# A $p$-adic quasi-quadratic point counting algorithm

Robert Carls, David Lubicz

August 2, 2008

Robert Carls
robert.carls@uni-ulm.de
Institute of Pure Mathematics
University of Ulm
D-89069 Ulm, Germany

David Lubicz
david.lubicz@univ-rennes1.fr
CELAR
BP 7419 35174 Bruz Cedex
France

**Abstract**

In this article we give an algorithm for the computation of the number of rational points on the Jacobian variety of a generic ordinary hyperelliptic curve defined over a finite field $\mathbb{F}_q$ of cardinality $q$ with time complexity $O(n^{2+o(1)})$ and space complexity $O(n^2)$, where $n = \log(q)$. In the latter complexity estimate the genus and the characteristic are assumed as fixed. Our algorithm forms a generalization of both, the AGM algorithm of J.-F. Mestre and the canonical lifting method of T. Satoh. We canonically lift a certain arithmetic invariant of the Jacobian of the hyperelliptic curve in terms of theta constants. The theta null values are computed with respect to a semi-canonical theta structure of level $2^\nu p$ where $\nu > 0$ is an integer and $p = \mathrm{char}(\mathbb{F}_q) > 2$. The results of this paper suggest a global positive answer to the question whether there exists a quasi-quadratic time algorithm for the computation of the number of rational points on a generic ordinary abelian variety defined over a finite field.

**Keywords:** point counting algorithm, canonical lift, theta function, p-adic method, CM construction.

## 1 Introduction

The study of the properties of non-singular projective algebraic curves over finite fields is a subject of central importance in algorithmic number theory and cryptography. It is well established that the Jacobian varieties of such curves constitute a suitable family of groups to be used in cryptographic protocols which are based upon the difficulty of solving the *discrete logarithm problem.* In order to avoid 'weak' Jacobians, i.e. Jacobian varieties which give a trivial instance of the general discrete logarithm problem, it is necessary to precompute the number of rational points on a given Jacobian. This issue has prompted a lot of research, focused on the design of efficient point counting algorithms.

Next we briefly recall how one can count points by computing the eigenvalues of the absolute Frobenius endomorphism on a Jacobian variety. We denote by $\mathbb{F}_q$ a finite field with $q$ elements. Let $\Sigma$ be the $q$-th power Frobenius morphism acting on the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Let $C$ be a smooth projective curve of genus $g$ over $\mathbb{F}_q$, and let $J(C)$ be its Jacobian. For a prime number $\ell$ not dividing $q$ we denote by $T_\ell$ the $\ell$-adic Tate module of $J(C)$. The latter is a free $\mathbb{Z}_\ell$-module of rank $2g$. Here $\mathbb{Z}_\ell$ stands for the $\ell$-adic integers. Let $\mathrm{End}(J(C))$ be the ring of endomorphisms of $J(C)$ and put $\mathrm{End}^0(J(C)) = \mathrm{End}(J(C)) \otimes \mathbb{Q}$. There exists a canonical injective morphism $\rho_\ell : \mathrm{End}^0(J(C)) \to \mathrm{End}_{\mathbb{Q}_\ell}(T_\ell \otimes \mathbb{Q}_\ell)$ which is called the *$\ell$-adic representation* of $\mathrm{End}^0(J(C))$. Let $F$ be the purely inseparable endomorphism of degree $q^g$ of $J(C)$ given by the action of $\Sigma$ on geometric point coordinates $(x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)$. One would like to compute, in an efficient way, the characteristic polynomial $\chi_F$ of $\rho_\ell(F)$. One recovers the number of rational points of the Jacobian $J(C)$ as $\chi_F(1)$.

Broadly speaking, there exists two classes of point counting algorithms. On one hand, there are the so-called *$\ell$-adic algorithms* initiated by the work of R. Schoof [Sch85]. These algorithms compute the action of the Frobenius morphism on the group of $\ell$-torsion points for different primes $\ell$, where the latter $\ell$ are chosen coprime to the characteristic of the finite field. If the product over all $\ell$ is sufficiently big, then one can recover $\chi_F$ by the Chinese remainder theorem. Schoof's algorithm for elliptic curves behaves very well, due to the improvements by O. Atkin and N. Elkies [Sch95] [Elk98]. Cryptographic sizes still seem to be difficult to reach in genus 2 [GS04] and higher. A generalization of the method of R. Schoof, the complexity of which is polynomial in the genus, has been proposed by B. Edixhoven [Edi06]. On the other hand, there are the so-called *$p$-adic methods*, introduced by the work of T. Satoh [Sat00]. These algorithms rely on the computation of the action of the Frobenius morphism on $p$-adic canonical lifts of certain arithmetic invariants, where $p > 0$ is the characteristic of the finite base field. They have in common a bad behavior with respect to the characteristic $p$. It is convenient to assess their complexity in terms of $\log(q)$, where $q$ is the number of elements of the finite field $\mathbb{F}_q$ and where the characteristic $p$ of the finite field is assumed as fixed.

In the following we recall existing work about $p$-adic point counting algorithms. First, a series of algorithmic improvements upon the algorithm of Satoh [Gau02, Har02b, Har02a, KPC$^+$02, LL03, VPV01] led to a *quasi-quadratic time point counting algorithm* for ordinary elliptic curves over finite fields. The special case of characteristic 2 was then interpreted by J.-F. Mestre in terms of a 2-adic analogue of Gauss' *algebraic geometric mean*. He gave a very elegant and simple quasi-cubic time point counting algorithm for ordinary elliptic curves over finite fields of characteristic 2 [Mes01]. The previously cited algorithmic improvements upon the algorithm of Satoh can also be applied to Mestre's algorithm, which results in a quasi-quadratic time point counting algorithm. Mestre has extended the scope of his algorithm by showing that the algebraic geometric mean formulas can be considered as a particular case of the Riemann duplication formulas for complex analytic theta functions [Mes02]. His ideas led to a quasi-quadratic time point counting algorithm for ordinary hyperelliptic curves defined over a finite field of characteristic 2 [LD06]. Other $p$-adic algorithms were found by K. Kedlaya [Ked01] and A. Lauder [LW02]. Their algorithms are based on the computation of the action of a formal Frobenius lift on the Monsky-Washnitzer and the Dwork cohomology groups, respectively.

The aim of this paper is to describe an algorithm for the computation of the number of points of a generic ordinary hyperelliptic curve over a finite field $\mathbb{F}_q$ with $q$ elements of characteristic $p > 2$ which has quasi-quadratic time and quadratic space complexity in terms of $\log_p(q)$. We give two versions of our algorithm: a proven version of the algorithm, for which we are able to prove that it is correct and that it has quasi-quadratic time and quadratic space complexity, and a heuristic version of the algorithm, the proof of which relies on some yet unproven facts.

The reason why we give both algorithms is that, due to the smaller constant term in the complexity estimate of the heuristic algorithm, it performs much faster than the proven algorithm for field sizes which are actually used in the applications. We have strong computational evidence that also the heuristic version of the algorithm is correct. Our method follows the point counting strategy of J.-F. Mestre, which relies on the computation of arithmetic invariants of canonical lifts using the coordinate system provided by the theta null values associated to an abelian variety with theta structure. In our case, the theta null point is computed with respect to a theta structure of level $2^\nu p$ where $\nu > 1$ is an integer and $p > 2$ is the characteristic of the residue field. The results of this paper suggest a global positive answer to the question whether there exists a quasi-quadratic time and quadratic space algorithm for the computation of the number of rational points of a generic ordinary abelian variety over a finite field.

Both versions of the algorithm consist of the following two main steps, according to the classical lift and norm paradigm. Let $C$ be an ordinary hyperelliptic curve over a finite field of characteristic $p > 2$ whose Jacobian is absolutely simple.

1. First, one computes a certain arithmetic invariant associated to the canonical lift of the Jacobian variety of the curve $C$. The arithmetic invariant is given by the theta null point of a Jacobian of $C$ with respect to a semi-canonical theta structure of level $2^\nu p$ with $\nu > 0$ an integer. The lifting is done using a multivariate Henselian lifting algorithm applied to certain theta identities of level $2^\nu p$ and degree $p^2$.

2. Secondly, the norm of a certain quotient of theta null values attached to the canonical lift is computed. This value coincides with the product of the invertible eigenvalues of the absolute Frobenius endomorphism on the reduction. If one computes the canonical lift and the norm with sufficiently high precision, then it is straight forward to recover the characteristic

polynomial of the Frobenius morphism from the latter approximation of the norm.

The only difference between the proven and the heuristic version of our algorithm lies in the choice of the parameter $\nu$ of Step 1. In the heuristic version of the algorithm the parameter $\nu$ is chosen to be equal 1. In the case that $\nu = 3$ we are able to give a complete proof of correctness of the algorithm.

This paper is organized as follows. In Section 2 we present some new theoretical results that form the basis of our algorithm.

- (Section 2.1) An important ingredient of our algorithm is given by theta relations of level $2^\nu p$ and degree $p^2$, which describe the action of a square of the unique Frobenius lift on the Serre-Tate formal torus with respect to the coordinates given by the canonical theta structure [Car07]. We remark, that the equations, which are described in Section 2.1, can also be used for CM construction in arbitrary characteristic generalizing the results of [CKL08].

- (Section 2.2) We give equations which, together with the relations of Section 2.1, define the local deformation space of an ordinary abelian variety with a $(2^\nu p)$-theta structure. Classically, equations in terms of theta constants defining the moduli space of abelian varieties are known if the level is divisible by 8 (see [Mum67, §6]).

- (Section 2.3) It is well-known that the 4-theta null point of the Jacobian variety of a hyperelliptic curve can be computed using the Thomae formulas. One can extend the 4-theta null point to a $(2^\nu p)$-theta null point using the equations for level $2^\nu p$ that are given in Section 2.2.

- (Section 2.4) We give a transformation formula which relates a certain quotient of theta null values of the canonical lift for level $2^\nu p$ with the product of the invertible eigenvalues of the absolute Frobenius morphism acting on the reduction.

In Section 3 we give a point counting algorithm for generic ordinary hyperelliptic curves over a finite field of characteristic $p > 2$. In Section 4 we provide a detailed complexity analysis of the latter algorithm. In Section 5, we prove that a closed variety defined from the equations of Section 2.2 has dimension 0. In Section 6 we give some examples that have been computed using an experimental implementation of our algorithm.

**Notations and complexity hypothesis.** We will denote by $\mathbb{F}_q$ a finite field of characteristic $p > 0$ having $q$ elements. Let $\mathbb{Z}_q$ denote the ring of Witt vectors with values in $\mathbb{F}_q$ and by $\mathbb{Q}_q$ the field of fractions of $\mathbb{Z}_q$. There exists a canonical lift $\sigma \in \mathrm{Aut}(\mathbb{Z}_q)$ of the $p$-th power Frobenius morphism of $\mathbb{F}_q$. If $a$ is an element of $\mathbb{Z}_q$ then we denote by $\bar{a}$ its reduction modulo $p$ in $\mathbb{F}_q$. We say that we have computed an element $x \in \mathbb{Z}_q$ to precision $m$, if we we can write down a bit-string representing its class in the quotient ring $\mathbb{Z}_q/p^m\mathbb{Z}_q$. In order to assess the complexity of our algorithm we use the computational model of a Random Access Machine [Pap94]. We assume that the multiplication of two $n$-bit length integers takes $O(n^\mu)$ bit operations. One can take $\mu = 1+\epsilon$ (for $n$ large), $\mu = \log_2(3)$ and $\mu = 2$ using the FFT multiplication algorithm, the Karatsuba algorithm and a naive multiplication method, respectively. Let $x, y \in \mathbb{Z}_q/p^m\mathbb{Z}_q$. For the following we assume the sparse modulus representation which is explained in [CFA$^+$06, pp.239]. Under this assumption one can compute the product $xy$ to precision $m$ by performing $O(\log(q)^\mu m^\mu)$ bit operations.

# 2 Theta relations of level $2p$

In this section we give some original results that form the basis of our point counting algorithm. In order to do explicit canonical lifting it is necessary to find theta identities that describe the *arithmetic invariants of canonical lifts*. It is not difficult to make up a theta relation. A hard problem is to make a 'complete' set of theta relations that is suitable for canonical lifting. We give such a complete set of equations in the following sections. Also we give a special theta relation, deduced from the classical *transformation formula*, which allows one to recover the eigenvalues of the Frobenius from the arithmetic invariant of the canonical lift.

## 2.1 A local $p^2$-correspondence

Let $R$ be a complete noetherian local ring with finite residue field $\mathbb{F}_q$ of characteristic $p > 0$. Suppose that we are given an abelian scheme $A$ over $R$ which has ordinary reduction. Let $\mathscr{L}$ be an ample symmetric line bundle of degree 1 on $A$. Assume that there exists a $\sigma \in \mathrm{Aut}(R)$ lifting the $p$-th power Frobenius automorphism of $\mathbb{F}_q$. For $m \geq 1$ we set $Z_m = (\mathbb{Z}/m\mathbb{Z})^g$ where $g$ is the relative dimension of $A$ over $R$.

Now assume that $p > 2$ and let $n \geq 1$ an integer with $(n,p) = 1$, i.e. $n$ is coprime to $p$. Suppose that we are given a symmetric theta structure $\Theta_{2n}$ of type $Z_{2n}$ for $\mathscr{L}^{2n}$ and an isomorphism

$$Z_{p,R} \xrightarrow{\sim} A[p]^{\mathrm{et}}, \tag{1}$$

where $A[p]^{\mathrm{et}}$ denotes the maximal étale quotient of $A[p]$. By [Car07, Th.2.2] there exists a canonical theta structure $\Theta_p$ of type $Z_p$ for the line bundle $\mathscr{L}^p$ which is uniquely determined by the isomorphism (1). Let $\Theta_{2np} = \Theta_{2n} \times \Theta_p$ be the semi-canonical symmetric product theta structure of type $Z_{2np}$ for $\mathscr{L}^{2np}$ (see [CKL08, §3.2]).

We denote the theta null point with respect to the theta structure $\Theta_{2np}$ by $(a_u)_{u \in Z_{2np}}$. In the following we consider $Z_2$, $Z_{np}$ and $Z_{2p}$ as embedded compatibly into $Z_{2np}$. Let $S$ be the set of all 4-tuples $(x, y, v, w) \in Z_{2np}^4$ such that the sets $\{x+y, x-y\}$ and $\{v+pw, v-pw\}$ are equal and contained in $Z_{np}$.

**Theorem 2.1.** *There exists an $\omega \in R^*$ such that for all $(x,y,v,w) \in S$ one has*

$$\sum_{z\in Z_2} a_{x+z}a_{y+z} = \omega \sum_{u\in Z_{2p}} a_{v+pu}a_{w+u}^{\sigma^2}.$$

*Proof.* Assume that we have chosen an isomorphism

$$Z_{p^3,R} \xrightarrow{\sim} A[p^3]^{\mathrm{et}} \tag{2}$$

which induces the trivialization (1) if one restricts to $Z_p$. The choice of the isomorphism (2) possibly requires a local-étale extension of the base. Nevertheless, the resulting formulas are defined over the original ring $R$. By [Car07, Th.2.2] there exists a canonical theta structure $\Theta_{p^3}$ of type $Z_{p^3}$ for the line bundle $\mathscr{L}^{p^3}$ depending on the trivialization (2). By [Car, Lem.2.1] the theta structures $\Theta_{p^3}$ and $\Theta_p$ are $p^2$-compatible in the sense of [Car, Def.5.5]. By [CKL08, Lem.3.3] there exists a semi-canonical product theta structure $\Theta_{2np^3} = \Theta_{2n} \times \Theta_{p^3}$ of type $Z_{2np^3}$ for $\mathscr{L}^{2np^3}$. We remark that by [Car07, Th.5.1] and [CKL08, Lem.3.2] the canonical theta structure $\Theta_{p^3}$ is symmetric. Hence by [CKL08, Lem.3.4] the theta structures $\Theta_p$, $\Theta_{2np}$, $\Theta_{p^3}$ and $\Theta_{2np^3}$ form a compatible system. Because of the symmetry of the theta structure $\Theta_{2n}$ there exists a theta structure $\Theta_n$ of type $Z_n$ for $\mathscr{L}^n$ which is 2-compatible with $\Theta_{2n}$ (see [Mum66, §2,Rem.1]). By the same reasoning as above there exists a semi-canonical product theta structure $\Theta_{np} = \Theta_n \times \Theta_p$ which is 2-compatible with $\Theta_{2np}$.

Suppose that we are given a rigidification of the line bundle $\mathscr{L}$. We set $V(Z_m) = \underline{\mathrm{Hom}}(Z_{m,R}, \mathcal{O}_R)$ for $m \geq 1$. Recall that $V(Z_m)$ is the module of finite theta functions as defined in [Mum66, §1]. One can choose theta group equivariant isomorphisms

$$\mu_i : \pi_* \mathscr{L}^i \xrightarrow{\sim} V(Z_i),$$

where $i \in I = \{np, 2np, 2np^3\}$ and where $\pi : A \to \mathrm{Sp}(R)$ denotes the structure morphism. The isomorphisms $\mu_i$ induce finite theta functions $q_{\mathscr{L}^i} \in V(Z_i)$ where $i \in I$ .

It follows from Corollary 2.5 taking $i = j = 1$ and $m = -n = p$ that there exists a $\lambda \in R^*$ such that

$$q_{\mathscr{L}^{np}}(v+pw)q_{\mathscr{L}^{np}}(v-pw) = \lambda \sum_{u\in Z_{2p}} q_{\mathscr{L}^{2np}}(v+pu)q_{\mathscr{L}^{2np^3}}(w+u).$$

It follows by [CKL08, Th.2.4] and [Car, Th2.3] in conjunction with [Car, Lem2.2] and [CKL08, Lem.3.5] that

$$q_{\mathscr{L}^{np}}(v+pw)q_{\mathscr{L}^{np}}(v-pw) = \lambda \sum_{u\in Z_{2p}} q_{\mathscr{L}^{2np}}(v+pu)q_{\mathscr{L}^{2np}}(w+u)^{\sigma^2}. \tag{3}$$

Corollary 2.5 implies by means of the choice $i = j = p$ and $m = -n = 1$ that there exists a $\lambda \in R^*$ such that

$$q_{\mathscr{L}^{np}}(x+y)q_{\mathscr{L}^{np}}(x-y) = \lambda \sum_{z\in Z_2} q_{\mathscr{L}^{2np}}(x+z)q_{\mathscr{L}^{2np}}(y+z). \tag{4}$$

By the assumption that $(x,y,v,w) \in S$, the left hand sides of the equations (3) and (4) are equal. As a consequence, there exists an $\omega \in R^*$ such that

$$\sum_{z \in Z_2} q_{\mathscr{L}^{2np}}(x+z) q_{\mathscr{L}^{2np}}(y+z) = \omega \sum_{u \in Z_{2p}} q_{\mathscr{L}^{2np}}(v+pu) q_{\mathscr{L}^{2np}}(w+u)^{\sigma^2}.$$

This completes the proof of the theorem. $\square$

In the following we illustrate Theorem 2.1 by some examples.

**Example $g = 1$, $n = 1$, $p = 3$:**

$$\begin{aligned}
a_1a_0 + a_2a_3 &= \omega(a_1a_0^{\sigma^2} + a_2a_3^{\sigma^2} + 2a_1a_2^{\sigma^2} + 2a_2a_1^{\sigma^2}) \\
a_2a_0 + a_1a_3 &= \omega(2a_1a_1^{\sigma^2} + a_2a_0^{\sigma^2} + a_1a_3^{\sigma^2} + 2a_2a_2^{\sigma^2}) \\
a_3a_3 + a_0a_0 &= \omega(2a_0a_2^{\sigma^2} + a_3a_3^{\sigma^2} + 2a_3a_1^{\sigma^2} + a_0a_0^{\sigma^2}) \\
a_0a_3 + a_3a_0 &= \omega(a_0a_3^{\sigma^2} + 2a_3a_2^{\sigma^2} + a_3a_0^{\sigma^2} + 2a_0a_1^{\sigma^2})
\end{aligned}$$

**Example $g = 1$, $n = 1$, $p = 5$:**

$$\begin{aligned}
a_2a_0 + a_3a_5 &= \omega(2a_3a_3^{\sigma^2} + 2a_3a_1^{\sigma^2} + a_2a_0^{\sigma^2} + 2a_2a_4^{\sigma^2} + 2a_2a_2^{\sigma^2} + a_3a_5^{\sigma^2}) \\
a_2a_5 + a_3a_0 &= \omega(2a_2a_3^{\sigma^2} + a_2a_5^{\sigma^2} + 2a_3a_4^{\sigma^2} + 2a_3a_2^{\sigma^2} + 2a_2a_1^{\sigma^2} + a_3a_0^{\sigma^2}) \\
a_0a_5 + a_5a_0 &= \omega(a_0a_5^{\sigma^2} + 2a_5a_4^{\sigma^2} + 2a_0a_3^{\sigma^2} + 2a_5a_2^{\sigma^2} + a_5a_0^{\sigma^2} + 2a_0a_1^{\sigma^2}) \\
a_4a_0 + a_1a_5 &= \omega(a_4a_0^{\sigma^2} + 2a_1a_1^{\sigma^2} + a_1a_5^{\sigma^2} + 2a_1a_3^{\sigma^2} + 2a_4a_4^{\sigma^2} + 2a_4a_2^{\sigma^2}) \\
a_5a_5 + a_0a_0 &= \omega(2a_0a_2^{\sigma^2} + 2a_5a_1^{\sigma^2} + 2a_0a_4^{\sigma^2} + a_5a_5^{\sigma^2} + 2a_5a_3^{\sigma^2} + a_0a_0^{\sigma^2}) \\
a_1a_0 + a_4a_5 &= \omega(a_1a_0^{\sigma^2} + 2a_4a_3^{\sigma^2} + a_4a_5^{\sigma^2} + 2a_1a_4^{\sigma^2} + 2a_1a_2^{\sigma^2} + 2a_4a_1^{\sigma^2})
\end{aligned}$$

### 2.1.1 A generalized theta multiplication formula

In the following we give a generalized multiplication formula in the context of Mumford's algebraic theta functions. We only sketch a proof. For more details we refer to [Koi76] and [Kem89].

Let $A$ be an abelian scheme over a local ring $R$ and let $\xi$ denote the isogeny $A^2 \to A^2$ given by the matrix

$$\begin{pmatrix} 1 & m \\ 1 & n \end{pmatrix}$$

where $m, n \in \mathbb{Z}$. Let $i, j \geq 1$ and $I = \{i, j, i+j, im^2+jn^2\}$. Assume that we are given an ample symmetric line bundle $\mathscr{L}$ on $A$ and compatible theta structures $\Theta_i$ for $\mathscr{L}^i$ of type $K_i$ where $i \in I$. We set $\mathcal{M}_{i,j} = p_1^*\mathscr{L}^i \otimes p_2^*\mathscr{L}^j$.

**Lemma 2.2.** *Suppose that $im + jn = 0$. Then one has*

$$\xi^*\mathcal{M}_{i,j} \cong \mathcal{M}_{i+j, im^2+jn^2}.$$

*Proof.* Let $(a,b) \in A^2$. We define

$$s_1 : A \to A^2, x \mapsto (a,x) \quad \text{and} \quad s_2 : A \to A^2, x \mapsto (x,b).$$

One computes

$$s_2^* \mathcal{M}_{i,j} = s_2^* p_1^* \mathscr{L}^i \otimes s_2^* p_2^* \mathscr{L}^j = (p_1 \circ s_2)^* \mathscr{L}^i \otimes (p_2 \circ s_2)^* \mathscr{L}^j = \mathscr{L}^i$$

where $p_k : A^3 \to A$ denotes the projection on the $k$-th factor. Similarly, we have $s_1^* \mathcal{M}_{i,j} = \mathscr{L}^j$. Also we have

$$\begin{aligned} s_2^* \xi^* \mathcal{M}_{i,j} &= (p_1 \circ \xi \circ s_2)^* \mathscr{L}^i \otimes (p_2 \circ \xi \circ s_2)^* \mathscr{L}^j = T_{[m]b}^* \mathscr{L}^i \otimes T_{[n]b}^* \mathscr{L}^j \\ &\overset{(*)}{=} \left(T_b^* \mathscr{L}^{im} \otimes \mathscr{L}^{-i(m-1)}\right) \otimes \left(T_b^* \mathscr{L}^{jn} \otimes \mathscr{L}^{-j(n-1)}\right) \\ &= T_b^* \mathscr{L}^{im+jn} \otimes \mathscr{L}^{-(im+jn)+(i+j)} = \mathscr{L}^{i+j}. \end{aligned}$$

The latter equality follows by our assumption $im + jn = 0$. The equality $(*)$ is implied by the *Theorem of the Square.* Now take $a = 0_A$ where $0_A$ denotes the zero section of $A$. Then one has

$$\begin{aligned} s_1^* \xi^* \mathcal{M}_{i,j} &= (p_1 \circ \xi \circ s_1)^* \mathscr{L}^i \otimes (p_2 \circ \xi \circ s_1)^* \mathscr{L}^j \\ &= [m]^* \mathscr{L}^i \otimes [n]^* \mathscr{L}^j = \mathscr{L}^{im^2+jn^2}. \end{aligned}$$

The latter equality comes from the symmetry of the line bundle $\mathscr{L}$. The proposition now follows by applying the *Seesaw Principle.* □

Assume now that we are given $n, m \in \mathbb{Z}$ such that $im + jn = 0$. There exists a product theta structure $\Theta_{i,j}$ of type $K_{i,j}$ for $\mathcal{M}_{i,j}$ where $K_{i,j} = K_i \times K_j$. On top of Lemma 2.2 one can verify that the theta structure $\Theta_{i+j,im^2+jn^2}$ is $\xi$-compatible with the theta structure $\Theta_{i,j}$ (compare [Mum66, §3] and [CKL08, Lem.3.8]). Hence we can apply the Isogeny Theorem (see [Mum66, §1,Th.4]) in order to get the following general addition formula.

**Proposition 2.3.** *There exists a $\lambda \in R^*$ such that for all $g \in V(K_{i,j})$ and $(x,y) \in K_{i+j,im^2+jn^2}$ we have*

$$\xi^*(g)(x,y) = \begin{cases} \lambda g\big(\xi(x,y)\big), & \xi(x,y) \in K_{i,j} \\ 0 & , \text{else} \end{cases}$$

Here we denote by $V(K_{i,j})$ the module of finite theta functions of type $K_{i,j}$. We define for $x \in K_{i+j}$

$$G_x = \{y \in K_{im^2+jn^2} | \xi(x,y) \in K_{i,j}\}.$$

Here $K_{im^2+jn^2}$ and $K_{i,j}$ are considered as subgroups of $A$ and $A^2$ via the theta structures $\Theta_{i+j,im^2+jn^2}$ and $\Theta_{i,j}$, respectively. As a corollary of Proposition 2.3 we get the following theorem.

**Theorem 2.4** (General Multiplication Formula)**.** *There exists a $\lambda \in R^*$ such that for all $x \in K_{i+j}$, $f_1 \in V(K_i)$ and $f_2 \in V(K_j)$ we have*

$$(f_1 \star f_2)(x) = \lambda \sum_{y \in G_x} f_1(x+my) f_2(x+ny) q_{\mathscr{L}^{im^2+jn^2}}(y).$$

The $\star$-product is defined as in [Mum66, §3]. A proof of Theorem 2.4 in terms of the classical analytic theory is given in [Koi76]. In [Kem89] the author sketches a proof of the general multiplication formula over a field of positive characteristic. We remark that for $i = j = m = -n = 1$ one obtains Mumford's 2-multiplication formula [Mum66, §3].

**Corollary 2.5.** *There exists a $\lambda \in R^*$ such that for all $(a, b) \in K_{i,j}$ we have*

$$q_{\mathscr{L}^i}(a) q_{\mathscr{L}^j}(b) = \lambda \sum_{\xi(x,y)=(a,b)} q_{\mathscr{L}^{i+j}}(x) q_{\mathscr{L}^{im^2+jn^2}}(y).$$

## 2.2 Riemann's equations for level $2^\nu p$

We use the notation that has been introduced in Section 2.1. Let $R$ be a noetherian local ring, $\ell > 0$ a prime and $\nu \geq 1$ an integer. Suppose we are given an abelian scheme $A$ of relative dimension $g$ over $R$. Assume that we are given an ample symmetric line bundle $\mathscr{L}$ of degree 1 on $A$ and a symmetric theta structure of type $Z_{2^\nu \ell}$ for the line bundle $\mathscr{L}^{2^\nu \ell}$ where $Z_{2^\nu \ell}$ is as in Section 2.1. We denote the theta null point with respect to the theta structure $\Theta_{2^\nu \ell}$ by $(a_u)_{u \in Z_{2^\nu \ell}}$. By symmetry we have $a_u = a_{-u}$ for all $u \in Z_{2^\nu \ell}$.

The higher dimensional analogue of *Riemann's equation* for the case of a level-$2^\nu \ell$ theta structure is given by the following theorem. We consider quadruples $(v_i, w_i, x_i, y_i) \in Z_{2^\nu \ell}^4$ where $i = 1, 2$ as equivalent if there exists a permutation matrix $P \in \mathrm{Mat}_4(\mathbb{Z})$ such that

$$(v_1 + w_1, v_1 - w_1, x_1 + y_1, x_1 - y_1) = (v_2 + w_2, v_2 - w_2, x_2 + y_2, x_2 - y_2)P.$$

Let $\hat{Z}_2$ be the character group of $Z_2$.

**Theorem 2.6.** *For equivalent quadruples $(v_1, w_1, x_1, y_1), (v_2, w_2, x_2, y_2) \in Z_{2^\nu \ell}^4$ and for all $\chi \in \hat{Z}_2$ the following equality holds*

$$\begin{aligned} &\sum_{t \in Z_2} \chi(t) a_{v_1+t} a_{w_1+t} \sum_{s \in Z_2} \chi(s) a_{x_1+s} a_{y_1+s} \\ &\qquad = \sum_{t \in Z_2} \chi(t) a_{v_2+t} a_{w_2+t} \sum_{s \in Z_2} \chi(s) a_{x_2+s} a_{y_2+s}. \end{aligned}$$

We refer to [Mum66, §3] for a proof of this theorem.

**Example $g = 1$, $p = 3$, $\nu = 1$:**

$$\begin{aligned} 0 = &\quad a_1 a_0^2 a_3 - 2a_1^2 a_2^2 + a_2 a_0 a_3^2 \\ 0 = &\quad a_2 a_0^3 + a_1 a_0^2 a_3 - a_2^4 - 2a_1^2 a_2^2 - a_1^4 + a_1 a_3^3 + a_2 a_0 a_3^2 \end{aligned}$$

**Example** $g = 1$**,** $p = 5$**,** $\nu = 1$**:**

$$
\begin{aligned}
0 =\ & -a_5^2a_2a_4 + a_2^2a_4^2 + a_3^2a_4^2 - a_1a_0^2a_3 + a_1^2a_2^2 - a_5^2a_1a_3 + a_1^2a_3^2 - a_2a_0^2a_4 \\
0 =\ & -a_1^2a_0a_4 + a_2a_3^2a_4 - a_5a_1a_4^2 + a_1a_2^2a_3 \\
0 =\ & -a_5a_0a_3a_4 + 2a_1a_2a_3a_4 - a_5a_1a_2a_0 \\
0 =\ & -a_5^2a_2a_0 + 2a_1^2a_4^2 - a_5a_0^2a_3 \\
0 =\ & a_2^3a_0 - a_1^3a_3 + a_5a_3^3 + a_2a_0a_3^2 + a_5a_2^2a_3 - a_1a_3a_4^2 - a_2a_4^3 - a_1^2a_2a_4 \\
0 =\ & -2a_1a_2a_3a_4 + a_5^2a_1a_3 - a_1^2a_3^2 + a_5a_1a_2a_0 + a_2a_0^2a_4 - a_2^2a_4^2 + a_5a_0a_3a_4 \\
0 =\ & -a_5^2a_2a_4 + a_3^2a_4^2 - a_5a_0a_3a_4 + a_1^2a_2^2 + 2a_1a_2a_3a_4 - a_5a_1a_2a_0 - a_1a_0^2a_3 \\
0 =\ & a_5^2a_0a_4 - 2a_2^2a_3^2 + a_5a_1a_0^2 \\
0 =\ & a_2a_0a_3^2 + a_5a_2^2a_3 - a_1a_3a_4^2 - a_1^2a_2a_4 \\
0 =\ & -a_1^2a_0a_4 + a_2^3a_4 + a_1a_3^3 - a_0a_4^3 - a_5a_1^3 - a_5a_1a_4^2 + a_2a_3^2a_4 + a_1a_2^2a_3 \\
0 =\ & a_2a_0^3 - a_1^4 + a_5a_0^2a_3 + a_5^3a_3 + a_5^2a_2a_0 - 2a_1^2a_4^2 - a_4^4 \\
0 =\ & a_5^3a_1 - a_2^4 + a_0^3a_4 + a_5^2a_0a_4 - a_3^4 - 2a_2^2a_3^2 + a_5a_1a_0^2
\end{aligned}
$$

## 2.3 Theta null points of level $2^\nu p$

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 2$. Let $A_{\mathbb{F}_q}$ be an ordinary abelian variety over $\mathbb{F}_q$. Suppose that we are given a semi-canonical symmetric product theta structure $\Theta_{2^\nu p} = \Theta_{2^\nu} \times \Theta_p$ as in Section 2.1. We denote the theta null point with respect to the theta structure $\Theta_{2^\nu}$ by $(a_u)_{u \in Z_{2^\nu}}$. We can assume that there exists a $v \in Z_{2^\nu}$ such that $a_v$ is a unit in $\mathbb{Z}_q$. Here $Z_{2^\nu}$ is considered as a subgroup of $Z_{2^\nu p}$ via the map $j \mapsto pj$. Let $I$ be the ideal of the multivariate polynomial ring $\mathbb{F}_q[x_u | u \in Z_{2^\nu p}]$ which is spanned by the relations of Theorem 2.6, taken modulo $p$, together with the symmetry relations $a_u = a_{-u}$ for all $u \in Z_{2^\nu p}$. Let $J$ be the image of $I$ under the specialization map

$$
\mathbb{F}_q[x_u | u \in Z_{2^\nu p}] \to \mathbb{F}_q[x_u | u \in Z_{2^\nu p}, 2^\nu u \neq 0], \quad x_u \mapsto \begin{cases} \frac{a_u}{a_v}, & \text{if} \quad u \in Z_{2^\nu} \\ \frac{x_u}{a_v}, & \text{else} \end{cases} .
$$

The following Theorem is proven in Section 5.

**Theorem 2.7.** *If $\nu \geq 2$, then the ideal $J$ defines a $0$-dimensional affine algebraic set.*

By the primitive element theorem there exists $f(x) \in \mathbb{F}_q[x]$ such that

$$
\mathbb{F}_q[x_u | u \in Z_{2^\nu p}, 2^\nu u \neq 0]/\mathrm{rad}(J) \cong \mathbb{F}_q[x]/(f).
$$

The theta null point $(a_u)_{u \in Z_{2^\nu p}}$ induces an element $z \in \mathbb{F}_q$ such that $f(z) = 0$. Generically, one can obtain the polynomial $f$ by a Groebner basis computation. The Theorem 2.7 enables one to calculate the full theta null point $(a_u)_{u \in Z_{2^\nu p}}$ over $\mathbb{F}_q$ from the knowledge of its $2^\nu$-torsion part. As a consequence, by means of the well-known Thomae formulas and a Groebner basis computation algorithm, one can produce arbitrary theta null points of level $2^\nu p$, which correspond to ordinary hyperelliptic curves over $\mathbb{F}_q$.

We remark that in the case $\nu = 1$, we have computationally verified in many cases that the conclusion of Theorem 2.7 still holds.

## 2.4 A generalized trace formula

Let $A$ be an abelian scheme over $\mathbb{Z}_q$. We assume that $A$ has ordinary reduction and that it is the canonical lift of the reduction $A_{\mathbb{F}_q}$. Suppose that $\Theta_{2^\nu p} = \Theta_{2^\nu} \times \Theta_p$ is a semi-canonical symmetric product theta structure over $\mathbb{Z}_q$ of type $Z_{2^\nu p}$ for $\mathscr{L}^{2^\nu p}$. Let $(a_u)_{u \in Z_{2^\nu p}}$ denote the theta null point with respect to the theta structure $\Theta_{2^\nu p}$.

Let $F \in \mathrm{End}_{\mathbb{F}_q}(A_{\mathbb{F}_q})$ be the absolute Frobenius endomorphism of $A_{\mathbb{F}_q}$, and let $\ell$ be a prime different from the characteristic $p$ of $\mathbb{F}_q$. We denote the $\ell$-adic Tate module of $A_{\mathbb{F}_q}$ by $T_\ell(A_{\mathbb{F}_q})$. Recall that the $\ell$-adic Tate module is a free $\mathbb{Z}_\ell$-module of rank $2g$, where $g$ is the dimension of $A_{\mathbb{F}_q}$. The absolute Frobenius morphism $F$ induces a $\mathbb{Z}_\ell$-linear map $\rho_\ell(F)$ on $T_\ell(A_{\mathbb{F}_q})$ which corresponds, once a basis of $T_\ell(A_{\mathbb{F}_q})$ is chosen, to a $(2g \times 2g)$-matrix $M_F$ with coefficients in $\mathbb{Z}_\ell$. Because of the ordinary reduction, we know that $M_F$ has precisely $g$ Eigenvalues $\pi_1, \ldots, \pi_g$, which are units modulo $p$ [Dem72, Ch.V].

**Theorem 2.8.** *Suppose that $\Theta_{2^\nu}$ is defined over $\mathbb{Z}_q$. Then the product $\pi_1 \cdot \ldots \cdot \pi_g$ is an element of the ring $\mathbb{Z}_q$ and we have*

$$\pi_1 \cdot \ldots \cdot \pi_g = \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\sum_{u \in Z_{2^\nu}} a_u}{\sum_{u \in Z_{2^\nu p}} a_u}\right). \tag{5}$$

Here $Z_{2^\nu}$ is considered as a subgroup of $Z_{2^\nu p}$ via the map $j \mapsto pj$.

The rest of this section is devoted to the proof of Theorem 2.8. We first fix some additional notations. If $\mathscr{L}$ is a line bundle on an abelian variety, we denote by $K(\mathscr{L})$ the kernel of the isogeny $A \to \mathrm{Pic}^0_A$ induced by $\mathscr{L}$. Denote by $\mathscr{G}(\mathscr{L})$ the theta group associated to $\mathscr{L}$ (see [Mum66, pp. 289]). For any positive integer $n$, we denote the Heisenberg group of type $Z_n$ by $\mathcal{H}(Z_n)$ [BL04, pp. 161]. Denote by $\hat{Z}_n$ the dual of $Z_n$, we have by definition $\mathcal{H}(Z_n) = \mathbb{G}_m \times Z_n \times \hat{Z}_n$ together with the group law defined by

$$(\alpha, x, l).(\alpha', x', l') = (\alpha.\alpha' l'(\alpha), x + x', l.l').$$

where $(\alpha, x, l)$ and $(\alpha', x', l')$ are points of $\mathcal{H}(Z_n)$.

During the course of the proof, as we are working with schemes over different base rings, to avoid ambiguity, we recall the base ring in subscript. In particular, we let $A = A_{\mathbb{Z}_q}$, $\mathscr{L} = \mathscr{L}_{\mathbb{Z}_q}$ and $\Theta_{2^\nu p} = \Theta_{\mathbb{Z}_q, 2^\nu p}$. We recall that $\Theta_{2^\nu p}$ induces a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}^{2^\nu p}) \times K_2(\mathscr{L}^{2^\nu p})$ into isotropic subgroups $K_1(\mathscr{L}^{2^\nu p})$ and $K_2(\mathscr{L}^{2^\nu p})$ for the commutator pairing.

We fix an embedding $\psi : \mathbb{C}_p \to \mathbb{C}$ where $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$ [Rob00, Ch.3]. The base extended abelian variety $A_{\mathbb{C}} = A_{\mathbb{Z}_q} \times_\psi$

$Spec(\mathbb{C})$ is a complex variety with a polarization $\mathscr{L}_{\mathbb{C}}^{2^\nu p}$ defined by $\mathscr{L}_{\mathbb{C}}^{2^\nu p} = \mathscr{L}_{\mathbb{Z}_q}^{2^\nu p} \otimes_\psi \mathbb{C}$. We remark that $K(\mathscr{L}_{\mathbb{C}}^{2^\nu p})$ comes equipped with a Lagrangian decomposition which is inherited from the theta structure $\Theta_{2^\nu p, \mathbb{C}} = \Theta_{2^\nu p} \otimes \mathbb{C}$. From the above decomposition we deduce the period matrix $(I \Omega)$ with $I$ the $g$ dimensional unity matrix and $\Omega$ an element of $\mathbb{H}_g$ the $g$ dimensional Siegel upper half space. In the following, for any $\Omega \in \mathbb{H}_g$, we denote by $\Lambda_\Omega$ the lattice $\mathbb{Z}^g + \Omega\mathbb{Z}^g$. If we let $A_{an} = \mathbb{C}^g/\Lambda_\Omega$, we have an analytic isomorphism $j_{an} : A_{\mathbb{C}} \to A_{an}$. Let $\kappa : \mathbb{C}^g \to \mathbb{C}^g/\Lambda_\Omega$ be the canonical projection.

We can suppose that $\Omega$ is chosen such that the $p$-torsion points of $A_{an}$, given by $\kappa((1/p).\mathbb{Z}^g)$ corresponds via $j_{an}^{-1}$ to a canonical lift of the maximal étale quotient of $A_{\mathbb{Z}_q}[p]$, where $A_{\mathbb{Z}_q}$ is identified to $A_{\mathbb{C}}$ via $\psi$.

For $\epsilon_1, \epsilon_2 \in \mathbb{Z}^g$ and $l \in \mathbb{Z}$, we define the theta function with rational characteristics as

$$\theta_l \left[ \begin{smallmatrix} \epsilon_1 \\ \epsilon_2 \end{smallmatrix} \right] (z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left[ \pi i^t (n + \frac{\epsilon_1}{l}) \Omega (n + \frac{\epsilon_1}{l}) + 2\pi i^t (n + \frac{\epsilon_1}{l}).(z + \frac{\epsilon_2}{l}) \right]. \quad (6)$$

Recall that $(a_u)_{u \in Z_{2^\nu p}}$ denote the theta null point with respect to the theta structure $\Theta_{2^\nu p}$. We have the

**Lemma 2.9.** *There exists a constant factor $\lambda \in \mathbb{C}$, $\chi \in \hat{Z}_{2^\nu p}$ a character of order 2 and $\delta \in Z_2$, such that for all $u \in Z_{2^\nu p}$,*

$$(a_u \otimes_{\mathbb{Q}_q} \mathbb{C}) = \lambda \chi(u) \theta_{2^\nu p} \left[ \begin{smallmatrix} 0 \\ u+\delta \end{smallmatrix} \right] (0, 1/(2^\nu p).\Omega), \quad (7)$$

*where $Z_2$ is considered as a subgroup of $Z_{2^\nu p}$ via the map $j \mapsto j2^{\nu-1}p$.*

*Proof.* From the theta structure $\Theta_{\mathbb{Z}_q, 2^\nu p}$ of type $Z_{2^\nu p}$ we deduce immediately by tensoring with $\mathbb{C}$ a theta structure $\Theta_{\mathbb{C}, 2^\nu p}$ of type $Z_{2^\nu p}$ for $\mathscr{L}_{\mathbb{C}}^{2^\nu p}$. Then $(a_u \otimes_{\mathbb{Q}_q} \mathbb{C})_{u \in Z_{2^\nu p}}$ is the theta null point defined by the theta structure $\Theta_{\mathbb{C}, 2^\nu p}$. As $\mathscr{L}_{\mathbb{C}}^{2^\nu p}$ is by hypothesis a symmetric line bundle, by [BL04, Lem.4.6.2], there exists a $\overline{c} \in A_{\mathbb{C}}[2] \cap K(\mathscr{L}_{\mathbb{C}}^{2^\nu p})$ such that $\tau_{\overline{c}}^*(\mathscr{L}_{\mathbb{C}}^{2^\nu p}) \simeq \mathscr{L}_0^{2^\nu p}$, where $\tau_{\overline{c}}$ denotes the translation by $\overline{c}$ and $\mathscr{L}_0^{2^\nu p}$ is the canonical bundle associate to the decomposition provided by the matrix period $\Omega$ (see [BL04, Lem.3.1.1]).

The line bundle $\mathscr{L}_0^{2^\nu p}$ comes with a symmetric theta structure $\Theta_0$ defined by the decomposition associated to $\Omega$ and the element $0 \in K(\mathscr{L}_0^{2^\nu p})$ (see [BL04, Lem.6.6.5]). The theta null point for the theta structure $\Theta_0$ is

$$(\theta_{2^\nu p} \left[ \begin{smallmatrix} 0 \\ u \end{smallmatrix} \right] (0, 1/(2^\nu p).\Omega))_{u \in Z_{2^\nu p}}$$

by [BL04, Prop.6.7.1].

As $\overline{c} \in K(\mathscr{L}_{\mathbb{C}}^{2^\nu p})$, we have an isomorphism of theta groups $\zeta : \mathscr{G}(\mathscr{L}_{\mathbb{C}}^{2^\nu p}) \to \mathscr{G}(\mathscr{L}_0^{2^\nu p})$ defined by $\zeta((y, \psi_y)) = (y, \tau_y^* \tau_{\overline{c}}^* \circ \psi_y \circ \tau_{\overline{c}}^{-1*})$. Note that this isomorphism induces the identity on $K(\mathscr{L}_{\mathbb{C}}^{2^\nu p}) = K(\mathscr{L}_0^{2^\nu p})$.

The isomorphism $\Theta_0 \circ \zeta : \mathscr{G}(\mathscr{L}_{\mathbb{C}}^{2^\nu p}) \to \mathcal{H}(Z_{2^\nu p})$ is a theta structure for $\mathscr{G}(\mathscr{L}_{\mathbb{C}}^{2^\nu p})$. Denote by $\overline{\Theta}_0$ the morphism $K(\mathscr{L}_{\mathbb{C}}^{2^\nu p}) \to Z_{2^\nu p} \times \hat{Z}_{2^\nu p}$ deduced from

$\Theta_0$. By definition of $\zeta$, the theta null point for the theta structure $\Theta_0 \circ \zeta$ is deduced from the theta null point for $\Theta_0$ by acting upon it with $\overline{\Theta}_0(c)$ (for a definition of this action see [Mum66, pp.297]) so that it can be written as $(\chi_1(u)\theta\left[\begin{smallmatrix}0\\u+\delta_1\end{smallmatrix}\right](z, 1/(2^\nu p).\Omega))_{u\in Z_{2^\nu p}}$ where$\overline{\Theta}_0(c) = (\delta_1, \chi_1) \in Z_{2^\nu p} \times \hat{Z}_{2^\nu p}$.

As $\Theta_{\mathbb{C},2^\nu p}$ and $\Theta_0 \circ \zeta$ are two symmetric theta structures of $\mathscr{L}_{\mathbb{C}}^{2^\nu p}$ which induce the same symplectic isomorphism $\overline{\Theta}_0$, they are defined up to a translation by an element $c_0$ in $A_{\mathbb{C}}[2]$ by [BL04, Prop.6.9.4]. Let $(\delta_2, \chi_2) = \overline{\Theta}_0(c_0)$, a theta null point for $\mathscr{L}_{\mathbb{C}}^{2^\nu p}$ with the theta structure $\Theta_{\mathbb{C},2^\nu p}$ is given modulo multiplication by a factor independent of $u$ by

$$(\chi_1(u)\chi_2(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\u+\delta_1+\delta_2\end{smallmatrix}\right](z, 1/(2^\nu p).\Omega))_{u\in Z_{2^\nu p}}.$$

We remark that $\chi_1, \chi_2$ and $\chi$ are charaters of order 2 of $Z_{2^\nu p}$. We conclude the proof by setting $\delta = \delta_1 + \delta_2$ and $\chi = \chi_1.\chi_2$. □

**Lemma 2.10.** *Let $F$ be the Frobenius morphism acting on $A_{\mathbb{F}_q}$ and let $\pi_1, \dots, \pi_g$ be the Eigenvalues of the $\ell$-adic representation $\rho_\ell(F)$ which are units modulo $p$. Let $n = \log_p(q)$. For all $\epsilon_1, \epsilon_2 \in Z_2$, we have*

$$\frac{\theta_2\left[\begin{smallmatrix}\epsilon_1\\\epsilon_2\end{smallmatrix}\right](0, 2^\nu.\Omega)^2}{\theta_2\left[\begin{smallmatrix}\epsilon_1\\\epsilon_2\end{smallmatrix}\right](0, 2^\nu p^n.\Omega)^2} = \pi_1 \dots \pi_g.$$

*Proof.* Let $A'_{\mathbb{Z}_q}$ be the quotient of $A_{\mathbb{Z}_q}$ by $K_1(\mathscr{L}_{\mathbb{Z}_q}^{2^\nu p})[2^\nu]$ the maximal $2^\nu$-torsion subgroup of $K_1$. As $K_1(\mathscr{L}_{\mathbb{Z}_q}^{2^\nu p})[2^\nu]$ is an isotropic subgroup of $K(\mathscr{L}_{\mathbb{Z}_q}^{2^\nu p})$ for the commutator pairing, the line bundle $\mathscr{L}_{\mathbb{Z}_q}^{2^\nu p}$ descends to a line bundle $\mathscr{L}'^p_{\mathbb{Z}_q}$ on $A'_{\mathbb{Z}_q}$ which comes with a Lagrangian decomposition $K(\mathscr{L}'^p_{\mathbb{Z}_q}) = K_1(\mathscr{L}'^p_{\mathbb{Z}_q}) \times K_2(\mathscr{L}'^p_{\mathbb{Z}_q})$ and a theta structure $\Theta'_p$ of type $Z_p$ inherited from $\Theta_{2^\nu p}$ by [Mum66, Prop.2].

We remark that $A'_{\mathbb{Z}_q}$ being the quotient of $A_{\mathbb{Z}_q}$ by an étale subgroup is a canonical lift of its special fiber $A'_{\mathbb{F}_q}$. As before, we can consider $A'_{\mathbb{C}} = A'_{\mathbb{Q}_p} \otimes_\psi \mathbb{C}$ and we have an isomorphism of analytic varieties $j' : A'_{\mathbb{C}} \to A'_{an} = \mathbb{C}^g/\Lambda_{2^\nu\Omega}$. Let $\kappa' : \mathbb{C}^g \to A'_{\mathbb{C}}$ be the canonical projection. By the choice we have made on $\Omega$, the $p-$torsion points of $A'_{an}$ given by $\kappa'(1/p.\mathbb{Z}^g)$ correspond via $j'^{-1}$ to a canonical lift of the maximal étale quotient of $A'_{\mathbb{Z}_q}[p]$.

We can then consider the analytic variety $A'^n_{an} = \mathbb{C}^g/\Lambda_{p^n 2^\nu\Omega}$. The inclusion of lattices $\Lambda_{p^n 2^\nu\Omega} \subset \Lambda_{2^\nu\Omega}$ gives an isogeny $\iota : A'^n_{an} \to A'_{an}$. Using exactly the same proof as in [Rit03, pp.78], one obtains that $\iota$ is a lift of the Frobenius morphism acting on $A'_k$, that $A'^n_{an}$ and $A'_{an}$ are two representatives of the same class element of $\mathbb{H}_g/\Gamma_g(p)$. Moreover, for all $\epsilon_1, \epsilon_2 \in Z_2$ we have

$$\theta_2\left[\begin{smallmatrix}\epsilon_1\\\epsilon_2\end{smallmatrix}\right](0, 2^\nu.\Omega)^2 = (\pi_1 \dots \pi_g)\theta_2\left[\begin{smallmatrix}\epsilon_1\\\epsilon_2\end{smallmatrix}\right](0, 2^\nu p^n.\Omega)^2,$$

where $\pi_1, \dots, \pi_g$ are the $g$ Eigenvalues of the $\ell$-adic representation of the Frobenius morphism acting on $A'_{\mathbb{F}_q}$ which are units modulo $p$.

The hypothesis that $\Theta_{2^\nu}$ is defined over $\mathbb{Z}_q$ implies that $K_1(\mathscr{L}_{\mathbb{F}_q}^{2^\nu p})[2^\nu]$ is defined over $\mathbb{F}_q$. As a consequence, the two abelian varieties $A_{\mathbb{F}_q}$ and $A'_{\mathbb{F}_q}$ are

$\mathbb{F}_q$-isogeneous and, using a theorem of Tate [Tat66], we deduce immediately that they have the same characteristic polynomial of the Frobenius morphism. $\square$

**Lemma 2.11.** *Let $\gamma : Z_{2^\nu} \to Z_{2^\nu p}$, $j \mapsto pj$. For each $\chi \in \hat{Z}_{2^\nu p}$ character of order 2, there exists $\epsilon \in Z_2$ such that*

$$\sum_{u \in Z_{2^\nu}} \chi(\gamma(u))\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ \gamma(u)\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega) = \theta_2\left[\begin{smallmatrix}\epsilon\\ 0\end{smallmatrix}\right](0, (2^\nu/p).\Omega).$$

*We have also:*

$$\sum_{u \in Z_{2^\nu p}} \chi(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ u\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega) = \theta_2\left[\begin{smallmatrix}\epsilon\\ 0\end{smallmatrix}\right](0, 2^\nu p.\Omega).$$

*Proof.* For $l \in \mathbb{N}^*$, $a, b \in Z_l$ and $\Omega_0 \in \mathbb{H}_g$, we put:

$$\begin{aligned} f_a &= \theta_1\left[\begin{smallmatrix}a/l\\ 0\end{smallmatrix}\right](lz, l.\Omega_0) \\ g_b &= \theta_1\left[\begin{smallmatrix}0\\ b/l\end{smallmatrix}\right](z, l^{-1}.\Omega_0) \end{aligned}$$

Then we have the following formula (see [Mum83, pp.124]):

$$f_a = \sum_{a \in Z_l} \exp(-2\pi i \frac{ab}{l}) g_b. \tag{8}$$

Let $\chi \in \hat{Z}_{2^\nu p}$ be a character of order 2 and let $\epsilon \in Z_2$ be such that for all $u \in Z_{2^\nu p}$, we have $\chi(u) = \exp(-\pi i \epsilon u)$. The lemma is obtained by applying formula (8) with $l = 2^\nu$, $\Omega_0 = p\Omega$ and then with $l = 2^\nu p$ and $\Omega_0 = \Omega$. $\square$

We are ready to prove Proposition 2.8. Let $\gamma' : Z_2 \to Z_{2^\nu p}$, $j \mapsto 2^{\nu-1}pj$. By applying successively Lemma 2.9 and Lemma 2.11, we obtain that for an element $\delta \in Z_2$ and $\chi \in Z_{2^\nu p}$ a character of order 2 we have

$$\begin{aligned} \psi\left(\frac{\sum_{u\in Z_{2^\nu}} a_u}{\sum_{u \in Z_{2^\nu p}} a_u}\right) &= \frac{\sum_{u\in Z_{2^\nu}} \chi(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ u+\gamma'(\delta)\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega)}{\sum_{u\in Z_{2^\nu p}} \chi(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ u+\gamma'(\delta)\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega)} \\ &= \frac{\sum_{u\in Z_{2^\nu}} \chi'(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ u\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega)}{\sum_{u\in Z_{2^\nu p}} \chi'(u)\theta_{2^\nu p}\left[\begin{smallmatrix}0\\ u\end{smallmatrix}\right](0, 1/(2^\nu p).\Omega)} \\ &= \frac{\theta_2\left[\begin{smallmatrix}\epsilon\\ 0\end{smallmatrix}\right](0, (2^\nu/p).\Omega)}{\theta_2\left[\begin{smallmatrix}\epsilon\\ 0\end{smallmatrix}\right](0, (2^\nu p).\Omega)}, \end{aligned}$$

where $\chi(u) = \chi'(u + \gamma'(\delta))$ and $\epsilon$ is chosen such that for all $u \in Z_{2^\nu p}$ we have $\chi'(u) = \exp(-\pi i \epsilon u)$. The second equality is due to the fact that $\Delta \in A_{\mathbb{C}} \cap K_1(\mathscr{L}_{\mathbb{C}})$.

On the other side we have

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\psi^{-1}\left(\frac{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,(2^\nu/p).\Omega)}{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,2^\nu p.\Omega)}\right)\right) &= \psi^{-1}\left(\frac{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,(2^\nu/p^n).\Omega)}{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,2^\nu p^n.\Omega)}\right)\\
&= \psi^{-1}\left(\frac{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,2^\nu\Omega)}{\theta_2\left[\begin{smallmatrix}\epsilon\\0\end{smallmatrix}\right](0,2^\nu p^n.\Omega)}\right)^2\\
&= \pi_1\ldots\pi_g,
\end{aligned}$$

by Lemma 2.10.

# 3 Description of the algorithm

In this section we explain how to use the formulas given in Section 2 in order to count points on the Jacobian of a generic ordinary hyperelliptic curve over a finite field of odd characteristic. Assume that we have chosen a prime $p > 2$ and an integer $g \geq 1$.

**Theorem 3.1.** *Let $C$ be an hyperelliptic curve of genus $g$ with all Weierstrass points rational over a finite field $\mathbb{F}_q$ of characteristic $p$ such that the Jacobian $J(C)$ is ordinary and absolutely simple. Let $\nu$ be an integer greater or equal 3, we suppose that the $2^\nu$-torsion of $J(C)$ is defined over $\mathbb{F}_q$. The algorithm for the computation of the number of $\mathbb{F}_q$-rational points $\#C(\mathbb{F}_q)$ of the curve $C$, that we give in the following, has asymptotic time complexity $O(n^{2+o(1)})$ and asymptotic space complexity $O(n^2)$ where $n = \log(\#\mathbb{F}_q)$.*

From Theorem 3.1, we deduce

**Corollary 3.2.** *Let $C$ be an hyperelliptic curve of genus $g$ over a finite field $\mathbb{F}_q$ of characteristic $p$ such that the Jacobian $J(C)$ is ordinary and absolutely simple. There exists an algorithm to compute the number of $\mathbb{F}_q$-rational points $\#C(\mathbb{F}_q)$ of the curve $C$ which has asymptotic time complexity $O(n^{2+o(1)})$ and asymptotic space complexity $O(n^2)$ where $n = \log(\#\mathbb{F}_q)$.*

*Proof.* Let $\nu$ be an integer greater or equal 3. Let $\mathbb{F}_{q^r}$ be an extension of $\mathbb{F}_q$ and consider $C_{\mathbb{F}_{q^r}}$ the curve obtained from $C$ by doing a base field extension from $\mathbb{F}_q$ to $\mathbb{F}_{q^r}$. We suppose that $r$ is chosen such that the $2^\nu$-torsion points of $J(C_{\mathbb{F}_{q^r}})$ are defined over $\mathbb{F}_{q^r}$. Using a rational expression of the group law on $J(C)$, we see that there exists a bound on $r$ which is independent of the choice of $C$ when $g$ is fixed.

Applying Theorem 3.1 we obtain in time $O(n^{2+o(1)})$ the characteristic polynomial $\chi_{F'}$ of the $q^r$-Frobenius morphism $F'$. Let $\alpha'_1, \ldots, \alpha'_{2g}$ be the roots of $\chi_{F'}$. On the other side, let $\alpha_1, \ldots, \alpha_{2g}$ be the roots of $\chi_F$ the characteristic polynomial of the $q$-Frobenius acting on $C$. We have by [Sti93] Theorem V.1.15, ${\alpha'}_i^r = \alpha_i$. By computing the roots $\alpha'_1, \ldots, \alpha'_{2g}$ and taking their $r^{th}$ root, we obtain a finite set of possible roots for $\chi_F$ up to permutation of the indices. In order to finish the proof, we just have to remark that all the above computations for a fixed genus have constant complexity with respect to $\log(q)$. Moreover, it is possible to check the result of the computations in quasi-quadratic time by taking a point $P$ of $J(C)$ and computing $\lambda.P$ where $\lambda$ is the supposed group order of $J(C)$. $\square$

We remark that the existence of such a quasi-quadratic time algorithm in the special case $p = 2$ is proved in [LD06]. In the following we give an algorithm which is expected to have the desired properties. In the case that we take $\nu = 1$ in the statement of Theorem 3.1, we have verified that the correctness of the algorithm still holds by counting points on many examples of elliptic curves in characteristic 3 and 5 and on some genus 2 curves in characteristic 3. Our algorithm follows the so-called lift and norm paradigm which was introduced by Satoh in [Sat00]. The algorithm is as follows.

We assume that the hyperelliptic curve $C$ is given by an equation of the form

$$y^2 = \prod_{i=1}^{2g+2} (x - \overline{\alpha}_i)$$

where $\overline{\alpha_i} \in \mathbb{F}_q$.

**Initialization phase:** Let $J(C)$ be the Jacobian of $C$. The aim of this first phase is to compute the theta null point associated to a semi-canonical product theta structure $\Theta_{2^\nu p} = \Theta_{2^\nu} \times \Theta_p$ for $\mathscr{L}^{2^\nu p}$ (compare Section 2.1) where $\mathscr{L}$ is a degree 1 symmetric ample line bundle on $J(C)$.

This can be done in the following way. First compute the theta null point associated to a theta structure $\Theta_2$ of type $Z_2$ for $\mathscr{L}^2$. By considering any lift $\mathcal{C}$ of $C$ over $W(\mathbb{F}_q)$ defined by lifts $\alpha_i$ of $\overline{\alpha_i}$ over $\mathbb{Z}_q$ and a given embedding $\psi : \mathbb{Z}_q \to \mathbb{C}$ one can view the Jacobian $J(\mathcal{C})$ of the lifted curve $\mathcal{C}$ as a complex abelian variety. One can consider a symplectic basis of $H_1(\mathcal{C}, \mathbb{Z})$ given by $A$-cycles and $B$-cycles as described in [Mum84]. The associated period matrix $\Omega$ of $J(\mathcal{C})$ is an element of $\mathbb{H}_g$, the $g$-dimensional Siegel upper half plane. For $\epsilon_1, \epsilon_2 \in \mathbb{N}^g$ and $l \in \mathbb{N}^*$, we denote by $\theta_l \left[\begin{smallmatrix}\epsilon_1\\ \epsilon_2\end{smallmatrix}\right](z, \Omega)$ the Riemann theta function with rational characteristic given by (6).

According to [Mum83, pp.124] a theta null point associated to a well chosen theta structure of the second power of the degree 1 canonical line bundle defined by $\Omega$ is given by $(a_u)_{u \in Z_2}$ with

$$a_u = \lambda \theta_2 \left[\begin{smallmatrix}0\\ u\end{smallmatrix}\right](0, 1/2\Omega),$$

where $\lambda \in \mathbb{C}^*$. This theta null point, which correspond to the case $\nu = 1$, can be computed in two steps.

**Step 1.** For $i = 1 \dots g$, let $\tau_i$ be the vector $(\tau_{i,j})_{j \in \{1,\dots,g\}}$ such that $\tau_{i,j} = 0$ if $j < i$ and $\tau_{i,j} = 1$ if $i \geq i$. Using the Thomae-Fay formulas [Mum84, pp.121], we compute

$$\theta_1 \left[\begin{smallmatrix}v\\ u\end{smallmatrix}\right](0, \Omega)^2 = \pm \sqrt{\prod_{0 \leqslant i < j \leqslant g} (\alpha_{2i+e_i} - \alpha_{2j+e_j})(\alpha_{2i+1-e_i} - \alpha_{2j+1-e_j})},$$

where $e_0 = 0$ and the vector $(e_i)_{i=1\dots g} \in \mathbb{F}_2^g$ is given by $(e_i) = u + \sum_{i=1}^g v_i.\tau_i$, for $i = 1, \dots, g$, where $v = (v_i) \in \mathbb{F}_2^g$. Here we choose the sign of the square root at random.

**Step 2.** Case $\nu = 1$. We proceed to a reverse duplication step which can be done according to the Riemann duplication formulas [Fay73] by finding $(a_u)_{u\in Z_2}$ such that

$$\theta_2 \left[\begin{smallmatrix} 0 \\ u \end{smallmatrix}\right](0, \Omega)^2 = \frac{1}{2^g} \sum_{v\in Z_2} a_{v+u} a_v.$$

This algebraic system may be solved by using the Groebner basis algorithm and by picking up any solution. We check that we obtain a valid theta null point by computing the associated 4-theta null point and verify that it satisfies the level-4 Riemann type equations (compare with Section 2.2). If this is not the case, we go back to Step one and choose different signs for the square roots.

Let $\mathrm{Sp}(2g, \mathbb{Z})$ be the group of symplectic matrices acting on $\mathbb{H}_g$. Denote by $\Gamma_2$ the subgroup of $\mathrm{Sp}(2g, \mathbb{Z})$ consisting of the elements $\gamma \in \mathrm{Sp}(2g, \mathbb{Z})$ such that $\gamma \equiv I_{2g} \bmod 2$ where $I_{2g}$ is the identity matrix of dimension $2g$. The resulting theta null point $(a_u)_{u\in Z_2}$ has the property that if we raise to the fourth power the coordinates of its image by the Riemann duplication formula, we recover the values deduced from the ramification points $\alpha_i$ of $\mathcal{C}$ by the Thomae formulas. According to [Mum84, pp.3.131] this means that $(a_u)_{u\in Z_2}$ is the theta null point associated to the second power of a degree one symmetric ample line bundle defined by $\Omega'$ where $\Omega' = \gamma.\Omega$ for an element $\gamma \in \Gamma_2$.

As all the computations described in this paragraph are algebraic, they can be made directly in $\mathbb{Z}_q$ using the embedding $\psi$, and even in $\mathbb{F}_q$ as $\mathcal{C}$ has good reduction modulo $p$. This procedure gives the computation of a theta null point $(a_u)_{u\in Z_2}$ for a symmetric theta structure $\Theta_2$ associated to the second power of a degree 1 ample symmetric line bundle $\mathscr{L}$ on $J(C)$. It should be noted that we have to assume that $\Theta_2$ is rational over $\mathbb{F}_q$ in order to have that $a_u \in \mathbb{F}_q$, for $u \in Z_2$.

Now, we describe a variation of Step 2 to cover the case $\nu > 1$.

**Step 2'.** Case $\nu > 1$. From the knowledge of $\theta_1 \left[\begin{smallmatrix} v \\ u \end{smallmatrix}\right](0, \Omega)$, we proceed to two reverse duplication steps which can be done by finding successively for $i = 1, 2$, $u, v \in Z_2$, $\theta_2 \left[\begin{smallmatrix} v \\ u \end{smallmatrix}\right](0, (1/2^i)\Omega)$ such that

$$\theta_2 \left[\begin{smallmatrix} v \\ u \end{smallmatrix}\right](0, (1/2^{i-1})\Omega)^2 = \frac{1}{2^g} \sum_{t\in Z_2} (-1)^{{}^t vt} \theta_2 \left[\begin{smallmatrix} 0 \\ u+t \end{smallmatrix}\right](0, (1/2^i)\Omega) \theta_2 \left[\begin{smallmatrix} 0 \\ u \end{smallmatrix}\right](0, (1/2^i)\Omega).$$

This algebraic system can easily be solved by using the Groebner basis algorithm and by picking up any suitable solution, we obtain $\theta_2 \left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right](0, (1/4).\Omega)$. If $v \in Z_2$, denote by $\hat{v}$ the element of $\hat{Z}_2$ defined by $\hat{v} : Z_2 \to \{-1, 1\} \subset \mathbb{Z}$, $z = (z_i) \mapsto (-1)^{\sum_{i=1}^g z_i v_i}$.

On the other side, we have $Z_2 \simeq Z_4/Z_2$ and let $\phi : Z_2 \simeq Z_4/Z_2 \to Z_4$ be a section of the canonical projection. Let $(b_u)_{u\in Z_4}$ be defined such that

$$\theta_2 \left[ \begin{smallmatrix} v \\ u \end{smallmatrix} \right] (0, (1/4).\Omega) = \sum_{t\in Z_2} \hat{v}(t) b_{\phi(u)+t},$$

where $Z_2$ is considered as a subgroup of $Z_4$ via $j \mapsto 2j$. We can compute $(b_u)_{u\in Z_4}$ from the knowledge of $\theta_4 \left[ \begin{smallmatrix} u \\ v \end{smallmatrix} \right] (0, \Omega)$ by solving a linear system of fixed size.

We know [Mum66, pp.334], that $(b_u)_{u\in Z_4}$ is the theta null point of $J(C)$ associated to a symmetric theta structure of type $Z_4$. Now, plugging $(b_u)_{u\in Z_4}$ into the relations given of the Riemann equations of level $2^\nu$ (compare with Section 2.2) together with the symmetric relations, we know by [Mum67, pp.87] that the so obtained system admits a unique solution $(a_u)_{u\in Z_{2^\nu}}$ which may easily be computed using a Groebner basis algorithm.

**Step 3.** In the following we explain how to compute a level $2^\nu p$-theta null point from the above $2^\nu$-theta null point. We use the notation of Section 2.3. Let $I$ be the ideal of the multivariate polynomial ring $\mathbb{F}_q[x_u | u \in Z_{2^\nu p}]$ which is spanned by the relations of Theorem 2.6 together with the symmetry relations $a_u = a_{-u}$ for $u \in Z_{2^\nu p}$. We find $v \in Z_2$ such that $a_v$ is a unit. Let $J$ be the image of $I$ under the evaluation map

$$\mathbb{F}_q[x_u | u \in Z_{2^\nu p}] \to \mathbb{F}_q[x_u | u \in Z_{2^\nu p}, 2^\nu u \neq 0], \quad x_u \mapsto \begin{cases} \frac{a_u}{a_v}, & u \in Z_{2^\nu} \\ \frac{x_u}{a_v}, & \text{else} \end{cases}$$

If we chose an order on the set of the remaining variables $x_u$, $u \in Z_{2^\nu p} \setminus Z_{2^\nu}$, it defines a well-ordered lexicographic monomial basis on $J$. One can compute a reduced Groebner basis for $J$ with respect to this monomial order. By Theorem 2.7, the closed subscheme of $\mathrm{Spec}(\mathbb{F}_q[x_u | u \in Z_{2^\nu p}, 2^\nu u \neq 0])$ defined by $J$ is of dimension 0. The last polynomial of this reduced Groebner basis is a univariate polynomial $f(x) \in \mathbb{F}_q[x]$ and by [BMMT94], we generically have

$$\mathbb{F}_q[x_u | u \in Z_{2^\nu p}, 2^\nu u \neq 0]/J \simeq \mathbb{F}_q[x]/(f),$$

where the degree of $f$ is uniformly bounded by a function of $g$ and $p$ which is constant with respect to the complexity parameter $\log_p(q)$. According to Theorem 2.7, one can pick up a solution $(a_u)_{u\in Z_{2^\nu p}}$ corresponding to the root of $f$ with multiplicity $p^{2g}$.

**Lift phase** Let $(a_u)_{u\in Z_{2^\nu p}}$ with $a_u \in \mathbb{F}_q$ the null point obtained from the initialization phase. Let $\mathcal{R}$ be the set of polynomials in $\mathbb{Z}_q[x_u, y_u | u \in Z_{2^\nu p}]$ deduced from the relations of Theorem 2.1 and Theorem 2.6, where in the Riemann type relations $a_u$ is replaced by $y_u$ for all $u \in Z_{2^\nu p}$, and in the Frobenius type relations, $a_u$ and $a_u^{\sigma^2}$ are replaced by $x_u$ and $y_u$, respectively, for all $u \in Z_{2^\nu p}$. We put $x_0 = y_0 = 1$ and use the symmetry relations in order to obtain a set of multivariate polynomials depending on $1/2[(2^\nu p)^g - 2^{\nu g}] + 2^{\nu g} - 1$ variables $x_u$ and a subset of the same cardinality of the coordinates $y_u$.

Pick up any subset $1/2[(2^\nu p)^g - 2^{\nu g}] + 2^{\nu g} - 1/2[g(g+1)] - 1$ of Riemann type equations and $1/2[g(g+1)]$ Frobenius type equations to form an application

$$\Phi : \mathbb{Z}_q^{2^{\nu g-1}(p^g+1)-1} \times \mathbb{Z}_q^{2^{\nu g-1}(p^g+1)-1} \mapsto \mathbb{Z}_q^{2^{\nu g-1}(p^g+1)-1}.$$

For a suitable choice of the Riemann and Frobenius equations, if $\nu \geq 3$, the conditions of [LD06, Th.2] are satisfied and one can use the lifting algorithm given ibid in order to lift in a canonical way the theta null point $(a_u)_{u \in Z_{2^\nu p}}$ to obtain the canonical theta null point $(b_u)_{u \in Z_{2^\nu p}}$ of the canonical lift with $b_u \in \mathbb{Z}_q$.

**Norm phase** We use the notation of Section 2.4. By Proposition 2.8, one computes the product of the Eigenvalues $\pi_1, \ldots, \pi_2$ of the absolute $q$-Frobenius morphism $F$, which are units modulo $p$, as

$$\pi_1 \ldots \pi_g = \mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p} \left( \frac{\sum_{u \in Z_2} b_u}{\sum_{u \in Z_{2^\nu p}} b_u} \right).$$

**Reconstruction phase** The problem here is to be able to recover $\chi_F$ where from the knowledge of $\lambda = \pi_1 \ldots \pi_g$ computed up to a certain precision $m$. If the genus $g$ of $C$ is one, then $\chi_F$ is immediately computed from $\pi_1$. In the case that the curve $C$ has genus 2 one can use the formulas described in [Rit03].

From now on, we suppose that $g \geq 2$. Following [Rit03, LD06], one can use the LLL algorithm in order to recover the symmetric polynomial of $C$ considered as a curve over $\mathbb{F}_q$ that we denote by $P_{sym}$. By definition, the symmetric polynomial of $C$ is the unitary degree $2^{g-1}$ polynomial whose roots are $x + q^g/x$ where $x$ runs over all products of $g$ terms taken successively in the pairs $\{\pi_1, q/\pi_1\}, \ldots, \{\pi_g, q/\pi_g\}$. It is easy to see that $P_{sym}$ is a polynomial with coefficients in $\mathbb{Z}$ and that there exists a quick algorithm, at least when $\chi_F$ is irreducible, to compute $\chi_F(\pm X)$ from the knowledge of $P_{sym}$ (see [Rit03]). By [Tat66], $\chi_F$ is irreducible when the Jacobian of $C$ is absolutely simple, and this last condition is generic. A last check on the curve allows us to obtain $\chi_F$. We explicitly determine bounds on the precision $m$ needed when the genus increases.

The computation of $P_{sym}$ from $\eta = \lambda + q^g/\lambda$, can be done by LLL reducing the lattice whose basis vectors are given by the columns of the following matrix:

$$\begin{bmatrix} \Upsilon \times M_0 & \Upsilon \times M_1 & \cdots & \Upsilon \times M_{2^{g-1}+1} & \Upsilon \times p^m \\ 0 & 0 & \cdots & p^{\lfloor n \times S_{2^{g-1}+1} \rfloor} & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & p^{\lfloor n \times S_2 \rfloor} & \cdots & 0 & 0 \\ p^{\lfloor n \times S_0 \rfloor} & 0 & \cdots & 0 & 0 \end{bmatrix},$$

where

$$[M_i]_{i=0,\dots,2^{g-1}} = \left[\; p^{(2^{g-1}-1-i)n}\eta^i \bmod 2^m \mid i \in \{0,\dots,2^{g-1}-1\}\right] \\ \cup[\eta^{2^{g-1}} \bmod 2^m].$$

and

$$[S_i]_{i=0,\dots,2^{g-1}+1} = \left[\frac{(i-1)(g-2)}{2} \mid i \in \{0,\dots,2^{g-1}-1\}\right] \cup \left[\frac{2^{g-1}(g-2)}{2}+1\right]$$

where $\Upsilon$ is some arbitrarily large constant. The power of $p$ appearing in the $M_i$ are meant to take into account the valuation of the coefficients of $P_{sym}$ while the $S_i$ offset the difference between the modulus of the coefficients of $P_{sym}$. This matrix can be used as long as $2^g < n$.

The coefficients of $P_{sym}$ are components of a vector $\Pi$ of small norm in $\mathcal{L}$. Asymptotic estimates state that a lattice reduction using the LLL algorithm [LLL82, Cop97] can compute it if its euclidean norm $||\ ||_2$ (or sup-norm $||\ ||_1$) satisfy $||\Pi||_1 \leqslant ||\Pi||_2 \leqslant \det(\mathcal{L})^{1/\dim\mathcal{L}}$. Since we can evaluate, on the first hand, the norm $||\ ||_1$ of $\Pi$ as a function of $n$ and $g$ using the Riemann hypothesis for curves and, on the other hand, the determinant of $\mathcal{L}$ as a function of $m$, $g$ and the size of $\Upsilon$ (product of the elements on diagonal), this yields

$$m > n\left[\ln(p)\, g^2\, 2^{3g-5} - \frac{\ln(p)}{\ln(2)}\,(g-2)\,2^{2(g-1)}\right].$$

From the knowledge of the roots of $P_{sym}$, it is possible to recover the set $\{\pi_i^2, i = 1\dots g\}$ [Rit03, pp.119] where the $\pi_i$ are the roots of $\chi_F$ which are units modulo $p$. In the case that $\chi_F$ is irreducible, we immediately deduce $\chi_F$ from the knowledge of its roots. In order to remove the sign ambiguity it remains to determine whether the order of the Jacobian is $\chi_F(1)$ or $\chi_F(-1)$ by multiplying points with possible group orders.

# 4 Complexity analysis

In this section, we give a complexity analysis of the previously described algorithm.

**Initialisation phase** The dominant complexity for this phase is the Groebner basis computation of Step 3. Let $J$ be as in Section 2.3.

Let $D$ be the degree of the ideal $J$. According to [Laz81], the computation of a Groebner basis with respect to a lexicographic monomial order can be done by doing a Gaussian elimination on a matrix of dimension given by the number of monomials of degree $D$. The theorem of Bezout gives a bound on $D$ which is the product of the degrees of the polynomials generating the ideal $J$. As the number of polynomial relations defined by Theorem 2.6 depends only on $g$ and $p$ and the degree of these relations is constant, $D$ is fixed as long as $g$ and $p$

are. This means that the Groebner basis can be computed by doing a Gaussian elimination on a matrix of fixed dimension whose coefficients are in $\mathbb{F}_q$. This requires $O(n^\mu)$ time operations where $n$ and $\mu$ have been defined at the end of the introduction.

We remark that [Laz83] gives a much finner bound on the degree of the Groebner basis if one chooses for the monomial order of $J$ a graded reverse lexicographic order. As a consequence, one should better first compute a Groebner basis of $J$ for a graded reverse lexicographic order and then use the FGLM algorithm in order to perform the change of order towards a lexicographic order.

**Lift phase** In the case that the base field admits a Gaussian Normal Basis one can lift in time $O(\log(n)m^\mu n^\mu)$ using the algorithm [LL03]. In the general case, one can use the algorithm of Harley which is in $O(\log(m)m^\mu n^\mu)$ time complexity [CFA$^+$06, pp.254].

**Norm phase** In the case that the base field admits a Gaussian Normal Basis of type $t$, H. Y. Kim et al. described an algorithm of the type "divide and conquer" in order to compute such a norm. This algorithm has time complexity $O(\log(n)m^\mu n^\mu)$. For the general case, one can use the algorithm described in [CFA$^+$06, pp.263] in order to compute the norm in time $O(\log(n)m^\mu n^\mu)$.

**Reconstruction phase** For fixed genus, the LLL step consists in applying LLL to a lattice of fixed dimension. Its complexity is the size of the coefficients of the matrix times the cost for one integer multiplication. This yields, with asymptotically fast algorithms for multiplying integers, a $O(m^{1+\mu})$ complexity in time. The cost of the second step is determined by the computation of roots of polynomials over $\mathbb{C}_p$ and requires $O(m^\mu)$. Finally, checking that the order of the Jacobian is $\chi_F(\pm 1)$ needs $O(m)$ applications of the group law, that is to say a complexity in time equal to $O(mn^\mu)$ with Cantor formulas [Can87].

# 5 A finiteness theorem

This section is devoted to the proof of Theorem 2.7. In Section 2.2, we recall several equivalent presentations of the Riemann equations which are used in the course of the proof given in Section 5.2.

We first fix some notations. Let $A$ be an abelian variety over a field $k$ and $\mathscr{L}$ be an ample symmetric line bundle over $A$. Let $\Theta_\ell$ be a theta structure for $\mathscr{L}$ of type $Z_\ell$. Let $(\theta_i^{\Theta_\ell})_{i\in Z_\ell}$ be a basis of the global sections of $\mathscr{L}$ determined by the theta structure $\Theta_\ell$ and let $x$ be a closed point of $A$. Denote by $\mathscr{O}_A$ the structure sheaf of $A$ and let $\rho : \mathscr{O}_{A,x} \to k'$ be the evaluation morphism onto the residual field $k'$ of $x$. We can choose an isomorphism $\xi_x : \mathscr{L}_x \simeq \mathscr{O}_{A,x}$. For all $i \in Z_\ell$ the evaluation of the section $\theta_i^{\Theta_\ell}$ in $x$ is

$$\theta_i^{\Theta_\ell}(x, \xi_x) = \rho \circ \xi_x(\theta_i^{\Theta_\ell}). \tag{9}$$

The resulting projective point that we denote by $(\theta_i^{\Theta_\ell}(x))_{i\in Z_\ell}$ over $\overline{k}$ does not depend on the choice of the isomorphism $\xi_x$.

### 5.1 Riemann's equations revisited

Let $A$ be a $g$ dimensional ordinary abelian variety over a finite field $\mathbb{F}_q$ of characteristic $p > 2$. Let $\mathscr{L}$ be an ample symmetric degree 1 line bundle on $A$. Let $\nu > 0$ be an integer and $\ell$ be an odd prime number which can be equal to $p$. Assume that we are given a symmetric theta structure $\Theta_{2^\nu\ell}$ of type $Z_{2^\nu\ell}$ for the line bundle $\mathscr{L}^{2^\nu\ell}$. The data of $\Theta_{2^\nu\ell}$ defines a basis of global sections of $\mathscr{L}^{2^\nu\ell}$ that we denote by $(\theta_u)_{u\in Z_{2^\nu\ell}}$ and as a consequence, a projective embedding of $A$ in $\mathbb{P}^{(2^\nu\ell)^g-1}$.

We denote the theta null point with respect to the theta structure $\Theta_{2^\nu\ell}$ by $(a_u)_{u\in Z_{2^\nu\ell}}$. The Riemann's equations for level $2^\nu\ell$ are given by the following theorem

**Theorem 5.1.** *For all $x, y, u, v \in Z_{2^{\nu+1}\ell}$ which are congruent modulo $Z_{2^\nu\ell}$, and all $l \in \hat{Z}_2$, we have*

$$\Big(\sum_{t\in Z_2} l(t)\theta_{x+y+t}\star\theta_{x-y+t}\Big).\Big(\sum_{t\in Z_2} l(t)a_{u+v+t}a_{u-v+t}\Big) = \\ = \Big(\sum_{t\in Z_2} l(t)\theta_{x+u+t}\star\theta_{x-u+t}\Big).\Big(\sum_{t\in Z_2} l(t)a_{y+v+t}a_{y-v+t}\Big), \quad (10)$$

*where $\star$-product is defined as in [Mum66, §3].*

*Proof.* By [Mum66][pp. 339], for all $x, y \in Z_{2^{\nu+1}\ell}$ such that $x + y \in Z_{2^\nu\ell}$ and for all $l \in \hat{Z}_2$, we have

$$\sum_{t\in Z_2} l(t)\theta_{x+y+t}\star\theta_{x-y+t} = \Big(\sum_{t\in Z_2} l(t).a_{y+t}\Big).\Big(\sum_{t\in Z_2} l(t).\theta_{x+t}\Big). \quad (11)$$

In particular, we have,

$$\sum_{t\in Z_2} l(t)a_{x+y+t}.a_{x-y+t} = \Big(\sum_{t\in Z_2} l(t).a_{y+t}\Big).\Big(\sum_{t\in Z_2} l(t).a_{x+t}\Big). \quad (12)$$

Now, using (11) and (12) the left hand side of (10) can be written as

$$\Big[\Big(\sum_{t\in Z_2} l(t).a_{y+t}\Big).\Big(\sum_{t\in Z_2} l(t).\theta_{x+t}\Big)\Big]\Big[\Big(\sum_{t\in Z_2} l(t).a_{u+t}\Big).\Big(\sum_{t\in Z_2} l(t).a_{v+t}\Big)\Big]. \quad (13)$$

In the same manner the right hand side of (10) can be written as

$$\Big[\Big(\sum_{t\in Z_2} l(t).a_{u+t}\Big).\Big(\sum_{t\in Z_2} l(t).\theta_{x+t}\Big)\Big]\Big[\Big(\sum_{t\in Z_2} l(t).a_{y+t}\Big).\Big(\sum_{t\in Z_2} l(t).a_{v+t}\Big)\Big]. \quad (14)$$

Obviously, (18) and (19) are equal. □

In the following, we suppose that $k$ is the field of definition of $(a_u)_{u\in Z_{2^\nu\ell}}$. In this section, we denote by $I_{\Theta_{2^\nu\ell}}$ the ideal of $k[x_u|u \in Z_{2^\nu\ell}]$ generated by the relations of Theorem 5.1 where the $\theta_u$ are replaced by $x_u$. It is proved in [Mum66, §4] that if $\nu \geq 2$ and $\ell \neq p$, $A$ is isomorphic to the closed projective sub-variety of $\mathbb{P}_k^{(2^\nu\ell)^g-1}$ defined by the homogeneous ideal $I_{\Theta_{2^\nu\ell}}$.

We recover Theorem 2.6 from Theorem 5.1, by evaluating at the point $O$ of $A$ the sections of $\mathscr{L}^{2^\nu\ell}$. The relations of Theorem 2.6 can be reformulated, by considering the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

and $(x_1, y_1, u_1, v_1), (x_2, y_2, u_2, v_2) \in (Z_{2^\nu\ell})^4$ such that

$$2\begin{pmatrix} x_2 \\ y_2 \\ u_2 \\ v_2 \end{pmatrix} = M\begin{pmatrix} x_1 \\ y_1 \\ u_1 \\ v_1 \end{pmatrix}.$$

If we suppose moreover that $x_2 + y_2 \in 2Z_{2^\nu\ell}$ and $u_2 + v_2 \in 2Z_{2^\nu\ell}$, we have

$$\Big(\sum_{t\in Z_2} l(t)a_{x_1+t}a_{y_1+t}\Big).\Big(\sum_{t\in Z_2} l(t)a_{u_1+t}a_{v_1+t}\Big) = \tag{15}$$

$$= \Big(\sum_{t\in Z_2} l(t)a_{x_2+t}a_{y_2+t}\Big).\Big(\sum_{t\in Z_2} l(t)a_{u_2+t}a_{v_2+t}\Big), \tag{16}$$

$l \in \hat{Z}_2$.

By developing and summing up over all the characters of $\hat{Z}_2$ the Equation (15), we obtain

$$\sum_{t\in Z_2} a_{x+t}a_{y+t}a_{u+t}a_{v+t} = \sum_{t\in Z_2} a_{x-\tau+t}a_{y+\tau+t}a_{u+\tau+t}a_{v+\tau+t}, \tag{17}$$

for all $x, y, u, v \in Z_{2^\nu\ell}$ and $\tau \in Z_{2^\nu\ell}$ such that $2\tau = x - y - u - v$.

These relations can also be presented in their classical form. For this, we keep the notations of the previous paragraph and suppose from here that $\nu \geq 2$. Recall that $(a_u)_{u\in Z_{2^\nu\ell}}$ denote the theta null point defined by the theta structure $\Theta_{2^\nu\ell}$. Let $H_{2^\nu\ell} = Z_{2^\nu\ell} \times \hat{Z}_{2^{\nu-1}}$ and for all $x = (x', x'') \in H_{2^\nu\ell}$, let $b_x = \sum_{t\in Z_{2^{\nu-1}}} x''(t)a_{x'+t}$. Let $H_2 = \frac{1}{2}Z_2 \times (\widehat{Z_{2^\nu\ell}})_2 = \{x \in H_{2^\nu\ell} | x \,\text{is}\, 2-\text{torsion modulo}\, Z_2 \times \{0\}\}$.

**Theorem 5.2.** *Let $(x, y, u, v) \in H_{2^\nu\ell}$ and $\tau = (\tau', \tau'') \in H_{2^\nu\ell}$ such that $2\tau = x - y - u - v$ then*

$$b_x b_y b_u b_v = \frac{1}{2^g}\sum_{t\in H_2} A(2t')b_{x-\tau+t}b_{y+\tau+t}b_{u+\tau+t}b_{v+\tau+t},$$

*where $t = (t', t'')$ and $A = \tau'' + t''$.*

*Proof.* It is possible to deduce these relations from (17) following exactly the same computations as [Mum66, pp. 334]. □

Let $(\theta_u)_{u\in Z_{2^\nu}}$ denote the basis of global sections of $\mathscr{L}^{2^\nu}$ defined by the theta structure $\Theta_{2^\nu}$. Let $H_{2^\nu} = Z_{2^\nu} \times \hat{Z}_{2^{\nu-1}}$ and $H_2 = \frac{1}{2}Z_2 \times (\hat{Z_{2^\nu}})_2$. For all $x = (x', x'') \in H_{2^\nu}$, set $\vartheta_x = \sum_{t\in Z_{2^{\nu-1}}} x''(t)\theta_{x'+t}$. We have the

**Theorem 5.3.** *Let $P, Q$ be two closed points of $A$. Denote by $\mathscr{O}_A$ the structure sheaf of $A$. For $X \in \{P, Q, P+Q, P-Q, 0\}$, we choose isomorphisms $\xi_X : \mathscr{L}_X^{2^\nu} \simeq \mathscr{O}_{A,X}$. Let $(x, y, u, v) \in H_{2^\nu}$ and $\tau = (\tau', \tau'') \in H_{2^\nu}$ such that $2\tau = x - y - u - v$, we have*

$$\vartheta_x(P+Q, \xi_{P+Q})\vartheta_y(P-Q, \xi_{P-Q})\vartheta_u(0, \xi_0)\vartheta_v(0, \xi_0) =$$

$$= \lambda \frac{1}{2^g} \sum_{t\in H_2} A(2t')\vartheta_{x-\tau+t}(P, \xi_P)\vartheta_{y+\tau+t}(P, \xi_P)\vartheta_{u+\tau+t}(Q, \xi_Q)\vartheta_{v+\tau+t}(Q, \xi_Q),$$

*where $t = (t', t'')$, $A = \tau'' + t''$ and $\lambda \in \overline{k}$ is independent of the choice of $(x, y, u, v) \in H_{2^\nu}$.*

If $k = \mathbb{C}$, this last formula is exactly [Igu72, pp.141].

## 5.2 Proof of Theorem 2.7

In this section, we denote by $\mathbb{F}_q$ a finite field of characteristic $p > 2$ with $q$ elements. Let $A$ be an ordinary abelian variety over $\mathbb{F}_q$ and let $\mathscr{L}$ be an ample symmetric line bundle of degree 1 on $A$. Let $\ell$ be an odd prime number and suppose that we are given a theta structure $\Theta_{2^\nu}$ for $\mathscr{L}^{2^\nu}$. We denote the theta null point with respect to the theta structure $\Theta_{2^\nu}$ by $(a_u)_{u\in Z_{2^\nu}}$. We suppose that $(a_u)_{u\in Z_{2^\nu}}$ is defined over $\mathbb{F}_q$.

In the following $Z_{2^\nu}$ is considered as a subgroup of $Z_{2^\nu\ell}$ via the map $j \mapsto \ell j$. Let $I$ be the ideal of the multivariate polynomial ring $\mathbb{F}_q[x_u | u \in Z_{2^\nu\ell}]$ which is spanned by the relations of Theorem 2.6, taken modulo $p$, together with the symmetry relations $x_u = x_{-u}$ for all $u \in Z_{2^\nu\ell}$. Let $J$ be the image of $I$ under the specialization map

$$\mathbb{F}_q[x_u | u \in Z_{2^\nu\ell}] \to \mathbb{F}_q[x_u | u \in Z_{2^\nu\ell}, 2^\nu u \neq 0], \quad x_u \mapsto \begin{cases} a_u, & u \in Z_{2^\nu} \\ x_u, & \text{else} \end{cases}.$$

We want to prove that if $\nu \geq 2$, the ideal $J$ defines a 0-dimensional affine algebraic set.

**Remark 5.4.** *In the case that $\nu \geq 3$ and $\ell$ is prime to $p$, the preceding theorem can be proved using the general description of the moduli space of abelian varieties with a theta marking given in [Mum67]. But this general description is not available under the hypothesis that we consider. It should also be remarked that the variety defined by $J$ when $\ell$ is equal to the characteristic of $\mathbb{F}_q$ is singular so that it is not possible to lift to the $p$-adics to recover the situation where $\ell$ is different from $p$. In the following we present a proof which is valid both in the situation where $\ell$ is equal to or different from the characteristic of $\mathbb{F}_q$.*

Denote by $J'$ the ideal of $\mathbb{F}_q[x_u|u \in Z_{2^\nu \ell}]$ generated by $J$ and elements $x_u - a_u$ for all $u \in Z_{2^\nu}$. Denote by $V_{J'}$ the closed sub-variety of the affine space of dimension $(2^\nu \ell)^g$, $\mathbb{A}^{(2^\nu \ell)^g}$ defined by $J'$. We want to show that $V_{J'}$ is a 0-dimensional variety.

We recall that the data of $\Theta_{2^\nu}$ gives a basis $(\theta_u)_{u \in Z_{2^\nu}}$ of the global sections of $\mathscr{L}^{2^\nu}$ on $A$ and as a consequence an embedding of $A$ in $\mathbb{P}^{2^\nu g - 1}_{\mathbb{F}_q}$. If we denote by $V_{I_{\Theta_{2^\nu}}}$ the projective variety defined by the homogeneous ideal $I_{\Theta_{2^\nu}}$, $A$ is isomorphic to $V_{I_{\Theta_{2^\nu}}}$ as an abelian variety [Mum66, §4].

The idea of the proof of the Theorem 2.7 is to interpret the solutions of $J'$ as closed points in the variety $A = V_{I_{\Theta_{2^\nu}}}$ and then to show that these points are $\ell$-torsion points of $A$. This is exactly the content of Lemma 5.5 and Lemma 5.6.

Let $\pi : Z_{2^\nu} \times Z_\ell \to Z_{2^\nu \ell}$ and $\pi' : Z_{2^{\nu+1}} \times Z_\ell \to Z_{2^{\nu+1} \ell}$ be the isomorphisms deduced from the Chinese reminder theorem.

**Lemma 5.5.** *Suppose that $(c_v)_{v \in Z_{2^\nu \ell}}$ is a closed point of $V_{J'}$. For any $i \in Z_\ell$ let $P_i$ be the closed point of $\mathbb{P}^{2^\nu g - 1}_{\mathbb{F}_q}$ with homogeneous coordinates $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$. For all $i \in Z_\ell$, $P_i$ is a closed point of $V_{I_{\Theta_{2^\nu}}}$.*

*Proof.* It is enough to verify that for all $i \in Z_\ell$, $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$ satisfy the equations provided by the elements of $I_{\Theta_{2^\nu}}$. For $i = 0$ this is an immediate consequence of the hypothesis that $(a_k)_{k \in Z_{2^\nu}}$ is the theta null point associated to $\Theta_{2^\nu}$ and that by definition of $J'$, $a_k = c_{\pi(k,0)}$ for all $k \in Z_{2^\nu}$.

Let $x, y, u, v \in Z_{2^{\nu+1}}$ which are congruent modulo $Z_{2^\nu}$. For any $i \in Z_\ell - \{0\}$, we remark that $\pi(x,i), \pi(y,0), \pi(u,0), \pi(v,0) \in Z_{2^{\nu+1}\ell}$ are congruent modulo $Z_{2^\nu \ell}$. By definition of $I$ and the relations of Theorem 2.6, $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$ satisfy the relation

$$\Big(\sum_{t \in Z_2} l(t) c_{\pi(x+y,i)+t} c_{\pi(x-y,i)+t}\Big).\Big(\sum_{t \in Z_2} l(t) c_{\pi(u+v,0)+t} c_{\pi(u-v,0)+t}\Big) =$$
$$= \Big(\sum_{t \in Z_2} l(t) c_{\pi(x+u,i)+t} c_{\pi(x-u,i)+t}\Big).\Big(\sum_{t \in Z_2} l(t) c_{\pi(y+v,0)+t} c_{\pi(y-v,0)+t}\Big),$$

for all $l \in \hat{Z}_2$.

Taking care of the fact that $c_{\pi(k,0)} = a_k$ for all $k \in Z_{2^\nu}$, we deduce that the point with homogeneous coordinates $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$ satisfy all the relations of Theorem 5.1 and as a consequence is a closed point of $V_{I_{\Theta_{2^\nu}}}$. □

**Lemma 5.6.** *Let $(c_v)_{v \in Z_{2^\nu \ell}}$ be a closed point of $V_{J'}$. Applying Lemma 5.5, for $i \in Z_\ell$, we denote by $P_i$ the closed point of $V_{I_{\Theta_{2^\nu}}}$ with homogeneous coordinates $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$. For all $i \in Z_\ell$, the closed point $P_i$ is a $\ell$-torsion point of $A$.*

*Proof.* Let $i \in Z_\ell$, for $\lambda \in \{0, \ldots, \ell - 1\}$ we set $Q_\lambda = P_{\lambda.i}$. We are going to prove inductively on $\lambda \in \{1, \ldots, \ell\}$ that on the abelian variety $V_{I_{\Theta_{2^\nu}}}$ the point $\lambda.Q_1$ is equal to the point $Q_\lambda$. Applying this result for $\lambda = \ell$, we obtain that $\ell Q_1 = Q_\ell = Q_0$ and $Q_0$ is the 0 point of $A$ which means that $Q_1 = P_i$ is a $\ell$-torsion point of $A$.

The induction hypothesis is clear for $\lambda = 1$. Let $(\theta_u)_{u \in Z_{2^\nu}}$ be the basis of global section of $\mathscr{L}^{2^\nu}$ defined by $\Theta_{2^\nu}$. We suppose that for all $1 \leq \mu \leq \lambda - 1$, there exists an isomorphism $\xi_{\mu.Q_1} : \mathscr{L}^{2^\nu}_{\mu.Q_1} \simeq \mathscr{O}_{A,\mu.Q_1}$ such that $(\theta_k(\mu.Q_1, \xi_{\mu.Q_1}))_{k \in Z_{2^\nu}} = (c_{\pi(k,\mu.i)})_{k \in Z_{2^\nu}}$. We have to prove that there exists an isomorphism $\xi_{\lambda.Q_1} : \mathscr{L}^{2^\nu}_{\lambda.Q_1} \simeq \mathscr{O}_{A,\lambda.Q_1}$ such that $(\theta_k(\lambda.Q_1, \xi_{\lambda.Q_1}))_{k \in Z_{2^\nu}} = (c_{\pi(k,\lambda.i)})_{k \in Z_{2^\nu}}$.

Let $H_{2^\nu} = Z_{2^\nu} \times \hat{Z}_{2^{\nu-1}}$. For all $x = (x', x'') \in H_{2^\nu}$, we let

$$\vartheta_x = \sum_{t \in Z_{2^{\nu-1}}} x''(t) \theta_{x'+t}.$$

Let $(x, y, u, v) \in H_{2^\nu}$ and $\tau = (\tau', \tau'') \in H_{2^\nu}$ such that $2\tau = x - y - u - v$. By the induction hypothesis, for $X \in \{(\lambda - 1)Q_1, Q_1, (\lambda - 2)Q_1, 0\}$, we have already a well defined isomorphisms $\mathscr{L}^{2^\nu}_X \simeq \mathscr{O}_{A,X}$. We choose any isomorphism $\xi_{\lambda.Q_1} : \mathscr{L}^{2^\nu}_{\lambda.Q_1} \simeq \mathscr{O}_{A,\lambda.Q_1}$.

By applying Theorem 5.3, we deduce a relation

$$\begin{aligned} &\vartheta_x(\lambda.Q_1, \xi_{\lambda.Q_1}) \vartheta_y((\lambda-2).Q_1, \xi_{(\lambda-2).Q_1}) \vartheta_u(0, \xi_0) \vartheta_v(0, \xi_0) = \\ &= \lambda \frac{1}{2^g} \sum_{t \in H_2} A(2t') \vartheta_{x-\tau+t}((\lambda-1).Q_1, \xi_{(\lambda-1).Q_1}) \vartheta_{y+\tau+t}((\lambda-1).Q_1, \xi_{(\lambda-1).Q_1}) \\ &\qquad \vartheta_{u+\tau+t}(Q_1, \xi_{Q_1}) \vartheta_{v+\tau+t}(Q_1, \xi_{Q_1}), \end{aligned} \tag{18}$$

where $t = (t', t'')$, $A = \tau'' + t''$ and $\lambda \in \overline{\mathbb{F}}_q^*$ does not depend on the choice of $(x, y, u, v) \in H_{2^\nu}$.

On the other side, denote by $H_{2^\nu \ell} = Z_{2^\nu \ell} \times \hat{Z}_{2^{\nu-1}}$. In the following we identify $H_{2^\nu \ell}$ with the Cartesian product $H_{2^\nu} \times Z_\ell$. For all $x = (x', x'') \in H_{2^\nu \ell}$, we let $d_x = \sum_{t \in Z_2} x''(t) c_{x'+t}$. Set $x_1 = (x, \lambda.i), y_1 = (y, (\lambda-2).i), u_1 = (u, 0), v_1 = (v, 0)$. Let $\tau \in H_{2^\nu}$ be such that $2\tau = x - y - u - v$ and $\tau_1 = \tau \times \{1\} \in H_{2^\nu \ell}$. We remark that $2\tau_1 = x_1 - y_1 - u_1 - v_1$ and by applying Theorem 5.2, we get a relation deduced from the definition of $I$

$$d_{x_1} d_{y_1} d_{u_1} d_{v_1} = \frac{1}{2^g} \sum_{t \in H_2} (\tau'' + t'')(2t') d_{x_1 - \tau_1 + t} d_{y_1 + \tau_1 + t} d_{u_1 + \tau_1 + t} d_{v_1 + \tau_1 + t}. \tag{19}$$

where $t = (t', t'') \in H_2$.

By the recurrence hypothesis and by the construction of the quadruples $(x_1, y_1, u_1, v_1)$, we have for all $t \in H_2$, $d_{x_1 - \tau_1 + t} = \vartheta_{x-\tau+t}((\lambda-1).Q_1, \xi_{(\lambda-1).Q_1})$, $d_{y_1+\tau+t} = \vartheta_{y+\tau+t}((\lambda-1).Q_1, \xi_{(\lambda-1).Q_1})$, $d_{u_1+\tau_1+t} = \vartheta_{u+\tau+t}(Q_1, \xi_{Q_1})$, $d_{v_1+\tau_1+t} = \vartheta_{v+\tau+t}(Q_1, \xi_{Q_1})$. In the same way, on the left hand side of (19), we have $d_{y_1} = \vartheta_y((\lambda-2).Q_1, \xi_{(\lambda-2).Q_1})$, $d_{u_1} = \vartheta_u(0, \xi_0)$ and $d_{v_1} = \vartheta_v(0, \xi_0)$.

There exists $u_0 \in H_{2^\nu}$ such that $\vartheta_{u_0}(0, \xi_0) \neq 0$. We can take $u = v = u_0$ in Equations (18) and (19) and we deduce immediately that $d_{x_1} = \vartheta_x(\lambda.Q_1, \xi_{\lambda.Q_1})$. By taking all possible values of $x_1''$ in $x_1 = (x_1', x_1'')$, we obtain that

- for all $k \in Z_{2^\nu}$, $c_{\pi(k,\lambda.i)}$ is uniquely determined from the knowledge of $c_{\pi(k,\mu.i)}$ for $\mu \leq \lambda - 1$;

- for all $k \in Z_{2^\nu}$, $c_{\pi(k,\lambda.i)} = \theta_k(\lambda.Q_1, \xi_{\lambda.Q_1})$ modulo multiplication by a constant factor independent of $k$ that we normalise to 1 by choosing a certain $\xi_{\lambda.Q_1}$.

□

*Proof.* Let $(c_v)_{v \in Z_{2^\nu \ell}}$ be a geometric point of $V_{J'}$. By the preceding lemma, for all $i \in Z_\ell$, $(c_{\pi(k,i)})_{k \in Z_{2^\nu}}$, being the homogeneous coordinate of a $\ell$-torsion point of $A$, can only assume a finite number of value up to a multiplication by a constant factor. In order to finish the proof, we only have to show that this constant factor belongs to a finite set. Let $\lambda$ such that $(\gamma c_{\pi(k,i)})_{k \in Z_{2^\nu}}$ can prolongued to a geometric point $(c'_v)_{v \in Z_{2^\nu \ell}}$ of $V_{J'}$. By applying formula, (19) we see inductively that for $\lambda = 1, \ldots, \ell$, there exists an integer $t_\lambda$ such that we have $c'_{\pi(k,\lambda.i)} = \gamma^{t_\lambda} c_{\pi(k,\lambda.i)}$. Applying this for $\lambda = \ell$, we obtain that $a_k = c'_{\pi(k,0)} = \gamma^{t_\ell} c_{\pi(k,0)} = \gamma^{t_\ell} a_k$. As a consequence, we have that $\gamma$ is a $(t_\ell)^{th}$ root of unity and we are done. □

# 6 Practical implementation and examples

The proved version of the algorithm involves the resolution of a big algebraic systems which makes it not suitable for practical applications. We have implemented the heuristic version of the algorithm for the case of genus 1 and genus 2 [CL07]. For the genus 2 implementation, using a special purpose Groebner basis algorithm it is possible to solve easily the algebraic system of the initialisation phase.

**A genus 1 characteristic 5 example.** Let $\mathbb{F}_{5^8}$ be represented by the quotient $\mathbb{F}_5[X]/(P)$ where $P(X) = X^8 + X^4 + 3X^2 + 4X + 2$ and let $u$ be the image of $X$ in $\mathbb{F}_{5^8}$ via the above isomorphism. Let $E$ be the ordinary elliptic curve given by the Weierstrass equation

$$y^2 = x^3 + x^2 + 3x.$$

After the initialisation phase we obtain the following six theta constants

$$[1, 4, u^{32552}, u^{309244}, u^{211588}, u^{32552}].$$

We consider $\mathbb{Z}_{5^8}$ given as the unramified extension of the 5-adic integers $\mathbb{Z}_5$ defined by the integer polynomial $X^8 + X^4 + 3X^2 + 4X + 2$ and denote by $z$ the image of $X$ in $\mathbb{Z}_{5^8}$. After the lift phase we get the following lifted theta constants to precision 5

$$\begin{aligned}
&[1, -1460z^7 - 10z^6 - 785z^5 + 715z^4 - 555z^3 + 420z^2 - 1035z - 1116, \\
&-1449z^7 - 819z^6 + 396z^5 + 746z^4 + 1108z^3 + 648z^2 + 546z - 1189, \\
&1438z^7 - 1497z^6 + 1548z^5 - 777z^4 + 354z^3 - 876z^2 + 998z + 1029, \\
&1449z^7 + 819z^6 - 396z^5 - 746z^4 - 1108z^3 - 648z^2 - 546z - 868, \\
&-1504z^7 + 101z^6 + 741z^5 + 591z^4 - 957z^3 - 492z^2 - 1109z - 834]
\end{aligned}$$

where $z$ is a generator

After the norm phase we obtain 1054 as the number of rational points on $E$.

**A genus 2 characteristic 3 example** Let $\mathbb{F}_{3^{28}}$ be represented by the quotient $\mathbb{F}_3[X]/(P)$ where

$$P(X) = X^{28} + 2X^{14} + X^{13} + X^{12} + 2X^{11} + X^{10} + X^9 + X^8 + 2X^6 + 2X^4 + X^3 + 2$$

and let $w$ be the image of $X$ in $\mathbb{F}_{5^8}$ via this isomorphism. Let $H$ be the ordinary genus 2 hyperelliptic curve given by the affine equation

$$\begin{aligned}
y^2 \quad = \quad & x^6 + (w^{18} + w^{17} + w^{16} + w^{11} + w^{10} + w^9 + w^8 + w^7 + 2w^5 + 2w^2 + w)x^5 \\
& +(w^{19} + 2w^{17} + 2w^{16} + w^{13} + w^{11} + w^{10} + 2w^8 + 2w^7 + w^6 + 2w^4 + w + 2)x^4 \\
& +(2w^{19} + 2w^{18} + 2w^{17} + 2w^{15} + 2w^{14} + 2w^{12} + 2w^{11} + 2w^{10} + 2w^9 + w^7 + 2w^6 \\
& \quad +w^5 + 2w^4 + w^3 + w + 1)x^3 \\
& +(w^{19} + 2w^{18} + 2w^{16} + 2w^{13} + w^{12} + w^{10} + 2w^9 + w^8 + w^6 + 2w^2 + 1)x^2 \\
& +(w^{19} + 2w^{18} + w^{17} + 2w^{15} + 2w^{14} + w^{13} + w^{12} + w^{11} + 2w^9 + w^8 + w^6 \\
& \quad +2w^5 + 2w^4 + w^3 + 2w^2 + 2)x \\
& +w^{19} + 2w^{16} + w^{15} + w^{14} + w^{12} + 2w^8 + w^7 + w^6 + w^4 + 2w^3 + w^2 + w + 1
\end{aligned}$$

First, we compute the following level 2 theta constants

$$\begin{aligned}
x_{00} &= w^{19} + w^{18} + 2 * w^{15} + w^{14} + w^{12} + 2w^{10} + w^7 + 2w^6 + 2w^5 + 2w^4 + w^3 + w + 2 \\
x_{03} &= w^{19} + 2w^{17} + 2w^{16} + 2w^{15} + 2w^{14} + 2w^{13} + w^{12} + 2w^{11} + 2w^{10} + 2w^9 + 2w^8 + w^7 + \\
& \quad w^6 + 2w^5 + w^4 + w^3 + 2w^2 + 2w + 2 \\
x_{30} &= w^{19} + 2w^{18} + w^{17} + w^{16} + 2w^{15} + 2w^{14} + 2w^{13} + w^{12} + 2w^{11} + 2w^{10} + 2w^9 \\
& \quad +2w^7 + 2w^3 + w^2 + 2 \\
x_{33} &= 2w^{19} + 2w^{18} + w^{17} + 2w^{15} + 2w^{13} + 2w^{12} + w^{10} + 2w^9 + w^8 + w^6 + 2w^4 + 2w^3 + w^2 + 2w + 1.
\end{aligned}$$

After the Groebner basis step, we obtain the following list of theta constants

$$\begin{aligned}
0 &= x_{01} + w^{18} + w^{16} + w^{15} + 2w^9 + w^8 + w^7 + w^6 + 2w^5 + w^4 + 2 \\
0 &= x_{02} + w^{19} + 2w^{17} + 2w^{16} + 2w^{15} + w^{14} + w^{13} + w^{12} + w^{11} + w^{10} + w^9 + \\
& \quad w^7 + 2w^5 + w^4 + w^3 + w^2 + w + 2 \\
0 &= x_{10} + 2w^{19} + 2w^{18} + w^{17} + 2w^{14} + 2w^{13} + 2w^{12} + w^{11} + w^{10} + w^9 + 2w^8 \\
& \quad +2w^6 + 2w^4 + w^3 + 2w^2 + 2 \\
0 &= x_{11} + 2w^{19} + w^{16} + w^{15} + 2w^{14} + 2w^{12} + 2w^{11} + 2w^{10} + 2w^9 + w^7 + w^5 \\
& \quad +w^4 + w^3 + 2w^2 + 2w + 2 \\
0 &= x_{12} + w^{19} + 2w^{18} + 2w^{17} + w^{16} + 2w^{15} + w^{14} + w^{13} + w^{12} + 2w^{10} + 2w^9 + w^8 + \\
& \quad 2w^7 + 2w^6 + w^4 + 2w^3 + 2w^2 + 2w + 1 \\
0 &= x_{13} + w^{18} + w^{17} + 2w^{14} + 2w^{13} + w^9 + 2w^6 + 2w^5 + 1 \\
0 &= x_{20} + w^{19} + w^{18} + 2w^{16} + w^{15} + w^{14} + w^{13} + w^{12} + w^{11} + 2w^{10} + w^9 + 2w^7 \\
& \quad +2w^6 + w^4 + w^3 + w + 2 \\
0 &= x_{21} + w^{19} + w^{17} + w^{16} + w^{15} + 2w^{14} + 2w^{12} + w^{10} + w^5 + w^3 + w^2 + w + 2 \\
0 &= x_{22} + 2w^{19} + w^{17} + 2w^{16} + 2w^{15} + w^{13} + w^{12} + 2w^{11} + 2w^{10} \\
& \quad +2w^9 + w^8 + 2w^7 + 2w^5 + w^4 + w^2 + w + 1 \\
0 &= x_{23} + w^{18} + 2w^{14} + w^{12} + 2w^{11} + 2w^{10} + w^8 + w^6 + w^5 + w^2 + w + 1 \\
0 &= x_{31} + w^{18} + w^{17} + w^{16} + 2w^{15} + 2w^{13} + 2w^{11} + w^9 + w^8 + w^7 + 2w^4 + 2w^3 + 2w^2 + 2 \\
0 &= x_{32} + 2w^{19} + 2w^{18} + 2w^{17} + 2w^{16} + w^{15} + 2w^{14} + w^{13} + w^{12} + w^{11} + w^9 + w^7 + w^6 + 2w^2 + w \\
0 &= x_{41} + w^{18} + 2w^{16} + 2w^{15} + 2w^{13} + w^{12} + w^{11} + w^{10} + 2w^9 + w^8 + w^7 + 2w^6 + w^4 + 2w \\
0 &= x_{42} + 2w^{16} + 2w^{14} + 2w^{12} + 2w^{10} + w^9 + 2w^8 + 2w^6 + 2w^5 + 2w^4 + w^3 + w^2 + w + 2 \\
0 &= x_{51} + 2w^{18} + w^{17} + 2w^{16} + 2w^{15} + 2w^{13} + w^{11} + w^{10} + w^9 + 2w^8 + w^7 + 2w^6 + \\
& \quad 2w^5 + 2w^4 + 2w^3 + w^2 + 2w \\
0 &= x_{52} + 2w^{17} + 2w^{16} + 2w^{15} + w^{14} + 2w^{12} + w^{10} + 2w^9 + 2w^7 + w^6 + w^5 + 2w^4 + w^3 + 2w^2 + w
\end{aligned}$$

After the norm phase, we obtain as a product of the Eigenvalues of the Frobenius morphism which are units modulo 3 the number

$$2023954210169141309384885 32$$

to precision 56. From here, we can recover the polynomial $\chi_F$ which is

$$\chi_F(X) = X^4 + 19612X^3 - 4108934426X^2 + 68382815672412X + 12157665459056928801.$$

## Conclusion

We have given an algorithm with quasi-quadratic time and quadratic space complexity with respect to the size of the base field to compute the number of points of a hyperelliptic curve whose Jacobian is ordinary and absolutely simple. We have presented two versions of our algorithm, one with proved complexity bound and a bad practical behaviour and a heuristic one which behaves very well in practice.

## References


[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BMMT94] Eberhard Becker, Teo Mora, Maria Grazia Marinari, and Carlo Traverso. The shape of the shape lemma. In *Proceedings of the international symposium on Symbolic and algebraic computation*, pages 129–133. ACM Press, 1994.

[Can87] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[Car] R. Carls. Galois theory of the canonical theta structure.

[Car07] R. Carls. Canonical coordinates on the canonical lift. *J. Ramanujan Math. Soc.*, 22(1):1–14, 2007.

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[CKL08] R. Carls, D. Kohel, and D. Lubicz. Higher dimensional 3-adic CM construction. *J. Algebra*, 319(3):971–1006, 2008.

[CL07] R. Carls and D. Lubicz. Magma implementation of the genus 1 point counting algorithm, 2007. Available at `http://www.mathematik.uni-ulm.de/ReineMath/mitarbeiter/carls/`.

[Cop97] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptology*, 10(4):233–260, 1997.

[Dem72] M. Demazure. *Lectures on p-divisible groups.* Number 302 in LNM. Springer, 1972.

[Edi06] B. Edixhoven. On the computation of the coefficients of a modular form. In *Algorithmic Number Theory Symposium VII*, number 4076 in LNCS, pages 30–39. Springer, 2006.

[Elk98] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, pages 21–76. AMS, 1998.

[Fay73] John D. Fay. *Theta functions on Riemann surfaces.* Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 352.

[Gau02] Pierrick Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In *Advances in cryptology—ASIACRYPT 2002*, Lecture Notes in Comput. Sci. Springer, Berlin, December 2002.

[GS04] P. Gaudry and É. Schost. Construction of secure random curves of genus 2 over prime fields. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Comput. Sci.*, pages 239–256. Springer-Verlag, 2004.

[Har02a] R. Harley. Asymptotically optimal $p$-adic point-counting. E-mail to the NMBRTHRY mailing list, December 2002.

[Har02b] R. Harley. Elliptic curve point counting: 32003 bits. E-mail to the NMBRTHRY mailing list, August 2002.

[Igu72] Jun-ichi Igusa. *Theta functions.* Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.

[Ked01] K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–328, 2001.

[Kem89] G. Kempf. Linear system on abelian varieties. *Amer. Journ. Math.*, 111:65–93, 1989.

[Koi76] S. Koizumi. Theta relations and projective normality of abelian varieties. *Amer. Journ. Math.*, 98:865–889, 1976.

[KPC+02] Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park, Jae Heon Kim, and Sang Geun Hahn. Fast Elliptic Curve Point Counting Using Gaussian Normal Basis. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V*, pages 292–307, Berlin, July 2002. Springer Verlag.

[Laz81] D. Lazard. Résolution des systèmes d'équation algébrique. *Theor. Comp. Sciences*, 15:77–110, 1981.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.

[LD06] R. Lercier and Lubicz D. A quasi-quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006.

[LL03] R. Lercier and D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In Eli Biham, editor, *Advances in Cryptology—EUROCRYPT '2003*, Lecture Notes in Computer Science. Springer-Verlag, May 2003.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.

[LW02] Alan G. B. Lauder and Daqing Wan. Computing Zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55 (electronic), 2002.

[Mes01] Jean-François Mestre. Lettre à Gaudry et Harley, 2001. Available at `http://www.math.jussieu.fr/mestre`.

[Mes02] Jean-François Mestre. Notes of a talk given at the cryptography seminar Rennes, 2002. Available at `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum67] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum83] David Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum84] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Pap94] Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.

[Rit03] Christophe Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7 - Denis Diderot, June 2003.

[Rob00] Alain M. Robert. *A course in $p$-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Math. Comp.*, 44(170):483–494, 1985.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des nombres de Bordeaux*, 7(1):219–254, 1995.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[VPV01] Frederik Vercauteren, Bart Preneel, and Joos Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2001.