \in \{0, \pm 1\}$. Therefore it follows by calculating N for each of the possible values of c_1 and c_2, that if $p^2 \mid N$, then $c_2 = 0$. This is again a contradiction. So if $D = 2$, then $p^2 \nmid N$. Similar it follows that if $D = 3$, then $p^2 \nmid N$.

Finally assume that $D \equiv 1 \pmod 4$. Then it follows from $\omega_1\overline{\omega}_1 = \omega_2\overline{\omega}_2 = p$ that $|c_1 + c_2\frac{1 \pm \sqrt{D}}{2}| \leq \sqrt{p}$. Thus, $|c_2\sqrt{D}| \leq 2\sqrt{p}$ and $|2c_1 - c_2| \leq 2\sqrt{p}$. Assume that $D > 20$. Then $|c_2| < 2\sqrt{\frac{5}{20}} = 1$, i.e. $c_2 = 0$, a contradiction. So $D \leq 20$. By calculating N for each of the possible values of p, D, c and c_2 it follows that $p^2 \nmid N$ also in this case. Hence the following lemma is established.

Lemma 8. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p \leq 5$. Assume that* $\mathrm{End}(C) \simeq \mathfrak{O}_K$ *and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

Summing up, the following theorem holds.

Theorem 9. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$. Assume that* $\mathrm{End}(C) \simeq \mathfrak{O}_K$ *and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

References

A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, vol. 61, pp. 29–68, 1993.

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.

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng. The p-adic CM-Method for Genus 2. 2005. `http://arxiv.org`.

N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1, pp. 139–150, 1989.

S. LANG. *Abelian Varieties.* Interscience, 1959.

G. SHIMURA. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, 1998.

A.-M. SPALLEK. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen.* PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

J. TATE. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, vol. 2, pp. 134–144, 1966.

A. WENG. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, vol. 72, pp. 435–458, 2003.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF AARHUS, NY MUNKEGADE, BUILDING 1530, DK-8000 AARHUS C

E-mail address: cr@imf.au.dk

Appendix C

Non-cyclic subgroups of Jacobians of genus two curves

This appendix contains the preprint (Ravnshøj, 2008b).

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* $U = \mathcal{J}_C(\mathbb{F}_p)[\ell]$, $V = \ker(\varphi - p) \cap \mathcal{J}_C[\ell]$ *and* φ *is the p-power Frobenius endomorphism on* $\mathcal{J}_C$.

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* $\mathcal{J}_C$ *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* $q^m - 1$.

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

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* $\mathcal{J}_C$. *Assume* $|\mathcal{J}_C(\mathbb{F}_{q^m})|$ *is even. Then*

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

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 $k \le 12$, cf. Galbraith [5] and Rubin and Silverberg [18]. If $\ell^2 \nmid |\mathcal{J}_C(\mathbb{F}_q)|$, 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 $P_m(X) = X^4 + sX^3 + tX^2 + sq^mX + q^{2m}$, 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,

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

$\square$

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 $\mathcal{J}_C[\ell]$ 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 $\mathcal{J}_C$. Then

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

Since ω_m is a q^m-Weil number of $\mathcal{J}_C$, we know that ω_m^k is a q^{mk}-Weil number of $\mathcal{J}_C$. 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 $\mathcal{J}_C[\ell]$. 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 $\mathcal{J}_C$. Assume $|\mathcal{J}_C(\mathbb{F}_{q^m})|$ is even. Then*

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

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, $\mathcal{J}_C[2] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{4m}})$ 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 $\mathcal{J}_C[2] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{6m}})$ 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 $\mathcal{J}_C$ 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. □

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`

Appendix D

Generators for the ℓ-torsion subgroup of Jacobians of genus two curves

This appendix contains the paper (Ravnshøj, 2008c).

Generators for the ℓ-torsion subgroup of Jacobians of Genus Two Curves

Christian Robenhagen Ravnshøj

Department of Mathematical Sciences
University of Aarhus
Ny Munkegade
Building 1530
DK-8000 Aarhus C
cr@imf.au.dk

Abstract. We give an explicit description of the matrix representation of the Frobenius endomorphism on the Jacobian of a genus two curve on the subgroup of ℓ-torsion points. By using this description, we can describe the matrix representation of the Weil-pairing on the subgroup of ℓ-torsion points explicitly. Finally, the explicit description of the Weil-pairing provides us with an efficient, probabilistic algorithm to find generators of the subgroup of ℓ-torsion points on the Jacobian of a genus two curve.

1 Introduction

In [13], 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 [14] then proposed using Jacobians of hyperelliptic curves. After Boneh and Franklin [1] proposed an identity based cryptosystem by using the Weil-pairing on an elliptic curve, pairings have been of great interest to cryptography [8]. The next natural step was to consider pairings on Jacobians of hyperelliptic curves.

Galbraith *et al* [9] survey the recent research on pairings on Jacobians of hyperelliptic curves. Their conclusion is that, for most applications, elliptic curves provide more efficient solutions than hyperelliptic curves. One way of making pairing based cryptography on Jacobians of hyperelliptic curves interesting is to exploit the full torsion subgroup of the Jacobian of a hyperelliptic curve. In particular, cryptographic applications of pairings on groups which require three or more generators will be interesting. If such applications are found, the next natural problem will be to give efficient methods to choose points in the particular subgroups. The present paper addresses this problem.

Let $\mathcal{J}_C$ be the Jacobian of a genus two curve defined over $\mathbb{F}_q$. In [5, Algorithm 4.3], Freeman and Lauter describe a probabilistic algorithm to determine generators of the subgroup $\mathcal{J}_C[\ell]$ of points of order ℓ, but the algorithm is incomplete in the sense that the output only *probably* is a generating set - it is not tested whether the output in fact *is* a generating set. Furthermore, if the output happens to be a generating set, it still may not be a *basis* of $\mathcal{J}_C[\ell]$.

In [21], the author describes an algorithm based on the Tate-pairing to determine a basis of the subgroup $\mathcal{J}_C(\mathbb{F}_q)[m]$ of points of order m on the Jacobian, where m is a number dividing $q-1$. The key ingredient of the algorithm is a "diagonalization" of a set of randomly chosen points $\{P_1, \ldots, P_4, Q_1, \ldots, Q_4\}$ on the Jacobian with respect to the (reduced) Tate-pairing ε; i.e. a modification of the set such that $\varepsilon(P_i, Q_j) \neq 1$ if and only if $i = j$. This procedure is based on solving the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[m]$. Contrary to the special case where m divides $q-1$, it is in general infeasible to solve the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[m]$. Hence, in general the algorithm in [21] does not apply.

Results

In the present paper, we generalize the algorithm in [21] to subgroups of points of prime order ℓ, where ℓ does not divide $q-1$. In order to do so, we must somehow alter the diagonalization step. We show and exploit the fact that the matrix representation on $\mathcal{J}_C[\ell]$ of the q-power Frobenius endomorphism on $\mathcal{J}_C$ can be described explicitly. This description enables us to describe the matrix representation of the Weil pairing on $\mathcal{J}_C[\ell]$ explicitly. Miller [18] uses the Weil pairing to determine generators of $E(\mathbb{F}_{q^a})$, where E is an elliptic curve defined over a finite field $\mathbb{F}_q$ and $a \in \mathbb{N}$. The basic idea of his algorithm is to decide whether points on the curve are independent by means of calculating pairing values. The explicit description of the matrix representation of the Weil pairing lets us transfer this idea to Jacobians of genus two curves. Hereby, computations of discrete logarithms are avoided, yielding the desired altering of the diagonalization step.

Setup Consider the Jacobian $\mathcal{J}_C$ of 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 $\mathcal{J}_C$, and with ℓ dividing neither q nor $q-1$. Assume that the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ is cyclic. Let k be the multiplicative order of q modulo ℓ, and let k_0 be the least number, such that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{k_0}})$. (Obviously, in applications k_0 must be small enough for representation of and computations with points on $\mathcal{J}_C(\mathbb{F}_{q^{k_0}})$ to be feasible. Hence, the algorithms presented are only efficient if k_0 is "small"). Write the characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ as $P_k(X) = X^4 + sX^3 + (2q^k + (s^2 - \tau_k)/4)X^2 + sq^kX + q^{2k}$. Let $\omega_k \in \mathbb{C}$ be a root of $P_k(X)$. Finally, if ℓ divides τ_k, we assume that ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark 1. Notice that most likely, in cases relevant to pairing based cryptography the considered Jacobian of a genus two curve fulfills these assumptions. Cf. Remark 13 and 21.

The algorithm Let $\mathcal{J}_C$, ℓ, q, k, k_0 and τ_k be given as in the above setup. Note that the numbers k and k_0 are *computed* from $\mathcal{J}_C$, ℓ and q - they are *not* chosen. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, it is implicitly assumed that $\mathcal{J}_C$ contains points of order ℓ defined over $\mathbb{F}_q$, i.e. that $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is non-trivial. Notice also that we assume to know the Weil polynomial (see Section 3) of $\mathcal{J}_C$ already - it is *not* computed in the algorithm. In particular, we know τ_k.

Now, first of all we notice that in the above setup the q-power Frobenius endomorphism φ on $\mathcal{J}_C$ can be represented on $\mathcal{J}_C[\ell]$ by either a diagonal matrix or a matrix of a particular form with respect to an appropriate basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$; cf. Theorem 14. (In fact, to show this we do not need the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ to be cyclic). From this observation it follows that all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$$

with respect to $\mathcal{B}$; cf. Theorem 19. By using this description of the pairings, the desired algorithm is given as follows.

Algorithm 16. *Let the notation and assumptions be as in the above setup. On input the Jacobian $\mathcal{J}_C$, the numbers ℓ, q, k, k_0, τ_k and a number $n \in \mathbb{N}$, the following algorithm outputs a basis of $\mathcal{J}_C[\ell]$ or "failure".*

1. *If ℓ does not divide τ_k, then do the following:*
   - (a) *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ and $x_3' \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$ (cf. Section 8 for details on how to choose points); compute $x_3 = q(x_3' - \varphi(x_3')) - \varphi(x_3' - \varphi(x_3'))$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
   - (b) *Let $i = j = 0$. While $i < n$ do the following:*
     - i. *Choose a random point $x_4 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
     - ii. *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
   - (c) *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*
2. *If ℓ divides τ_k, then do the following:*
   - (a) *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$.*
   - (b) *Let $i = j = 0$. While $i < n$ do the following:*
     - i. *Choose a random point $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
     - ii. *If $\varepsilon(x_1, x_2) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
   - (c) *If $j = 0$, then output "failure" and stop.*
   - (d) *Let $i = j = 0$. While $i < n$ do the following:*
     - i. *Choose random points $y_3, y_4 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
     - ii. *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
   - (e) *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

Algorithm 24 finds generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - {}^1\!/\!_{\ell^n})^2$ and in expected running time $O\left(\log \ell \log \frac{q^{k_0}-1}{\ell} {k_0}^3 \log k_0 \log q\right)$ field operations in $\mathbb{F}_q$ (ignoring $\log \log q$ factors); this is contained in Theorem 25. The algorithm [5, Algorithm 4.3] runs in expected time $O(k^2 \log k (\log p)^2 \ell^{s-4} \sqrt{-\log \epsilon})$, where the number s is given by $|\mathcal{J}_C(\mathbb{F}_{q^{k_0}})| = m\ell^s$ and $\ell \nmid m$, and ϵ is the rate of failure. Hence, if $s > 4$, then Algorithm 24 is by far more efficient than [5, Algorithm 4.3]. [5, Algorithm 4.3] is used in [5] to compute endomorphism rings of Jacobians of genus two curves, and this in turn has applications for generating Jacobians of genus two curves using the CRT version of the CM method [4]. Hence, Algorithm 24 also has applications for generating Jacobians of genus two curves.

If the Weil polynomial splits in distinct factors modulo ℓ, then the problem of determining a basis of the ℓ-torsion subgroup is trivially solved: the ℓ-torsion subgroup decomposes in four eigenspaces of the q-power Frobenius endomorphism, so to find a basis, simply choose an ℓ-torsion point and project it to the eigenspaces. A standard example is the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by $y^2 = x^5 + 1$. The Weil polynomial of $\mathcal{J}_C$ is given by $P(X) = X^4 + 9$, the number of $\mathbb{F}_3$-rational points on $\mathcal{J}_C$ is $|\mathcal{J}_C(\mathbb{F}_3)| = P(1) = 10$, and $P(X)$ factors modulo 5 as $P(X) \equiv (X-1)(X-2)(X-3)(X-4) \pmod 5$. But there *are* cases where the Weil polynomial does not split in distinct factors; cf. the following example.

Example 1. Consider the Jacobian $\mathcal{J}_C$ of the curve over $\mathbb{F}_3$ given by

$$y^2 = x^5 + 2x^2 + x + 1 \ .$$

The Weil polynomial of $\mathcal{J}_C$ is given by $P(X) = X^4 + X^3 - X^2 + 3X + 9$, the number of $\mathbb{F}_3$-rational points on $\mathcal{J}_C$ is $|\mathcal{J}_C(\mathbb{F}_3)| = P(1) = 13$, and $P(X)$ factors modulo 13 as $P(X) \equiv (X-1)(X-3)(X-4)^2 \pmod{13}$.

Remark 2. To implement Algorithm 24, we need to find the *Weil polynomial* of the Jacobian. On Jacobians generated by the *complex multiplication method* [23, 10, 4], we know the Weil polynomial in advance. Hence, Algorithm 24 is particularly well suited for such Jacobians.

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. [2, 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

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

The Jacobian is an abelian group. We write the group law additively, and denote the zero element of the Jacobian by $\mathcal{O}$.

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. [15, 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. [11].

Definition 3 (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 4 (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 k_0, such that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{k_0}})$.*

Remark 5. If $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{k_0}})$, then $\ell \mid q^{k_0} - 1$; cf. [15, Theorem 6, p. 109] and [6, Proposition 5.78, p. 111]. Hence, the full embedding degree is a multiple of the embedding degree.

3 The Frobenius endomorphism

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; cf. [15, pp. 109–110]. $P(X)$ 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 [15, pp. 109–110]); i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$.

Definition 6 (Weil number). *Let notation be as above. Let $P_k(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on $\mathfrak{J}_C$. A complex number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$ is called a* q^m-Weil number *of $\mathfrak{J}_C$.*

Remark 7. Note that $\mathfrak{J}_C$ has four q^m-Weil numbers. If $P_1(X) = \prod_i (X - \omega_i)$, then $P_m(X) = \prod_i (X - \omega_i^m)$. Hence, if ω is a q-Weil number of $\mathfrak{J}_C$, then ω^m is a q^m-Weil number of $\mathfrak{J}_C$.

4 Non-cyclic subgroups

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 on the Jacobian $\mathfrak{J}_C$. $P_m(X)$ 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 $\tau = 8q^m + s^2 - 4t$. Then $P_m(X) = X^4 + sX^3 + (2q^m + (s^2 - \tau)/4)X^2 + sq^m X + q^{2m}$. In [22], the author proves the following Theorem 8 and Theorem 9.

Theorem 8. *Consider the Jacobian $\mathfrak{J}_C$ of a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism on $\mathfrak{J}_C$ as $P_m(X) = X^4 + sX^3 + (2q^m + (s^2 - \tau)/4)X^2 + sq^m X + q^{2m}$. 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 $\ell \nmid \tau$, 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 $q^m - 1$.*

Theorem 9. *Let notation be as in Theorem 8. Furthermore, let ω_m be a q^m-Weil number of $\mathfrak{J}_C$, and assume that ℓ is unramified in $\mathbb{Q}(\omega_m)$. Now assume that $\ell \mid \tau$. 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 $\ell \mid q^{mk} - 1$.*

Example 10 (The case $\ell \nmid \tau_k$). Let $P(X) = X^4 + X^3 - X^2 + 3X + 9 \in \mathbb{Q}[X]$. By [16] and [12] 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 $P(1) = 13$, and the embedding degree of $\mathfrak{J}_C(\mathbb{F}_3)$ with respect to $\ell = 13$ is $k = 3$. The characteristic polynomial of the 3^3-power Frobenius endomorphisms is given by $P_3(X) = X^4 + 13X^3 + 89X^2 + 351X + 729$. Hence, $\mathfrak{J}_C(\mathbb{F}_{27})[13]$ is bicyclic by Theorem 8.

Example 11 (The case $\ell \mid \tau_k$). Let $P(X) = (X^2 - 5X + 9)^2 \in \mathbb{Q}[X]$. By [16] and [12] it follows that $P(X)$ is the Weil polynomial of the Jacobian of a genus two curve C defined over $\mathbb{F}_9$. The number of $\mathbb{F}_9$-rational points on the Jacobian is $P(1) = 25$, so $\ell = 5$ is an odd prime divisor of $|\mathfrak{J}_C(\mathbb{F}_9)|$ not dividing $q = 9$. Notice that $P(X) \equiv X^4 + 2qX^2 + q^2 \pmod 5$. The complex roots of $P(X)$ are given by $\omega = \frac{5+\sqrt{-11}}{2}$ and $\bar{\omega}$, and 5 is unramified in $\mathbb{Q}(\omega)$. Since $9^2 \equiv 1 \pmod 5$, it follows by Theorem 9 that $\mathfrak{J}_C(\mathbb{F}_9)[5] \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathfrak{J}_C[5] \subseteq \mathfrak{J}_C(\mathbb{F}_{81})$.

Inspired by Theorem 8 and Theorem 9 we introduce the following notation.

Definition 12. *Consider the Jacobian $\mathcal{J}_C$ of a genus two curve C defined over a finite field $\mathbb{F}_q$. We say that the Jacobian is a $\mathbb{J}(\ell, q, k, \tau_k)$-Jacobian or is of type $\mathbb{J}(\ell, q, k, \tau_k)$, and write $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, if the following holds.*

1. *The number ℓ is an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, ℓ divides neither q nor $q-1$, and $\mathcal{J}_C(\mathbb{F}_q)$ is of embedding degree k with respect to ℓ.*
2. *The characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ is given by $P_k(X) = X^4 + sX^3 + (2q^k + (s^2 - \tau_k)/4)X^2 + sq^kX + q^{2k}$.*
3. *Let ω_k be a q^k-Weil number of $\mathcal{J}_C$. If ℓ divides τ_k, then ℓ is unramified in $\mathbb{Q}(\omega_k)$.*

Remark 13. Since ℓ is ramified in $\mathbb{Q}(\omega_k)$ if and only if ℓ divides the discriminant of $\mathbb{Q}(\omega_k)$ (see [20, Theorem 2.6, p. 199]), ℓ is unramified in $\mathbb{Q}(\omega_k)$ with probability approximately $1 - 1/\ell$. Hence, most likely, in cases relevant to pairing based cryptography the considered Jacobian is a $\mathbb{J}(\ell, q, k, \tau_k)$-Jacobian.

5 Matrix representation of the Frobenius endomorphism

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 $\mathcal{J}_C[\ell]$. If ψ can be represented on $\mathcal{J}_C[\ell]$ by a diagonal matrix with respect to an appropriate basis of $\mathcal{J}_C[\ell]$, then we say that ψ is *diagonalizable* or has a *diagonal representation* on $\mathcal{J}_C[\ell]$.

Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ (see [15, 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 [15, Theorem 3, p. 186],

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

By Theorem 8 and Theorem 9 we get the following explicit description of the matrix representation of the Frobenius endomorphism on the Jacobian of a genus two curve.

Theorem 14. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$. If φ is not diagonalizable on $\mathcal{J}_C[\ell]$, then φ is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} \tag{1}$$

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. In particular, $c \not\equiv q+1 \pmod{\ell}$.

Proof. Assume at first that ℓ does not divide τ_k. Then we know that $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic and that $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 8. Choose points $x_1, x_2 \in \mathcal{J}_C[\ell]$, such that $\varphi(x_1) = x_1$ and $\varphi(x_2) = qx_2$. Then the set $\{x_1, x_2\}$ is a basis of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Now, extend $\{x_1, x_2\}$ to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. If x_3 and x_4 are eigenvectors of φ, then φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Assume x_3 is not an eigenvector of φ. Then $\mathcal{B}' = \{x_1, x_2, x_3, \varphi(x_3)\}$ is a basis of $\mathcal{J}_C[\ell]$, and φ is represented by a matrix of the form (1) with respect to $\mathcal{B}'$.

Now, assume ℓ divides τ_k. Since ℓ divides $q^k - 1$, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 9. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of the Weil polynomial $P(X)$ modulo ℓ. Assume that 1 is an root of $P(X)$ modulo ℓ of multiplicity ν. Since the roots of $P(X)$ occur in pairs of the form $(\alpha, q/\alpha)$, it follows that

$$P(X) \equiv (X-1)^\nu (X-q)^\nu Q(X) \pmod{\ell} ,$$

where $Q \in \mathbb{Z}[X]$ is a polynomial of degree $4-2\nu$, $Q(1) \not\equiv 0 \pmod{\ell}$ and $Q(q) \not\equiv 0 \pmod{\ell}$. Let $U = \ker(\varphi-1)^\nu$, $V = \ker(\varphi-q)^\nu$ and $W = \ker(Q(\varphi))$. Then U, V and W are φ-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U) = \operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(V) = \nu$, and $\mathcal{J}_C[\ell] \simeq U \oplus V \oplus W$. If $\nu = 1$, then it follows as above that φ is either diagonalizable on $\mathcal{J}_C[\ell]$ or represented by a matrix of the form (1) with respect to some basis of $\mathcal{J}_C[\ell]$. Hence, we may assume that $\nu = 2$. Now, choose $x_1 \in U$ such that $\varphi(x_1) = x_1$, and extend $\{x_1\}$ to a basis $\{x_1, x_2\}$ of U. Similarly, choose a basis $\{x_3, x_4\}$ of V with $\varphi(x_3) = qx_3$. With respect to the basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$, φ is represented by a matrix of the form

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

Notice that

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

Since $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$, we know that $\varphi^k = \varphi_k$ is the identity on $\mathcal{J}_C[\ell]$. Hence, $M^k = I$. So $\alpha \equiv \beta \equiv 0 \pmod{\ell}$, i.e. φ is represented by a diagonal matrix with respect to $\mathcal{B}$.

Finally, if $c \equiv q + 1 \pmod{\ell}$, then M is diagonalizable. The theorem is proved. □

6 Determining fields of definition

In [5], Freeman and Lauter consider the problem of determining the field of definition of the ℓ-torsion points on the Jacobian of a genus two curve, i.e. the problem of determining the full embedding degree k_0. They describe a probabilistic algorithm to determine if $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\kappa})$; see [5, Algorithm 4.3]. (Notice that Freeman and Lauter consider a Jacobian defined over a prime field $\mathbb{F}_p$, and [5, Algorithm 4.3] determines if $\mathcal{J}_C[\ell^d] \subseteq \mathcal{J}_C(\mathbb{F}_q)$, where $q = p^k$ and $d \in \mathbb{N}$. This algorithm is easily generalized to determine if $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\kappa})$ for Jacobians defined over $\mathbb{F}_q$, $q = p^a$).

In most applications, a probabilistic algorithm to determine k_0 is sufficient. But we may have to compute k_0. To this end, consider a $\mathbb{J}(\ell, q, k, \tau_k)$-Jacobian $\mathcal{J}_C$. Let ω be a q-Weil number of $\mathcal{J}_C$. In cases relevant to pairing based cryptography, ℓ is most likely unramified in $\mathbb{Q}(\omega)$; cf. Remark 13. But then the full embedding degree of $\mathcal{J}_C$ with respect to ℓ can be computed directly by the following Algorithm 15.

Algorithm 15. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let ω be a q-Weil number of $\mathcal{J}_C$. Assume that ℓ is unramified in $\mathbb{Q}(\omega)$. Choose an upper bound $N \in \mathbb{N}$ of the full embedding degree k_0 of $\mathcal{J}_C$ with respect to ℓ. If $k_0 \leq N$, then the following algorithm outputs k_0. If $k_0 > N$, then the algorithm outputs "$k_0 > N$".*

1. *Let $j = 1$.*
2. *If the Weil polynomial $P(X)$ of $\mathcal{J}_C$ does not split in linear factors modulo ℓ, then φ is represented by a matrix M of the form* (1) *on $\mathcal{J}_C[\ell]$. In this case, let $k_0 = \min\{\kappa \in k\mathbb{N}, \kappa \leq N, M^\kappa \equiv I \pmod{\ell}\}$, if the minimum exists. Else let $j = 0$.*
3. *If $P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}$, then do the following:*
   (a) *If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then let $k_0 = \min\{\kappa \in k\mathbb{N}, \kappa \leq N, \alpha^\kappa \equiv 1 \pmod{\ell}\}$, if the minimum exists. Else let $j = 0$.*
   (b) *If $\alpha \equiv 1, q \pmod{\ell}$, then let $k_0 = k$.*
   (c) *If $\alpha \equiv q/\alpha \pmod{\ell}$, then let $k_0 = 2k$.*
4. *If $j = 0$ then output "$k_0 > N$". Else output k_0.*

Proof. First of all, recall that $k_0 \in k\mathbb{N}$; cf. Remark 5. As usual, let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$.

Assume at first that the Weil polynomial of $\mathcal{J}_C$ does not split in linear factors modulo ℓ. Then φ is not diagonalizable on $\mathcal{J}_C[\ell]$. Thus, φ is represented by a matrix M of the form (1) on $\mathcal{J}_C[\ell]$. Since φ^{k_0} is the identity on $\mathcal{J}_C[\ell]$, it is represented by the identity matrix I on $\mathcal{J}_C[\ell]$. But φ^{k_0} is also represented by M^{k_0} on $\mathcal{J}_C[\ell]$. So $M^{k_0} \equiv I \pmod{\ell}$. On the other hand, if $M^\kappa \equiv I \pmod{\ell}$ for some number $\kappa \leq k_0$, then φ^κ is the identity on $\mathcal{J}_C[\ell]$, i.e. $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\kappa})$. But then $\kappa = k_0$ by the definition of k_0. Hence, k_0 is the least number, such that $M^{k_0} \equiv I \pmod{\ell}$.

Now, assume the Weil polynomial factors modulo ℓ as

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell} \ .$$

The case $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$ is obvious. If $\alpha \equiv 1, q \pmod{\ell}$, then

$$P(X) \equiv (X-1)^2(X-q)^2 \equiv X^4 + 2\sigma X^3 + (2q + \sigma^2 - \tau)X^2 + 2\sigma q X + q^2 \pmod{\ell} \ ,$$

where $\sigma \equiv -(q+1) \pmod{\ell}$ and $\tau \equiv 0 \pmod{\ell}$. By Theorem 9 it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; i.e. $k_0 = k$ in this case. Finally, assume that $\alpha \equiv q/\alpha \pmod{\ell}$, i.e. that $\alpha^2 \equiv q \pmod{\ell}$. Then the q-power Frobenius endomorphism is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form

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

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. Notice that

$$M^{2k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2k\alpha^{2k-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix} .$$

Thus, $P_{2k}(X) \equiv (X-1)^4 \pmod{\ell}$. By Theorem 9 it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{2k}})$, i.e. $k_0 = 2k$. □

Theorem 16. *Let the notation and assumptions be as in Algorithm 15. On input $\mathcal{J}_C$, the Weil polynomial modulo ℓ and a number $N \in \mathbb{N}$, Algorithm 15 outputs either "$k_0 > N$" or the full embedding degree of $\mathcal{J}_C$ with respect to ℓ in at most $O(N)$ number of operations in $\mathbb{F}_\ell$.*

Proof. If the Weil polynomial of $\mathcal{J}_C$ does not split in linear factors modulo ℓ, then powers $\{M^k, (M^k)^2, \ldots, (M^k)^{\lfloor N/k \rfloor}\}$ of M modulo ℓ are computed; here, M is the matrix representation of the q-power Frobenius endomorphism on $\mathcal{J}_C[\ell]$. M is of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} .$$

Hence, computing powers of M is equivalent to computing powers of $M' = \left[\begin{smallmatrix} 0 & -q \\ 1 & c \end{smallmatrix}\right]$ and powers of q. Computation of the product of two matrices $A, B \in \mathrm{Mat}_2(\mathbb{F}_\ell)$ takes 12 operations in $\mathbb{F}_\ell$, so computing the powers of M modulo ℓ takes $O(N)$ operations in $\mathbb{F}_\ell$.

Assume the Weil polynomial factors as $(X-1)(X-q)(X-\alpha)(X-q/\alpha)$ modulo ℓ. If $\alpha \equiv 1, q, q/\alpha \pmod{\ell}$, then no computations are needed. If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then powers $\{\alpha^k, (\alpha^k)^2, \ldots, (\alpha^k)^{\lfloor N/k \rfloor}\}$ of α modulo ℓ are computed; this takes $O(N)$ operations in $\mathbb{F}_\ell$. □

Remark 17. Recall that $q = p^a$ for some power $a \in \mathbb{N}$. Assume ℓ and p are of the same size. For small N (e.g. $N < 200$), a limit of $O(N)$ number of operations in $\mathbb{F}_\ell$ is a better result than the expected number of operations in $\mathbb{F}_p$ of [5, Algorithm 4.3] given by [5, Proposition 4.6]. Furthermore, the algorithm of [5] only checks if a given number $\kappa \in \mathbb{N}$ is the full embedding degree k_0 of the Jacobian. Hence, to find k_0 using [5, Algorithm 4.3], we must apply it to every number in the set $\{\kappa \in k\mathbb{N} | \kappa \leq N\}$. Thus, we must multiply the number of expected operations in $\mathbb{F}_p$ with a factor $O(\lfloor N/k \rfloor)$. So if ℓ and p are of the same size, then Algorithm 15 is more efficient than [5, Algorithm 4.3]. On the other hand, if $\ell \gg p$, then field operations in $\mathbb{F}_p$ is faster than field operations in $\mathbb{F}_\ell$, and [5, Algorithm 4.3] may be the more efficient one. Hence, the choice of algorithm to compute the full embedding degree depends strongly on the values of ℓ and p in the implementation.

7 Anti-symmetric pairings on the Jacobian

On $\mathfrak{J}_C[\ell]$, a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathfrak{J}_C[\ell] \times \mathfrak{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times$$

exists, e.g. the Weil pairing; cf. e.g. [19, chapter 12]. Here, μ_ℓ is the group of ℓ^{th} roots of unity. A fast algorithm for computing the Weil pairing is given in [3]. Since ε is bilinear, it is given by

$$\varepsilon(x, y) = \zeta^{x^T \mathcal{E} y} \ , \tag{2}$$

for some matrix $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ with respect to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathfrak{J}_C[\ell]$.

Remark 18. To be more precise, the points x and y on the right hand of equation (2) should be replaced by their column vectors $[x]_\mathcal{B}$ and $[y]_\mathcal{B}$ with respect to $\mathcal{B}$. To ease notation, this has been omitted.

Let φ denote the q-power Frobenius endomorphism on $\mathfrak{J}_C$. Since ε is Galois-invariant,

$$\forall x, y \in \mathfrak{J}_C[\ell] : \varepsilon(x, y)^q = \varepsilon(\varphi(x), \varphi(y)) \ .$$

This is equivalent to

$$\forall x, y \in \mathfrak{J}_C[\ell] : q(x^T \mathcal{E} y) = (Mx)^T \mathcal{E} (My) \ ,$$

where M is the matrix representation of φ on $\mathfrak{J}_C[\ell]$ with respect to $\mathcal{B}$. Since $(Mx)^T \mathcal{E}(My) = x^T M^T \mathcal{E} M y$, it follows that

$$\forall x, y \in \mathfrak{J}_C[\ell] : x^T q\mathcal{E} y = x^T M^T \mathcal{E} M y \ ,$$

or equivalently, that $q\mathcal{E} = M^T \mathcal{E} M$.

Now, let $\varepsilon(x_i, x_j) = \zeta^{a_{ij}}$. By anti-symmetry,

$$\mathcal{E} = \begin{bmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{bmatrix} \ .$$

At first, assume that φ is represented by a matrix of the form (1) with respect to $\mathcal{B}$. Since $M^T \mathcal{E} M = q\mathcal{E}$, it follows that

$$a_{14} - qa_{13} \equiv a_{23} - a_{24} \equiv a_{14}(c - (1+q)) \equiv a_{24}(c - (1+q)) \equiv 0 \pmod{\ell} \ .$$

Thus, $a_{13} \equiv a_{14} \equiv a_{23} \equiv a_{24} \equiv 0 \pmod{\ell}$, cf. Theorem 14. So

$$\mathcal{E} = \begin{bmatrix} 0 & a_{12} & 0 & 0 \\ -a_{12} & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{34} \\ 0 & 0 & -a_{34} & 0 \end{bmatrix} \ .$$

Since ε is non-degenerate, $a_{12}^2 a_{34}^2 = \det \mathcal{E} \not\equiv 0 \pmod{\ell}$.

Finally, assume that φ is represented by a diagonal matrix $\mathrm{diag}(1, q, \alpha, q/\alpha)$ with respect to $\mathcal{B}$. Then it follows from $M^T \mathcal{E} M = q\mathcal{E}$, that

$$a_{13}(\alpha - q) \equiv a_{14}(\alpha - 1) \equiv a_{23}(\alpha - 1) \equiv a_{24}(\alpha - q) \equiv 0 \pmod{\ell} \ .$$

If $\alpha \equiv 1, q \pmod{\ell}$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bi-cyclic. Hence the following theorem holds.

Theorem 19. *Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on $\mathcal{J}_C$. Choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by either a diagonal matrix* $\mathrm{diag}(1, q, \alpha, q/\alpha)$ *or a matrix of the form* (1) *with respect to $\mathcal{B}$. If the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of ℓ-torsion points on the Jacobian is cyclic, then all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices*

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix} , \qquad a, b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$$

with respect to $\mathcal{B}$.

Remark 20. Let notation and assumptions be as in Theorem 19. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_C[\ell]$, and let ε be given by $\mathcal{E}_{a,b}$ with respect to a basis $\{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Then ε is given by $\mathcal{E}_{1,1}$ with respect to $\{a^{-1}x_1, x_2, b^{-1}x_3, x_4\}$.

Remark 21. In cases relevant to pairing based cryptography, we consider a prime divisor ℓ of size q^2. Assume ℓ is of size q^2. Then ℓ divides neither q nor $q-1$. The number of $\mathbb{F}_q$-rational points on the Jacobian is approximately q^2. Thus, $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic in cases relevant to pairing based cryptography.

8 Generators of $\mathcal{J}_C[\ell]$

Consider a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Assume the $\mathbb{F}_q$-rational subgroup of ℓ-torsion points $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic. Let φ be the q-power Frobenius endomorphism of $\mathcal{J}_C$. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times \ .$$

In the following, frequently we will choose a random point $P \in \mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$ for some power $a \in \mathbb{N}$. This is done as follows: (1) Choose a random point $P \in \mathcal{J}_C(\mathbb{F}_{q^a})$. (2) Compute $P := [m](P)$, where $|\mathcal{J}_C(\mathbb{F}_{q^a})| = m\ell^s$ and $\ell \nmid m$. (3) Compute the order $|P| = \ell^{t(P)}$ of P. (4) If $t(P) > 0$, then let $P := [\ell^{t(P)-1}](P)$. Since the power $t(P)$ will be different for each point P, this procedure does not define a group homomorphism from $\mathcal{J}_C(\mathbb{F}_{q^a})$ to $\mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$. Thus, the image of points uniformly distributed in $\mathcal{J}_C(\mathbb{F}_{q^a})$ will not necessarily be uniformly distributed in $\mathcal{J}_C(\mathbb{F}_{q^a})[\ell]$. A method of choosing points uniformly at random is given in [5, Section 5.3], but it leads to a significant extra cost. In practice we believe it is better to not use the method in [5], even though this means one might need to sample a few extra points.

We consider the cases where $\ell \nmid \tau_k$ and where $\ell \mid \tau_k$ separately.

8.1 The case $\ell \nmid \tau_k$

If ℓ does not divide τ_k, then $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 8. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and extend $\{x_1\}$ to a basis $\{x_1, y_2\}$ of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$, where $\varphi(y_2) = qy_2$. Let $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ be a random point. If $x_2' \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, then choose another random point $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. After two trials, $x_2' \notin \mathcal{J}_C(\mathbb{F}_q)[\ell]$ with probability $1 - 1/\ell^2$. Hence, we may ignore the case where $x_2' \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$. Write $x_2' = \alpha_1 x_1 + \alpha_2 y_2$. Then

$$\mathcal{O} \neq x_2 = x_2' - \varphi(x_2') = \alpha_2(1-q)y_2 \in \langle y_2 \rangle \ ,$$

i.e. $\varphi(x_2) = qx_2$. Now, let $\mathcal{J}_C[\ell] \simeq \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \oplus W$, where W is a φ-invariant submodule of rank two. Choose a random point $x_3' \in \mathcal{J}_C[\ell]$. Since $x_3' - \varphi(x_3') \in \langle y_2 \rangle \oplus W$, we may assume that $x_3' \in \langle y_2 \rangle \oplus W$. But then

$$x_3 = qx_3' - \varphi(x_3') \in W$$

as above. If $\varphi(x_3') = qx_3'$, then $x_3' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. This will only happen with probability $1/\ell^2$. Hence, we may ignore this case. Notice that

$$\mathcal{J}_C[\ell] = \langle x_1, x_2, x_3, \varphi(x_3) \rangle \text{ if and only if } \varepsilon(x_3, \varphi(x_3)) \neq 1;$$

cf. Theorem 19.

Assume $\varepsilon(x_3, \varphi(x_3)) = 1$. Then x_3 is an eigenvector of φ. Let $\varphi(x_3) = \alpha x_3$. Then the Weil polynomial of $\mathcal{J}_C$ is given by

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}$$

modulo ℓ. Assume $\alpha \equiv q/\alpha \pmod{\ell}$. Then $\alpha^2 \equiv q \pmod{\ell}$, and it follows that the characteristic polynomial of φ^k is given by

$$P_k(X) \equiv (X-1)^2(X+1)^2 \equiv X^4 - 2q^k X^2 + q^{2k} \pmod{\ell}$$

modulo ℓ. But then $\ell \mid \tau_k$. This is a contradiction. So $\alpha \not\equiv q/\alpha \pmod{\ell}$. Therefore, we can extend $\{x_1, x_2, x_3\}$ to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 20.

Now, choose a random point $x \in \mathcal{J}_C[\ell]$. Write $x = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4$. Then $\varepsilon(x_3, x) = \zeta^{\alpha_4}$. So $\varepsilon(x_3, x) \neq 1$ if and only if ℓ does not divide α_4. On the other hand, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only ℓ does not divide α_4. Thus, if ℓ does not divide τ_k, then the following Algorithm 22 outputs generators of $\mathcal{J}_C[\ell]$ with probability at least $1 - 1/\ell^n$.

Algorithm 22. *On input a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, the numbers ℓ, q, k and τ_k, the full embedding degree k_0 of $\mathcal{J}_C$ with respect to ℓ and a number $n \in \mathbb{N}$, if ℓ does not divide τ_k, then the following algorithm outputs a basis of $\mathcal{J}_C[\ell]$ or "failure".*

1. *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ and $x_3' \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$; compute $x_3 = q(x_3' - \varphi(x_3')) - \varphi(x_3' - \varphi(x_3'))$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
2. *Let $i = j = 0$. While $i < n$ do the following:*
   (a) *Choose a random point $x_4 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
   (b) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

8.2 The case $\ell \mid \tau_k$

Assume ℓ divides τ_k. Then $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 9. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and let $y_2 \in \mathcal{J}_C[\ell]$ be a point with $\varphi(y_2) = q y_2$. Write $\mathcal{J}_C[\ell] = \langle x_1, y_2 \rangle \oplus W$, where W is a φ-invariant submodule of rank two; cf. the proof of Theorem 14. Let $\{y_3, y_4\}$ be a basis of W, such that φ is represented on $\mathcal{J}_C[\ell]$ with respect to the basis $\mathcal{B} = \{x_1, y_2, y_3, y_4\}$ by either a diagonal matrix

$$M_1 = \operatorname{diag}(1, q, \alpha, q/\alpha) \ ,$$

or a matrix of the form

$$M_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} \ ,$$

where $c \not\equiv q + 1 \pmod{\ell}$; cf. Theorem 14.

Now, choose a random point $z \in \mathcal{J}_C[\ell]$. Since $z - \varphi(z) \in \langle y_2, y_3, y_4 \rangle$, we may assume that $z \in \langle y_2, y_3, y_4 \rangle$. Write $z = \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Assume at first that

φ is represented on $\mathcal{J}_C[\ell]$ by M_1 with respect to $\mathcal{B}$. Then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 \alpha y_3 + \alpha_4 (q/\alpha) y_4) \\ &= \alpha_3 (q - \alpha) y_3 + \alpha_4 (q - q/\alpha) y_4; \end{aligned}$$

so $qz - \varphi(z) \in \langle y_3, y_4 \rangle$. If $qz - \varphi(z) = 0$, then it follows that $q \equiv 1 \pmod{\ell}$. This contradicts the choice of the Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$ in this case. Now assume that φ is represented on $\mathcal{J}_C[\ell]$ by M_2 with respect to $\mathcal{B}$. Then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 y_4 + \alpha_4 (-q y_3 + c y_4)) \\ &= q(\alpha_3 + \alpha_4) y_3 + (\alpha_4 q - \alpha_3 - \alpha_4 c) y_4; \end{aligned}$$

so again $qz - \varphi(z) \in \langle y_3, y_4 \rangle$. If $qz - \varphi(z) = 0$, then it follows that $c \equiv q + 1 \pmod{\ell}$. This is a contradiction. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$ also in this case.

Choose random points $x_3, x_4 \in W$. Write $x_i = \alpha_{i3} y_3 + \alpha_{i4} y_4$ for $i = 3, 4$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 20. But then $\varepsilon(x_3, x_4) = \zeta^{\alpha_{33}\alpha_{44} - \alpha_{34}\alpha_{43}}$. Hence, $\varepsilon(x_3, x_4) = 1$ if and only if $\alpha_{33}\alpha_{44} \equiv \alpha_{34}\alpha_{43} \pmod{\ell}$. So $\varepsilon(x_3, x_4) \neq 1$ with probability $1 - 1/\ell$. Hence, we have a procedure to find a basis of W.

Until now, we have found points $x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3, x_4 \in W$, such that $W = \langle x_3, x_4 \rangle$. Now, choose a random point $x_2 \in \mathcal{J}_C[\ell]$. Write $x_2 = \alpha_1 x_1 + \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Then $\varepsilon(x_1, x_2) = \zeta^{\alpha_2}$, i.e. $\varepsilon(x_1, x_2) = 1$ if and only if $\alpha_2 \equiv 0 \pmod{\ell}$. Thus, with probability $1 - 1/\ell$, the set $\{x_1, x_2, x_3, x_4\}$ is a basis of $\mathcal{J}_C[\ell]$.

Summing up, if ℓ divides τ_k, then the following Algorithm 23 outputs generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$.

Algorithm 23. *On input a Jacobian $\mathcal{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$, the numbers ℓ, q, k and τ_k, the full embedding degree k_0 of $\mathcal{J}_C$ with respect to ℓ and a number $n \in \mathbb{N}$, if ℓ divides τ_k, then the following algorithm outputs a basis of $\mathcal{J}_C[\ell]$ or "failure".*

1. *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$.*
2. *Let $i = j = 0$. While $i < n$ do the following:*
   (a) *Choose a random point $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$.*
   (b) *If $\varepsilon(x_1, x_2) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$, then output "failure" and stop.*
4. *Let $i = j = 0$. While $i < n$ do the following:*
   (a) *Choose random points $y_3, y_4 \in \mathcal{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
   (b) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
5. *If $j = 0$, then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

8.3 The complete algorithm

Combining Algorithm 22 and 23, we obtain the desired algorithm to find generators of $\mathcal{J}_C[\ell]$.

Algorithm 24. *On input a Jacobian* $\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$*, the numbers* ℓ*,* q*,* k *and* τ_k*, the full embedding degree* k_0 *of* $\mathfrak{J}_C$ *with respect to* ℓ *and a number* $n \in \mathbb{N}$*, the following algorithm outputs a basis of* $\mathfrak{J}_C[\ell]$ *or "failure".*

1. *If* $\ell \nmid \tau_k$*, run Algorithm 22 on input* $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$*.*
2. *If* $\ell \mid \tau_k$*, run Algorithm 23 on input* $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$*.*

Theorem 25. *Let* $\mathfrak{J}_C$ *be a* $\mathbb{J}(\ell, q, k, \tau_k)$*-Jacobian of full embedding degree* k_0 *with respect to* ℓ*. On input* $(\mathfrak{J}_C, \ell, q, k, \tau_k, k_0, n)$*, Algorithm 24 outputs generators of* $\mathfrak{J}_C[\ell]$ *with probability at least* $(1 - 1/\ell^n)^2$*. We expect Algorithm 24 to run in*

$$O\left(\log \ell \log \frac{q^{k_0} - 1}{\ell} {k_0}^3 \log k_0 \log q\right)$$

field operations in $\mathbb{F}_q$ *(ignoring* $\log \log q$ *factors).*

Proof. We must compare the cost of the steps in Algorithm 24. From [5, proof of Proposition 4.6], [7, proof of Corollary 1] and [17] we get the following estimates: (1) Choosing a random point on $\mathfrak{J}_C(\mathbb{F}_{q^a})$ for some power $a \in \mathbb{N}$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$, and computing a multiple $[m](P)$ of a point $P \in \mathfrak{J}_C(\mathbb{F}_{q^a})$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$. (2) Evaluating the q^a-power Frobenius endomorphism of the Jacobian on a point $P \in \mathfrak{J}_C[\ell]$ takes $O(a \log q)$ field operations in $\mathbb{F}_{q^a}$. (3) Evaluating the Tate pairing on two point of $\mathfrak{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$ takes $O(\log \ell)$ field operations in $\mathbb{F}_{q^{k_0}}$. The Weil pairing can be computed by computing two Tate pairings, raising the results to the power $\frac{q^{k_0}-1}{\ell}$ and finally computing the quotient of these numbers; see [8]. The exponentiation takes $O(\log \frac{q^{k_0}-1}{\ell})$ field operations in $\mathbb{F}_{q^{k_0}}$, and a division takes $O({k_0}^2)$ field operations in $\mathbb{F}_{q^{k_0}}$. Hence, evaluating the Weil pairing on two point of $\mathfrak{J}_C(\mathbb{F}_{q^{k_0}})[\ell]$ takes $O(\log \ell) O(\log \frac{q^{k_0}-1}{\ell}) O({k_0}^2)$ field operations in $\mathbb{F}_{q^{k_0}}$. (4) By using fast multiplication techniques, one field operation in $\mathbb{F}_{q^a}$ takes $O(\log q^a \log \log q^a) = O(a \log a \log q)$ field operations in $\mathbb{F}_q$ (ignoring $\log \log q$ factors).

We see that the pairing computation is the most expensive step in Algorithm 24. Thus, Algorithm 24 runs in $O(\log \ell \log \frac{q^{k_0}-1}{\ell} {k_0}^3 \log k_0 \log q)$ field operations in $\mathbb{F}_q$ (ignoring $\log \log q$ factors). □

9 Implementation issues

To check if ℓ ramifies in $\mathbb{Q}(\omega_k)$ in the case where ℓ divides τ_k, a priori we need to find a q^k-Weil number ω_k of the Jacobian $\mathfrak{J}_C$. On Jacobians generated by the *complex multiplication method* [23, 10, 4], we know the Weil numbers in advance. Hence, Algorithm 24 is particularly well suited for such Jacobians.

Fortunately, most likely ℓ does not divide τ_k, and then we do not have to find a q^k-Weil number (ℓ divides a random number $n \in \mathbb{Z}$ with vanishing probability $1/\ell$). And if the Weil polynomial splits in distinct linear factors modulo ℓ, then we do not even have to compute τ_k. To see this, assume that the Weil polynomial of $\mathfrak{J}_C$ splits as

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell} ,$$

where $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$. Let φ be the q-power Frobenius endomorphism of $\mathfrak{J}_C$, and let $P_k(X)$ be the characteristic polynomial of φ^k. Then

$$P_k(X) \equiv (X-1)^2(X-\alpha^k)(X-1/\alpha^k) \pmod{\ell} .$$

If ℓ divides τ_k, then $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 9. But then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ divides } \tau_k \text{ if and only if } \alpha^k \equiv 1 \pmod{\ell}. \tag{3}$$

Assume $\alpha^k \equiv 1 \pmod{\ell}$. Then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ ramifies in } \mathbb{Q}(\omega^k) \text{ if and only if } \omega^k \notin \mathbb{Z}. \tag{4}$$

See [20, Proposition 8.3, p. 47]. Here, ω is a q-Weil number of $\mathfrak{J}_C$.

Consider the case where $\alpha^k \equiv 1 \pmod{\ell}$ and $\omega^k \in \mathbb{Z}$. Then $\omega = \sqrt{q}e^{in\pi/k}$ for some $n \in \mathbb{Z}$ with $0 < n < k$. Assume k divides mn for some $m < k$. Then $\omega^{2m} = q^m \in \mathbb{Z}$. Since the q-power Frobenius endomorphism is the identity on the $\mathbb{F}_q$-rational points on the Jacobian, it follows that $\omega^{2m} \equiv 1 \pmod{\ell}$. Hence, $q^m \equiv 1 \pmod{\ell}$, i.e. k divides m. This is a contradiction. So n and k has no common divisors. Let $\xi = \omega^2/q = e^{in2\pi/k}$. Then ξ is a primitive k^{th} root of unity, and $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\omega)$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] \leq 4$ and $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(k)$, where ϕ is the Euler phi function, it follows that $k \leq 12$. Hence,

$$\text{if } \alpha^k \equiv 1 \pmod{\ell}, \text{ then } \omega^k \in \mathbb{Z} \text{ if and only if } k \leq 12. \tag{5}$$

The criteria (3), (4) and (5) provides the following efficient algorithm to check whether a given Jacobian is of type $\mathbb{J}(\ell, q, k, \tau_k)$, and whether ℓ divides τ_k.

Algorithm 26. *Let $\mathfrak{J}_C$ be the Jacobian of a genus two curve C. Assume that the odd prime number ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathfrak{J}_C$, and that ℓ divides neither q nor $q-1$. Let k be the multiplicative order of q modulo ℓ.*

1. *Compute the Weil polynomial $P(X)$ of $\mathfrak{J}_C$. Let $P(X) \equiv \prod_{i=1}^{4}(X-\alpha_i) \pmod{\ell}$.*
2. *If $\alpha_i^k \not\equiv 1 \pmod{\ell}$ for an $i \in \{1,2,3,4\}$, then output "$\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$ and ℓ does not divide τ_k" and stop.*
3. *If $k > 12$ then output "$\mathfrak{J}_C \notin \mathbb{J}(\ell, q, k, \tau_k)$" and stop.*
4. *Output "$\mathfrak{J}_C \in \mathbb{J}(\ell, q, k, \tau_k)$ and ℓ divides τ_k" and stop.*

References

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

[2] 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.

[3] I. Duursma and H.-S. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In *Advances in Cryptology - ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 111–123. Springer, 2003.

[4] K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2007. Preprint, `arXiv:math/0405305`, to appear in *Proceedings of AGCT-10*.

[5] D. Freeman and K. Lauter. Computing endomorphism rings of jacobians of genus 2 curves over finite fields. In J. Hirschfeld, J. Chaumine, and R. Rolland, editors, *Algebraic geometry and its applications, Proceedings of the First SAGA conference, 7–11 May 2007, Papeete*, volume 5 of *Number Theory and Its Applications*, pages 29–66. World Scientific, 2008.

[6] 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.

[7] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[8] 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.

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

[10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic CM-method for genus 2, 2005. Preprint, `arXiv:math/0503148`.

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

[12] E.W. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields, 2007. Preprint, `arXiv:math/0607515`.

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

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

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

[16] 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.

[17] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

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

[19] J.S. Milne. Abelian varieties, 1998. Available at `http://www.jmilne.org`.

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

[21] C.R. Ravnshøj. Generators of Jacobians of hyperelliptic curves, 2007. Preprint, `arXiv:0704.3339`.

[22] C.R. Ravnshøj. Non-cyclic subgroups of Jacobians of genus two curves, 2008. Preprint, `arXiv:0801.2835`.

[23] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72:435–458, 2003.

Bibliography

R. Balasubramanian and N. Koblitz. The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm. *J. Cryptology*, vol. 11:pp. 141–145 (1998).

D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing (2001). Cryptology ePrint Archive, Report 2001/090.
`http://eprint.iacr.org`

D. Boneh, B. Lynn and H. Shacham. Short Signatures from the Weil Pairing. *J. Cryptology*, vol. 17:pp. 297–319 (2004).

S. Duquesne and T. Lange. Arithmetic of Hyperelliptic Curves. In H. Cohen and G. Frey (editors), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 303–354. Chapman & Hall/CRC (2006).

I. Duursma and H.-S. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In C. S. Laih (editor), *Advances in Cryptology - ASIACRYPT 2003*, *Lecture Notes in Computer Science*, vol. 2894, pp. 111–123. Springer (2003).

K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields (2007). Preprint, `arXiv:math/0405305`. To appear in *Proceedings of AGCT-10*.
`http://arxiv.org`

D. Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. In T. Takagi, T. Okamoto, E. Okamoto and T. Okamoto (editors), *Pairing-Based Cryptography - Pairing 2007*, *Lecture Notes in Computer Science*, vol. 4575, pp. 152–176. Springer (2007).

D. Freeman and K. Lauter. Computing endomorphism rings of Jacobian of genus 2 curves over Finite Fields. In J. Hirschfeld, J. Chaumine and R. Rolland (editors), *Algebraic geometry and its applications, Proceedings of the First SAGA conference, 7–11 May 2007, Papeete*, *Number Theory and Its Applications*, vol. 5, pp. 29–66. World Scientific (2008).
`http://eprint.iacr.org`

G. FREY and T. LANGE. Varieties over Special Fields. In H. COHEN and G. FREY (editors), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 87–113. Chapman & Hall/CRC (2006).

G. FREY and H.-G. RÜCK. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, vol. 62:pp. 865–874 (1994).

S. D. GALBRAITH. Supersingular curves in cryptography. In BOYD and COLIN (editors), *Advances in Cryptology - Asiacrypt 2001*, *Lecture Notes in Computer Science*, vol. 2248, pp. 495–513. Springer (2001).

S. D. GALBRAITH. Pairings. In I. F. BLAKE, G. SEROUSSI and N. P. SMART (editors), *Advances in Elliptic Curve Cryptography*, *London Mathematical Society Lecture Note Series*, vol. 317, pp. 183–213. Cambridge University Press (2005).

S. D. GALBRAITH, F. HESS and F. VERCAUTEREN. Hyperelliptic pairings. In T. TAKAGI, T. OKAMOTO, E. OKAMOTO and T. OKAMOTO (editors), *Pairing-Based Cryptography - Pairing 2007*, *Lecture Notes in Computer Science*, vol. 4575, pp. 108–131. Springer (2007).

S. D. GALBRAITH, J. F. MCKEE and P. C. VALENÇA. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, vol. 13, no. 4:pp. 800–814 (2007).

S. D. GALBRAITH, J. PUJOLÀS, C. RITZENTHALER and B. SMITH. Distortion maps for genus two curves. Cryptology ePrint Archive, Report 2006/375 (2006).
`http://eprint.iacr.org`

P. GAUDRY, T. HOUTMANN, D. KOHEL, C. RITZENTHALER and A. WENG. The p-adic CM-Method for Genus 2 (2005). Preprint, `arXiv:math/0503148`.
`http://arxiv.org`

F. HESS. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, vol. 82:pp. 28–32 (2004).

L. HITT. Families of genus 2 curves with small embedding degree. Cryptology ePrint Archive, Report 2007/001 (2007).
`http://eprint.iacr.org`

T. HONDA. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, vol. 20:pp. 83–95 (1968).

E. W. HOWE, E. NART and C. RITZENTHALER. Jacobians in isogeny classes of abelian surfaces over finite fields (2007). Preprint, `arXiv:math/0607515`.
`http://arxiv.org`

N. KOBLITZ. Elliptic curve cryptosystems. *Math. Comp.*, vol. 48:pp. 203–209 (1987).

N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1:pp. 139–150 (1989).

N. Koblitz and A. Menezes. Pairing-Based Cryptography at High Security Levels (2005). Cryptology ePrint Archive, Report 2005/076.
`http://eprint.iacr.org`

S. Lang. *Abelian Varieties*. Interscience (1959).

D. Maisner and E. Nart. Abelian Surfaces over Finite Fields as Jacobians. *Experimental Mathematics*, vol. 11, no. 3:pp. 321–337 (2002).

A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press (1997).

V. S. Miller. Short Programs for Functions on Curves (1986). Unpublished manuscript.
`http://crypto.stanford.edu/miller/miller.pdf`

V. S. Miller. The Weil Pairing, and Its Efficient Calculation. *J. Cryptology*, vol. 17:pp. 235–261 (2004).

J. Neukirch. *Algebraic Number Theory*. Springer (1999).

K. G. Paterson. Cryptography from Pairings. In I. Blake, G. Seroussi and N. Smart (editors), *Advances in Elliptic Curve Cryptography*, *London Mathematical Society Lecture Note*, vol. 317, pp. 215–251. Cambridge University Press (2005).

S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory*, vol. 24:pp. 106–110 (1978).

C. R. Ravnshøj. Generators of Jacobians of Hyperelliptic Curves (2007a). Cryptology ePrint Archive, Report 2007/150. Submitted to *Math. Comp.*
`http://eprint.iacr.org`

C. R. Ravnshøj. Embedding Degree of Hyperelliptic Curves with Complex Multiplication (2007b). Cryptology ePrint Archive, Report 2007/175. Submitted to *Math. Comp.*
`http://eprint.iacr.org`

C. R. Ravnshøj. p-torsion of Genus Two Curves Over Prime Fields of Characteristic p (2007c). Preprint, `arXiv:0705.3537`. Submitted to *Math. Comp.*
`http://arxiv.org`

C. R. Ravnshøj. Non-Cyclic Subgroups of Jacobians of Genus Two Curves with Complex Multiplication (2008a). Cryptology ePrint Archive, Report 2008/025. Submitted to *Proceedings of AGCT 11*.
`http://eprint.iacr.org`

C. R. RAVNSHØJ. Non-Cyclic Subgroups of Jacobians of Genus Two Curves (2008b). Cryptology ePrint Archive, Report 2008/029. Submitted to *Design, Codes and Cryptography.*
`http://eprint.iacr.org`

C. R. RAVNSHØJ. Generators of Jacobians of Genus Two Curves (2008c). To appear in *Proceedings of Pairing 2008.*

K. RUBIN and A. SILVERBERG. Supersingular abelian varieties in cryptology. In M. YUNG (editor), *CRYPTO 2002*, Lecture Notes in Computer Science, pp. 336–353. Springer (2002).

K. RUBIN and A. SILVERBERG. Using Abelian Varieties to Improve Pairing-Based Cryptography (2007). Unpublished manuscript. Preliminary versions of parts of this manuscript appeared in the proceedings of Crypto 2002, ANTS VI and the Daewoo Workshop on Cryptography.
`http://math.uci.edu/~asilverb/bibliography/rubsilav.pdf`

I. R. SHAFAREVICH. *Basic Algebraic Geometry.* Springer (1974).

J. H. SILVERMAN. *The Arithmetic of Elliptic Curves.* Springer (1986).

H. STICHTENOTH and C. XING. On the structure of the divisor class group of a class of curves over finite fields. *Arch. Math.*, vol. 65:pp. 141–150 (1995).

J. TATE. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, vol. 2:pp. 134–144 (1966).

A. WENG. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, vol. 72:pp. 435–458 (2003).

H. J. ZHU. Group structures of elementary supersingular abelian varieties over finite fields. *J. Number Theory*, vol. 81:pp. 292–309 (2000).

M. E. ZIEVE. p^k-torsion of genus two curves over $\mathbb{F}_{p^m}$ (2007). Preprint, `arXiv:0705.3932`.
`http://arxiv.org`

Index