Journal of Symbolic Computation 44 (2009) 1255–1267

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Quasi-quadratic elliptic curve point counting using rigid cohomology☆

Hendrik Hubrechts [1]

Department of Mathematics, Katholieke Universiteit Leuven, Celestijnenlaan 200B - bus 2400, B-3001 Heverlee, Belgium

ARTICLE INFO

Article history:
Received 19 October 2007
Accepted 22 February 2008
Available online 13 February 2009

Keywords:
Elliptic curve
Point counting
Rigid cohomology
Cryptography

ABSTRACT

Let E be a nonsupersingular elliptic curve over the finite field with p^n elements. We present a deterministic algorithm that computes the zeta function and hence the number of points of such a curve E in time quasi-quadratic in n. An older algorithm having the same time complexity uses the canonical lift of E, whereas our algorithm uses rigid cohomology combined with a deformation approach. An implementation in small odd characteristic turns out to give very good results.

1. Introduction

Elliptic curves are a central research object in mathematics, not only centuries and decades ago, but even today with a lot of important unsolved problems concerning such curves. The most notorious example is of course the conjecture of Birch and Swinnerton-Dyer (1965), a solution of which is worth a million dollars (Millenium Prize Problems, 2000). In recent times elliptic curves over finite fields have drawn the attention of cryptographers, as Koblitz (1987) and Miller (1986) suggested exploiting the group structure on such curves for creating a trapdoor one-way function. The motivation for this proposal is that computing discrete logarithms — i.e. solving equations of the kind $x \cdot P = Q$ for given points P and Q on E and an unknown integer x — is considered to be very hard for most elliptic curves, while computing the group operation and hence the product $x \cdot P$ can be done very fast. Such one-way functions can be used in many cryptographic protocols, for example Diffie–Hellman key exchange (Diffie and Hellman, 1976) or ElGamal encryption (ElGamal, 1985). A very broad exposition can be found in the book by Cohen et al. (2006). An important parameter required for estimating the security

☆ The author is a Postdoctoral Fellow of the Fund for Scientific Research - Flanders (Belgium) (F.W.O. Vlaanderen).
E-mail address: Hendrik.Hubrechts@wis.kuleuven.be.
URL: http://wis.kuleuven.be/algebra/hubrechts/.
[1] Tel.: +32 0 16 32 70 06; fax: +32 0 16 32 79 98.

0747-7171/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.02.015

level of this kind of application is the order of the group involved, in this case hence the order of the elliptic curve — it should for example have one large prime factor. We will further on give a brief overview of the large amount of work that has been done on this *point counting* subject. For now, we content ourselves with noting that determining the number of rational points on curves over a finite field of characteristic 2 and of sizes suitable for cryptography can be accomplished in time (far) less than a second (Vercauteren, 2003).

1.1. The zeta function and supersingular curves

Let $\mathbb{F}_q$ be the finite field with q elements and E an elliptic curve defined over $\mathbb{F}_q$; then the zeta function of E is defined as follows:

$$Z(T) := \exp\left(\sum_{k=1}^{\infty} \frac{\#E(\mathbb{F}_{q^k})}{k} T^k\right),$$

where $\#E(\mathbb{F}_{q^k})$ is the number of $\mathbb{F}_{q^k}$-rational points on E (seen as a projective curve). It is well-known that $Z(T)$ is actually a rational function, or more precisely

$$Z(T) = \frac{qT^2 - tT + 1}{(1-T)(1-qT)}, \quad t \in \mathbb{Z},\ |t| \leq 2\sqrt{q}.$$

A proof of this theorem of Hasse and Weil can be found for example in §V.2 of Silverman (1992). The integer t in the zeta function is called the trace of Frobenius (also called just the trace), for reasons that will become clear further on in this paper. It is not hard to see that the number $\#E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on E is precisely $q + 1 - t$. We can conclude that counting the number of points on E is equivalent to computing its zeta function or its trace t.

Curves for which $t \equiv 0 \bmod p$ are called supersingular, and in §V.4 of Silverman (1992) an easy criterion is given for deciding whether a given curve is supersingular. These curves are quite rare and there are only a few possible values for their trace; a list with a proof can be found in Waterhouse (1969).

We note that if we are given the zeta function of E over $\mathbb{F}_q$, it is easy to find the zeta function over extension fields of $\mathbb{F}_q$. Indeed, if we denote with $Z_k(T)$ the numerator of the zeta function of E over $\mathbb{F}_{q^k}$, then an easy calculation shows that $Z_k(T)$ equals the following resultant:

$$Z_k(T) = \mathrm{Res}_X(Z_1(X); X^k - T). \tag{1}$$

1.2. Point counting algorithms

In the following overview we limit our exposition to nonsupersingular elliptic curves over finite fields with $q := p^n$ elements, where p is a small prime number (e.g. $p \leq 7$). For the complexity estimates – which are always meant bitwise – we use the classical Big-Oh notation $\mathcal{O}$, together with the Soft-Oh notation $\widetilde{\mathcal{O}}$ as defined in von zur Gathen and Gerhard (2003, Definition 25.8) that ignores logarithmic factors. Using the above remark we ignore the dependency on p of the algorithms, which is irrelevant for very small primes. In all complexity estimates asymptotically fast arithmetic is assumed; see Bernstein (in press). The algebraic closure of a field k will be denoted by $\bar{k}$.

A very nice and complete overview of the history of elliptic curve point counting can be found in Chapter 17 of the book by Cohen et al. (2006). The first general algorithm is due to Schoof, and improvements by Elkies and Atkin have led to the well-known SEA algorithm, which runs in heuristic time $\widetilde{\mathcal{O}}(n^4)$ and requires $\mathcal{O}(n^2)$ memory. It is often called 'ℓ-adic', because it works by computing the trace of Frobenius modulo prime numbers $\ell \neq p$. Having done this for enough small primes ℓ, this allows one to recover the trace.

A different approach was considered by Satoh, who found that p-adic methods might be much more efficient for small primes p than the technique of Schoof. Satoh's method is based on the *canonical lift* $\mathcal{E}$ of the curve E. Let $\mathbb{Q}_q$ be the unramified degree n extension of the p-adic field $\mathbb{Q}_p$; then $\mathcal{E}$ is defined to be the unique (up to isomorphism) lift of E to an elliptic curve over $\mathbb{Q}_q$ which has an endomorphism

ring that is isomorphic to the one of E, with the isomorphism given by reduction modulo p. The idea then is to approximate the j-invariant J of this canonical lift modulo an appropriate power of p and afterwards analyze the action of the qth-power Frobenius on the lift in order to compute its trace. In later optimizations of the algorithm two main steps arose. First we have to solve a polynomial equation $\psi(J, J^\sigma) = 0$ over $\mathbb{Q}_q$, where J is congruent modulo p to the j-invariant of E and $\sigma : \mathbb{Q}_q \to \mathbb{Q}_q$ is the Frobenius automorphism. A second step consists of computing the norm $\mathcal{N}_{\mathbb{Q}_q/\mathbb{Q}_p}$ of an element of $\mathbb{Q}_q$. Satoh's original algorithm (Satoh, 2000) worked in time $\widetilde{\mathcal{O}}(n^3)$ and required $\mathcal{O}(n^3)$ memory space. After a lot of improvements by Vercauteren et al. (2001), Mestre's AGM Mestre (2000) and Satoh et al. (SST) (2003) and others, a computation time of $\widetilde{\mathcal{O}}(n^{2.5})$ and space $\mathcal{O}(n^2)$ were achieved. The fastest method however, working for all finite fields of small characteristic, is the algorithm of Harley, as described in his e-mail (Harley, 2002). It requires time $\widetilde{\mathcal{O}}(n^2)$ and memory $\mathcal{O}(n^2)$, and does not need any precomputations, in contrast to SST. The basic improvements of Harley are fast ways to compute a good representation of $\mathbb{Q}_q$, to solve equations of the kind $aX^\sigma + pbX + c = 0$ over $\mathbb{Z}_q$ and to compute the norm $\mathcal{N}_{\mathbb{Q}_q/\mathbb{Q}_p}$ of an element of $\mathbb{Q}_q$. A complete description can be found in Section 3.10 of Vercauteren (2003).

1.3. An $\widetilde{\mathcal{O}}(n^2)$, $\mathcal{O}(n^2)$ algorithm using a rigid lift

In this paper we describe a new algorithm that has the same complexities as Harley's result, but is based on a different approach. Kedlaya (2001) gave an algorithm for computing the zeta function of a hyperelliptic curve of genus g over $\mathbb{F}_{p^n}$ for odd p in time $\widetilde{\mathcal{O}}(g^4 n^3)$ and space $\mathcal{O}(g^3 n^3)$. It uses not the canonical lift (for elliptic curves), but a rigid lift, which is trivial to compute. If we take the de Rham cohomology of this lifted curve, a Lefschetz fixed point theorem of Monsky and Washnitzer tells us that the characteristic polynomial of the Frobenius operator on this cohomology yields the zeta function of the curve. Three points are crucial. First, if the lift is well-chosen (it has to preserve the geometry of the curve) we can effectively compute in this Monsky–Washnitzer cohomology due to it being isomorphic to the de Rham cohomology of the algebraic lift. Second, because Kedlaya cuts out Weierstrass points, the action of the pth-power Frobenius is readily computable. And third, factoring the qth-power Frobenius in repeated applications of the pth-power Frobenius makes sure that the power series appearing converge well enough. Later on Denef and Vercauteren (2006) extended Kedlaya's method to the technically more challenging case of characteristic 2.

Lauder (2004) started using deformation in order to compute the zeta function of higher dimensional varieties. This works by placing the variety in a well-chosen one-parameter family, say with formal parameter Γ, and computing the general matrix $F(\Gamma)$ of the pth-power Frobenius. As shown earlier by Dwork (1963) such a matrix satisfies a differential equation, the Picard–Fuchs equation of the deformation, and this equation allows fast calculation of $F(\Gamma)$ modulo a certain power of Γ. In a next step the matrix $F(\Gamma)$ is specialized to $F(\gamma)$ for some $\gamma \in \mathbb{Q}_q$ and computing the matrix of the qth-power Frobenius from this $F(\gamma)$ yields then the zeta function. In Hubrechts (2008, 2007) we followed a suggestion of Denef and Lauder of trying to combine such a deformation with Kedlaya's and Denef and Vercauteren's algorithms, which resulted in an $\widetilde{\mathcal{O}}(n^{2.667})$ algorithm for hyperelliptic curves in certain families. The most time-consuming step in these algorithms is the computation of the 'norm' of the matrix $F(\gamma)$, i.e. the product of its conjugates in the right order. For elliptic curves we show in this paper that all curves can be placed in a good family and that we can reduce the matrix-norm computation to calculating the norm of just *one* element of $\mathbb{Q}_q$. Using Harley's fast norm computation algorithm this gives then the aforementioned complexities. We note that Harley's other basic improvements are also used in our algorithm.

We now briefly sketch the structure of this paper. In Section 2 we describe how to place an elliptic curve in a good linear family defined over the prime field. In the next two sections we repeat in a concise way how the theory of Hubrechts (2008, 2007) allows us to compute efficiently the matrix of the pth-power Frobenius for curves in such a family. In addition we explain how to recover a p-adic integral matrix of this Frobenius operator, which is not guaranteed by the original algorithms of these papers. In the fifth section is shown how to compute the trace of the qth-power Frobenius from this matrix and in the last section we present an overview of our algorithm and some results obtained with an implementation of (a variant of) it.

2. The curve placed in a one-parameter family

Let E be a nonsupersingular elliptic curve over a finite field $\mathbb{F}_q$, given by its Weierstrass equation

$$Y^2 + (aX + b)Y = X^3 + cX^2 + \mathrm{d}X + e \quad \text{with } a, b, c, d, e \in \mathbb{F}_q. \tag{2}$$

We will show in this section how to efficiently reduce the equation for E to another equation over $\mathbb{F}_q$, defining E', such that this last one can be tackled directly using the deformation technique of Sections 3 and 4. The resulting elliptic curve E' will be isomorphic either to the original curve or to its quadratic twist, denoted by Twist(E). It is well-known (and easily proven) that the trace of Frobenius t of E equals minus the trace of Frobenius of Twist(E), and hence it suffices to work with E'. Note that it will be clear in each case which one of the two isomorphisms, $E' \cong E$ or $E' \cong \mathrm{Twist}(E)$, holds. We have to stress that these results are certainly not new, but we did not find a good reference and the explicit way to find the curve E', along with a bound on the computational complexity of this step, is an important part of the algorithm.

2.1. Odd characteristic

Let p be an odd prime and $\mathbb{F}_q$ the finite field of cardinality $q = p^n$. We may suppose that the elliptic curve E over $\mathbb{F}_q$ is given by

$$Y^2 = X^3 + aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_q. \tag{3}$$

If $p \neq 3$ the translation $X \mapsto X - a/3$ removes the term with X^2 in (3), so we can suppose in this case that $a = 0$. If moreover $c = 0$ this can be written as $Y^2 = X^3 + \bar{\gamma}X$ with $\bar{\gamma} := b$, a form suitable for Section 3, so we may assume that $c \neq 0$. Similarly we can assume that $b \neq 0$. The notation $(\mathbb{F}_q)^2$ will be used for the set of squares of $\mathbb{F}_q$.

Proposition 1. *Suppose that $bc \neq 0$ and that E is given by $Y^2 = X^3 + bX + c$. Let $\bar{\gamma} := b^3/c^2$ and let E' be the elliptic curve over $\mathbb{F}_q$ defined by $Y^2 = X^3 + \bar{\gamma}X + \bar{\gamma}$. If $b/c \in (\mathbb{F}_q)^2$ we have that $E' \cong E$ (over $\mathbb{F}_q$), and otherwise $E' \cong$ Twist(E).*

Proof. Let $d := b/c$. The equation of E' is then given by $Y^2 = X^3 + bd^2X + cd^3$ and hence satisfies the conclusions in the proposition. □

Now let us consider the case $p = 3$. When $a = 0$ in (3) the curve is supersingular because its j-invariant is zero. For $a \neq 0$ the translation $X \mapsto X - \frac{b}{2a}$ removes the linear term in (3), so we can suppose for the next proposition that $a \neq 0$ and $b = 0$.

Proposition 2. *Let E be given by $Y^2 = X^3 + aX^2 + c$ where $ac \neq 0$. Define $\bar{\gamma} := c/a^3$ and the elliptic curve E' with equation $Y^2 = X^3 + X^2 + \bar{\gamma}$. If $a \in (\mathbb{F}_q)^2$ we have that $E' \cong E$, and otherwise $E' \cong$ Twist(E).*

Proof. If we 'twist' E using a^{-1}, we find immediately the result $Y^2 = X^3 + X^2 + c/a^3$. □

We can conclude that given any elliptic curve over $\mathbb{F}_q$ with q odd, we can always find $\bar{\gamma} \in \mathbb{F}_q$ and some polynomial $Q(X, \Gamma)$ over $\mathbb{F}_p$ such that the following holds: $Q(X, \Gamma)$ is monic of degree 3 in X and linear in Γ and it suffices to compute the zeta function of $Y^2 = Q(X, \bar{\gamma})$. In addition, $Q(X, \Gamma)$ and $\bar{\gamma}$ can be computed very fast. Indeed, the complexity is dominated by verifying whether b/c (or a) is a square in $\mathbb{F}_q$ and as $x \in (\mathbb{F}_q^{\times})^2$ is equivalent to $x^{(q-1)/2} = 1$, this can certainly be done in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n)$. For practical purposes a much faster algorithm can be found in Cohen et al. (2006, Section 11.3.5).

In Section 3 we will need that $Y^2 = Q(X, 0)$ defines an elliptic curve over $\mathbb{F}_p$, but this can always be achieved by the translation $\Gamma \mapsto \Gamma + \alpha$ for some $\alpha \in \mathbb{F}_p$. It is interesting to make the degree in Γ of the resultant $\mathrm{Res}_X(Q(X, \Gamma); \frac{\partial}{\partial X}Q(X, \Gamma))$ as small as possible (where we interpret $Q(X, \Gamma) \in \mathbb{Z}[X, \Gamma]$ for the moment). In Proposition 1 this will be 3 and in Proposition 2 we find degree 2. If $\bar{\gamma} \in (\mathbb{F}_q)^2$ in Proposition 1, we can twist over $1/\sqrt{\bar{\gamma}}$ and find $Y^2 = X^3 + X + \bar{\gamma}'$ for some $\bar{\gamma}' \in \mathbb{F}_q$, which also gives a resultant of degree two. Although this requires the computation of a square root in $\mathbb{F}_q$, it might still be advantageous in the end.

It is a classical result that for every elliptic curve you can find an isomorphic curve with equation $Y^2 = X(X-1)(X-\bar{\lambda})$ — called the Legendre form — which after the substitution $\Gamma - 1 \leftarrow \bar{\lambda}$ also satisfies the requirements needed in Section 3. However, often the isomorphism, or even the parameter $\bar{\lambda}$ itself, is not defined over the base field $\mathbb{F}_q$, and hence this Legendre form would allow us only to compute the zeta function of E over some extension field of $\mathbb{F}_q$.

2.2. Characteristic 2

We now take $q = 2^n$ and E the elliptic curve over $\mathbb{F}_q$ given by (2). The fact that E is not supersingular is easily seen to be equivalent to $a \neq 0$. The translation $X \mapsto X + b/a$ shows that we can suppose that $b = 0$, and with $b = 0$ the translation $Y \mapsto Y + \sqrt{e}$ gives that we can take $e = 0$ as well. Finally $Y \mapsto a^3 Y$ and $X \mapsto a^2 X$ gives the form

$$Y^2 + XY = X(X^2 + AX + B), \qquad A, B \in \mathbb{F}_q$$

as the equation for the curve E. Hilbert's Satz 90 shows that $\alpha^2 + \alpha + A = 0$ has a solution $\alpha \in \mathbb{F}_q$ if and only if $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 0$. If this trace equals 1 we can take α in a degree 2 extension of $\mathbb{F}_q$. The change of variables $Y \mapsto Y + \alpha X$ yields then the elliptic curve E' with equation $Y^2 + XY = X(X^2 + B)$. The conclusion is that $E' \cong E$ over $\mathbb{F}_q$ if $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 0$; otherwise we have $E' \cong \mathrm{Twist}(E)$.

Analogously we can find for supersingular curves an equation $Y^2 + \bar{\gamma} Y = X^3 + X^2$ or $Y^2 + \bar{\gamma} Y = X^3$ with properties similar to the above. We do not work this out, as we do not need it anyway.

Define $H(X) := X$, $Q_f(X, \Gamma) := X^2 + \Gamma + 1$ and $\bar{\gamma} := B$; then we have proven that it suffices to compute the zeta function of the elliptic curve with equation

$$Y^2 + H(X) \cdot Y = H(X) \cdot Q_f(X, \bar{\gamma} + 1),$$

where $H(X), Q_f(X, \Gamma) \in \mathbb{F}_2[X, \Gamma]$ and $\bar{\gamma} \in \mathbb{F}_q$. Moreover, the equation $Y^2 + H(X) \cdot Y = H(X) \cdot Q_f(X, 0)$ also defines an elliptic curve. Again the above transformations can be done very fast in practice. The most time-consuming step is computing $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A)$, which can easily be done in time $\widetilde{\mathcal{O}}(n^2)$, or in time $\mathcal{O}(n^2)$ using the algorithm in Shoup (1999). The memory requirements are only $\mathcal{O}(n)$.

3. *p*th-power Frobenius in odd characteristic

Now that we have put our elliptic curve – possibly up to a quadratic twist – in a linear family, we will show how to compute the matrix of the pth-power Frobenius on its Monsky–Washnitzer cohomology. This cohomology was first applied by Kedlaya (2001) in an algorithm to count the number of points on hyperelliptic curves in odd characteristic. We have worked out the deformation approach in great detail in Hubrechts (2008) and we will give a short summary in this section, specified to genus 1 and with $\mathbb{F}_p$ as base field. We refer the reader to the original paper for more details.

3.1. A sketch of the deformation theory

We assume in this section that p is an odd prime. Let $\bar{Q}(X, \Gamma) \in \mathbb{F}_p[X, \Gamma]$ be of the form explained at the end of Section 2.1, in particular monic of degree 3 in X and squarefree for $\Gamma = 0$. Suppose that we need the zeta function of the elliptic curve $E : Y^2 = \bar{Q}(X, \bar{\gamma})$ for some parameter $\bar{\gamma}$ algebraic over $\mathbb{F}_p$, and let the finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$ be defined as $\mathbb{F}_p[x]/\bar{\varphi}(x)$ with $\bar{\varphi}(x)$ the minimal polynomial of $\bar{\gamma}$ over $\mathbb{F}_p$.

Remark 3. The general case can indeed be reduced to this setting. Suppose that we are given $\mathbb{F}_{p^m}$ and $\bar{\gamma} \in \mathbb{F}_{p^m}$ with $1 \leq n \leq m$; then Shoup (1999) shows how to compute the minimal polynomial of $\bar{\gamma}$ over $\mathbb{F}_p$ in time $\mathcal{O}(m^2)$, with which we can denote $\mathbb{F}_q$ in the form explained above. Having computed the zeta function over $\mathbb{F}_q$ and if $n < m$, we can use formula (1) to conclude the algorithm.

Denote with $\mathbb{Q}_p$ the field of p-adic numbers and with $\mathbb{Q}_q$ the unique degree n unramified extension of $\mathbb{Q}_p$. In fact we need a very specific representation of $\mathbb{Q}_q$, which will be explained at the end of Section 3.2. We write $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for the rings of integers of these fields. The Frobenius automorphism

on $\mathbb{Q}_q$ — the lift to $\mathbb{Q}_q$ of the map $x \mapsto x^p$ on $\mathbb{F}_q$ — is denoted by σ. The valuation on $\mathbb{Q}_q$ is written as ord, normalized to $\mathrm{ord}(p) = 1$. The Teichmüller lift γ of an element $\bar{\gamma} \in \mathbb{F}_q$ is defined as the unique root of unity in $\mathbb{Q}_q$ that reduces modulo p to $\bar{\gamma}$.

The Monsky–Washnitzer construction starts with a degree preserving lift $Q(X, \Gamma) \in \mathbb{Z}_p[X, \Gamma]$ of $\bar{Q}(X, \Gamma)$. Define the resultant

$$r(\Gamma) := \mathrm{Res}_X \left(Q(X, \Gamma); \frac{\partial}{\partial X} Q(X, \Gamma) \right).$$

Then we find that $\bar{r}(0)$ and $\bar{r}(\bar{\gamma})$ (where $\bar{}$ denotes the reduction modulo p) are both nonzero due to the fact that 0 and $\bar{\gamma}$ give (nonsingular) elliptic curves. Write $r(\Gamma) = \sum r_i \Gamma^i$ and let ρ' be the largest index i such that $\mathrm{ord}(r_i) = 0$. Then we define $R(\Gamma) := \sum_{i=0}^{\rho'} r_i \Gamma^i$, so that $R(\Gamma)$ has as leading coefficient a unit in $\mathbb{Z}_p$ and $R(\Gamma) \equiv r(\Gamma) \bmod p$. Define the ring $S^\dagger := \mathbb{Q}_p[\Gamma, 1/R(\Gamma)]^\dagger$ and the $S^\dagger$-module

$$T^\dagger := \frac{\mathbb{Q}_p[X, Y, 1/Y, \Gamma, 1/R(\Gamma)]^\dagger}{(Y^2 - Q(X, \Gamma))}.$$

Here $\dagger$ denotes the overconvergent completion as defined in Kedlaya (2001), e.g. $\mathbb{Q}_q[\Gamma]^\dagger$ consists of all power series in Γ that converge on a disk strictly bigger than the unit disk. On $T^\dagger$ there act two differential operators, namely $d : T^\dagger \to T^\dagger \mathrm{d}X : v \mapsto \frac{\partial v}{\partial X} \mathrm{d}X$, and the connection $\nabla : T^\dagger \to T^\dagger d\Gamma : v \mapsto \frac{\partial v}{\partial \Gamma} d\Gamma$ satisfying $d\Gamma = \nabla X = 0$. The submodule H^-_{MW} of $T^\dagger \mathrm{d}X / dT^\dagger$ is defined as the eigenspace corresponding to the eigenvalue -1 under the elliptic involution and is a free $S^\dagger$-module of rank 2. With F_p as the pth-power Frobenius map on H^-_{MW} and $F_p(d\Gamma) := d(F_p(\Gamma))$, we find the following commutative diagram:

$$\begin{array}{ccc} H^-_{MW} & \xrightarrow{\nabla} & H^-_{MW} d\Gamma \\ \downarrow{\scriptstyle F_p} & & \downarrow{\scriptstyle F_p} \\ H^-_{MW} & \xrightarrow{\nabla} & H^-_{MW} d\Gamma. \end{array} \tag{4}$$

The basis used in Hubrechts (2008) for H^-_{MW} is the pair $\{\mathrm{d}X/\sqrt{Q}, X\mathrm{d}X/\sqrt{Q}\}$, and with $F(\Gamma)$ as matrix for the map F_p w.r.t. this basis and $G(\Gamma)$ for ∇, diagram (4) gives the differential equation

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) G(\Gamma) = p \Gamma^{p-1} G(\Gamma^p) F(\Gamma). \tag{5}$$

Let γ be the Teichmüller lift of $\bar{\gamma}$ in $\mathbb{Z}_q$; then the matrix $F(\gamma)$ is precisely the matrix of the pth-power Frobenius on the Monsky–Washnitzer cohomology of the curve $Y^2 = Q(X, \gamma)$ as found by Kedlaya (2001).

3.2. Computational issues

In Section 5 we will need the matrix $F(\gamma)$ up to a certain p-adic precision $N = \mathcal{O}(n)$. Following the algorithm in Hubrechts (2008) with $g = a = \kappa = 1$ and limiting ourselves to Steps 1 to 7 of the algorithm, this can be achieved in time $\tilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$.

There are two important points to note. First, we will need that $F(\gamma)$ is p-adic integral, which is a priori only guaranteed with our chosen basis if $p > 3$ (see Section 3.5 of Kedlaya (2004)). Two possible solutions emerge. We can imitate the proofs of our earlier paper, but now with the basis $\{\mathrm{d}X/\sqrt{Q}^3, X\mathrm{d}X/\sqrt{Q}^3\}$, which does give an integral matrix as explained in Kedlaya (2004). The asymptotic complexity estimates will remain the same in this case; this is the solution used in the implementation that we made. Another possible work-around is to compute the matrix of the change between the two bases, a matrix that can be shown to become integral after multiplication with p and is easily retrieved using the reduction algorithm of Kedlaya (2001). Transforming $F(\gamma)$ using this matrix yields then an integral matrix of Frobenius.

Second, in the algorithm a particular representation of $\mathbb{Q}_q = \mathbb{Q}_p[x]/\varphi(x)$ is used, namely $\varphi(x)$ has to be a *Teichmüller modulus* lift of $\bar{\varphi}(x)$. This means that both polynomials are congruent modulo p and that $\varphi(x)$ is a monic divisor of $x^q - x$. Equivalently we can say that $\varphi(x)$ is the minimal polynomial of the Teichmüller lift γ of $\bar{\gamma}$. In Cohen et al. (2006, Section 12.1.2) a very efficient algorithm for computing $\varphi(x)$ is given, originally due to Harley, that computes $\varphi(x)$ modulo $p^{\mathcal{O}(n)}$ in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$.

4. Second-power Frobenius in characteristic 2

As proven in Section 2.2, it suffices to consider elliptic curves given by

$$Y^2 + XY = X(X^2 + \bar{\gamma} + 1), \quad \bar{\gamma} \in \mathbb{F}_q,\ q = 2^n. \tag{6}$$

Again we will explain briefly how to compute the matrix of the second-power Frobenius on the Monsky–Washnitzer cohomology of the curve. It was first shown by Denef and Vercauteren (2006) how to do this in time $\widetilde{\mathcal{O}}(n^3)$ and space $\mathcal{O}(n^3)$, and in Hubrechts (2007) we extended this result so that it worked faster and used less memory in one-dimensional families. We will now sketch how this works; all details can be found in our earlier paper.

4.1. Computing the matrix of Frobenius

We suppose as in the previous section that $\mathbb{F}_q$ is given as $\mathbb{F}_2[x]$ modulo the minimal polynomial of $\bar{\gamma}$. Define $\mathbb{Q}_2$, $\mathbb{Q}_q$, $\mathbb{Z}_2$, $\mathbb{Z}_q$, σ and $\gamma \in \mathbb{Z}_q$ as before and let $H(X) := X$ and $Q_f(X, \Gamma) := X^2 + \Gamma + 1$. The polynomial $c(\Gamma)$ from Hubrechts (2007) is just equal to 1 in our case. The resultant needed is $r(\Gamma) = \mathrm{Res}_X(H; Q_f \cdot \frac{\partial H}{\partial X}) = \Gamma + 1$ and clearly both $\bar{r}(0)$ and $\bar{r}(\bar{\gamma})$ are nonzero in $\mathbb{F}_q$. Moreover, defining $R(\Gamma)$ as before yields $R(\Gamma) = r(\Gamma)$. The ring $S^\dagger$ is defined as $S^\dagger := \mathbb{Q}_2[\Gamma, 1/(\Gamma + 1)]^\dagger$ and the $S^\dagger$-module $T^\dagger$ as

$$T^\dagger := \frac{\mathbb{Q}_2[X, Y, 1/X, \Gamma, 1/(\Gamma + 1)]^\dagger}{(Y^2 + XY - X(X^2 + \Gamma + 1))}.$$

Using the definitions of d, ∇ and H^-_{MW} as before we find again diagram (4) and Eq. (5) with $\mathcal{B} := \{Y\mathrm{d}X, XY\mathrm{d}X\}$ as basis for H^-_{MW}. Here too we get $F(\gamma)$ with precision $N = \mathcal{O}(n)$, again using the Teichmüller modulus representation of $\mathbb{Q}_q$. However, in order to get an integral matrix our chosen basis does not suffice. Indeed, from the proof of Proposition 11 from Hubrechts (2007) it follows that only $2^6 \cdot F(\gamma)$ is guaranteed to be integral. We will show in the next subsection how this problem can be solved. The conclusion will be that we have to compute $F(\gamma)$ modulo 2^{N+13} and can transform this matrix afterwards into a matrix of Frobenius modulo 2^N (w.r.t. a different basis) with integral coefficients. As follows from the algorithm of Hubrechts (2007), we can find this approximation of $F(\gamma)$ in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$.

We would like to mention that Gerkmann (2008) considered a deformation for the same family $Y^2 + XY = X(X^2 + \gamma)$ that we used above.

4.2. An integral matrix of Frobenius

We will now show how to remedy the 'integrality problem'. The eigenvalues of the qth-power Frobenius map are the reciprocal zeros of the numerator of the zeta function, and are hence p-adic integers. This implies that a $\mathbb{Z}_q$-submodule of maximal rank of H^-_{MW} does exist that is stable under this map. Indeed, in Section 5 we will show that the two eigenvalues are different; hence the submodule spanned by corresponding eigenvectors satisfies this condition. Edixhoven (2003, Proposition 5.3.1) showed how to find a basis for a submodule that is stable under F_p, and Denef and Vercauteren (2007) applied this to their characteristic 2 situation. We will show that $\mathcal{D} := \{\frac{\mathrm{d}X}{2Y+X}, \frac{X\mathrm{d}X}{2Y+X}\}$ is such an 'integral basis'. It might be possible to reconstruct the algorithm explained above using this basis, but in this section we will explain how to use the matrix of the change of basis in order to achieve an integral matrix of Frobenius.

We now briefly recall the result of the erratum (Denef and Vercauteren, 2007), specialized to our situation. The modules H_1 and H_1^- are as defined in Denef and Vercauteren (2006); essentially

they are the modules $T^\dagger \mathrm{d}X/dT^\dagger$ and H^-_{MW} from above, but specialized to $\Gamma = \gamma$. The curve $E : Y^2 + XY - X(X^2 + \gamma + 1) = 0$ is a smooth and proper curve over $\mathbb{Z}_q$, and $E\backslash\{P_\infty\}$ is affine, with P_∞ the point at infinity of E. Let $D = kP_\infty$ be a divisor on E for some $k \geq 2$. We define a $\mathbb{Z}_q$-module L as consisting of those differentials ω on $E\backslash\{P_\infty\}$ that satisfy the following two conditions. First, we require that $\mathrm{div}(\omega) + D \geq 0$, and second, each term with valuation less than -1 in the local expansion of ω at P_∞ is integrable over $\mathbb{Z}_q$. Then the image of L in H_1 is independent of the choice of the divisor D and invariant under the pth-power Frobenius, and L generates H_1. Hence we have also that $L \cap H_1^-$ generates H_1^-.

To see that $\mathcal{D}$ is a basis for this $\mathbb{Z}_q$-module $L \cap H_1^-$ one can work as follows. Recall from Denef and Vercauteren (2006) that with $t := X/Y$ as local parameter at P_∞, we have

$$X = t^{-2} \cdot \left(1 + \sum_{i=1}^{\infty} \alpha_i t^i\right) \quad \text{and} \quad Y = t^{-3} \cdot \left(1 + \sum_{i=1}^{\infty} \beta_i t^i\right)$$

with all α_i and β_i in $\mathbb{Z}_q$. One verifies easily that, with $a := \mathrm{d}X/(2Y + X)$ and $b := X\mathrm{d}X/(2Y + X)$, equalities

$$a = \left(-1 + \sum_{i=1}^{\infty} \gamma_i t^i\right) \mathrm{d}X \quad \text{and} \quad b = \left(-t^{-2} + \sum_{i=-1}^{\infty} \delta_i t^i\right) \mathrm{d}X$$

hold, and from the expansion (7) below it follows that also all γ_i and δ_i are in $\mathbb{Z}_q$. Moreover, a and b satisfy the integrability condition explained above and are hence both in $L \cap H_1^-$. As $\mathcal{D}$ certainly forms a $\mathbb{Q}_q$-vector space basis for $(L \cap H_1^-) \otimes \mathbb{Q}_q$, we only have to verify that it is a generating set for $L \cap H_1^-$ as $\mathbb{Z}_q$-module. This follows immediately: if for some $\alpha, \beta \in \mathbb{Q}_q$ we have $\alpha a + \beta b \in L$, then $\alpha, \beta \in \mathbb{Z}_q$.

We need a lower bound on the valuation of the matrix of change of basis and its inverse. The differential forms $Y\mathrm{d}X$ and $XY\mathrm{d}X$ from $\mathcal{B}$ have poles of order 6 and 8 respectively at the point P_∞. If we take $D = 8P_\infty$, both forms satisfy the condition $\mathrm{div}(\omega) + D \geq 0$, and 4ω for $\omega \in \mathcal{B}$ will also satisfy the second condition on the integrability. Indeed, during integration only $-7, \ldots, -1$ can appear as denominators, and 4 divided by one of these is always integral in $\mathbb{Z}_2$. This implies that both $4Y\mathrm{d}X$ and $4XY\mathrm{d}X$ are in the $\mathbb{Z}_q$-module $L \cap H_1^-$, which has $\mathcal{D}$ as basis, and hence the matrix defining the change of basis from $\mathcal{D}$ to $\mathcal{B}$ has valuation at least -2.

For the inverse we have to reduce the basis $\mathcal{D}$ to $\mathcal{B}$ and use Lemmata 2 and 3 of Denef and Vercauteren (2006). As

$$\frac{\mathrm{d}X}{2Y + X} = \frac{(2Y + X)\mathrm{d}X}{4X(X^2 + \gamma + 1) + X^2} = \frac{2Y + X}{X^2}\mathrm{d}X \cdot \left(\sum_{k=0}^{\infty} (-4)^k \left(X + \frac{\gamma + 1}{X}\right)^k\right), \tag{7}$$

an easy computation gives as lower bound for the valuation of the matrix of this change of basis

$$\min\left\{\min_{k\geq 3}(1 + 2k - 3 - \lfloor \log_2(k) \rfloor); \min_{k\geq 0}(1 + 2k - 3 - \lfloor \log_2(k + 3) \rfloor)\right\} = -3.$$

Computing this last matrix, denoted with B, modulo 2^M with $M = \mathcal{O}(n)$ is easy using the reduction formulae in Denef and Vercauteren (2006), but this would require time $\widetilde{\mathcal{O}}(n^3)$. We can see however that we do not need B modulo such a large power of 2. Indeed, let B' be any invertible matrix over $\mathbb{Q}_q$ such that $F' := (B'^{-1})^\sigma F(\gamma) B'$ is integral, then B' gives the change to a new (and a priori unknown) basis, and the resulting integral matrix F' is still a matrix of Frobenius. So let $B' \equiv B \bmod 2^\alpha$ for some α; then if B'^{-1} exists and $(B'^{-1})^\sigma F(\gamma) B'$ is integral, we are done. We will show that $\alpha = \mathcal{O}(1)$ suffices. As a consequence, the algorithm of Denef and Vercauteren (2006) allows us to compute B' in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$.

From the valuation bound -2 on B^{-1} above we see that $\mathrm{ord}(\det B)$ is not larger than 4, and hence working with $\alpha \geq 5$ suffices already in order to be able to invert B' (which has to be done to the maximal required precision). It is not hard to verify that $B'^{-1} \equiv B^{-1} \bmod 2^{\alpha-4}$. By writing $B = B' + 2^\alpha B''$ and $B^{-1} = B'^{-1} + 2^{\alpha-4} B'''$ for integral matrices B'' and B''', we can compute the product $(B'^{-1})^\sigma F(\gamma) B'$ and see that it is integral as soon as $\alpha \geq 13$. Hence taking $\alpha := 13$ suffices. The loss in precision in this product is at most $2 + 6 + 3 \leq 13$; hence it suffices certainly to compute $F(\gamma)$ modulo 2^{N+13}.

5. An eigenvalue of the qth-power Frobenius

In this section we will first show that it suffices to compute an approximation of one eigenvalue of the matrix of the qth-power Frobenius, and that this can be reduced to computing a 'semi-eigenvalue' of $F(\gamma)$, in fact an eigenvalue of the σ-linear Frobenius map F_p. In a second subsection we explain how to solve this last problem, by showing that we can always satisfy certain conditions required for an algorithm that computes solutions of a specific type of p-adic equation.

5.1. Reduction to an 'eigenvalue' of $F(\gamma)$

Suppose that E is a nonsupersingular elliptic curve over $\mathbb{F}_q$, where $q = p^n$, and $F = F(\gamma)$ is the p-adic integral matrix of the pth-power Frobenius on its Monsky–Washnitzer cohomology over $\mathbb{Q}_q$, as explained in the two previous sections. For

$$\mathcal{F} := F^{\sigma^{n-1}} \cdot F^{\sigma^{n-2}} \cdots F^{\sigma} \cdot F,$$

the matrix of the qth-power Frobenius, Kedlaya (2001) and Denef and Vercauteren (2006) showed that for the zeta function $Z(T)$ of E over $\mathbb{F}_q$ we have

$$Z(T) = \frac{\det(1 - \mathcal{F}T)}{(1-T)(1-qT)}.$$

As we can write $qT^2 - tT + 1$ for the numerator of the zeta function, it follows immediately that $\det(\mathcal{F}) = q$ and $\mathrm{Tr}(\mathcal{F}) = t$. Let λ_1 and λ_2 be the eigenvalues of $\mathcal{F}$; then obviously $\lambda_1, \lambda_2 \in \mathbb{Z}_q$ and we will prove in the next subsection that we may suppose that $\mathrm{ord}(\lambda_1) = 0$ and hence $\mathrm{ord}(\lambda_2) = \mathrm{ord}(q/\lambda_1) = n$. We are trying to compute $t = \mathrm{Tr}(\mathcal{F}) = \lambda_1 + q/\lambda_1$. The Hasse–Weil bound says for nonsupersingular curves that $|t| < 2\sqrt{q}$; hence we only need to compute λ_1 modulo p^N with

$$N := \lceil \log_p(4\sqrt{q}) \rceil = \lceil n/2 + \log_p(4) \rceil = \mathcal{O}(n). \tag{8}$$

It is clear that – except for some trivial cases – we have $N \leq n$, so $\lambda_2 = q/\lambda_1 \equiv 0 \bmod p^N$. To conclude, it suffices to compute λ_1 modulo p^N in order to find the zeta function of E: the trace t is then the unique rational integer congruent to λ_1 modulo p^N that satisfies $|t| < 2\sqrt{q}$.

If we have matrices C and D over $\mathbb{Z}_q$ such that $F = C^{\sigma} D C^{-1}$ with D in upper triangular form, this implies

$$\mathcal{F} = C \cdot \left(D^{\sigma^{n-1}} \cdot D^{\sigma^{n-2}} \cdots D^{\sigma} \cdot D \right) \cdot C^{-1},$$

and with μ the upper diagonal element of D this gives that the norm $\mathcal{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\mu)$ is an eigenvalue of $\mathcal{F}$. We will show in Section 5.2 that such μ with valuation 0 exists and can be found efficiently provided that E is not supersingular. It is easily seen that a factorization $F = C^{\sigma} D C^{-1}$ over $\mathbb{Q}_q$ cannot exist if the curve is supersingular: the product of the two diagonal elements of D has valuation one, and the sum of their norms has in this case valuation at least one. This is clearly impossible as the valuation is a map from $\mathbb{Q}_q$ to the integers.

Having found μ we still have to compute its norm. For this we can apply an algorithm from Harley, which uses an adaptation of Moenck's extended GCD algorithm in order to compute a certain resultant. Indeed, if $\mathbb{Z}_q = \mathbb{Z}_p[x]/\varphi(x)$ with $\varphi(x)$ a monic irreducible polynomial, and $\mu(x) \in \mathbb{Z}_p[x]/\varphi(x)$, then

$$\mathcal{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\mu) = \mathrm{Res}_x(\mu(x); \varphi(x)).$$

A complete description of the algorithm has been given by Vercauteren (2003, Section 3.10.3). It requires $\widetilde{\mathcal{O}}(n^2)$ time and $\mathcal{O}(n^2)$ space. As noted there, in order for the algorithm to work well, $\mu(x)$ should have as leading coefficient a unit in $\mathbb{Z}_p$. This is however easily forced: suppose $\mu(x) \bmod p$ has degree $n-1-r$; then $x^r \mu(x)$ satisfies this condition. Moreover, x^r itself satisfies the condition as well; hence computing $\mathcal{N}(\mu) = \mathcal{N}(x^r \mu(x))/\mathcal{N}(x^r)$ gives the required result. Note that x^r is a Teichmüller lift with $\mathcal{N}(x^r) = ((-1)^n \varphi(0))^r$, and its norm can thus be computed much faster.

5.2. Computation of an 'eigenvalue' μ of $F(\gamma)$

In this subsection $\equiv$ will always mean 'congruence modulo p', unless 'mod p^N' is explicitly written. We will need an algorithm of Harley with the following input and output; it can be found as Algorithm 12.23 in Cohen et al. (2006). Note that this algorithm requires $\mathbb{Z}_q$ to be given as $\mathbb{Z}_p[x]$ modulo a Teichmüller modulus in order to be efficient.

INPUT: A polynomial $\psi(X, Y) \in \mathbb{Z}_q[X, Y]$, $x_0 \in \mathbb{Z}_q$, such that

$$\psi(x_0, x_0^\sigma) \equiv \frac{\partial \psi}{\partial X}(x_0, x_0^\sigma) \equiv 0, \qquad \frac{\partial \psi}{\partial Y}(x_0, x_0^\sigma) \not\equiv 0.$$

OUTPUT: An element $\alpha \in \mathbb{Z}_q$ such that

$$\psi(\alpha, \alpha^\sigma) \equiv 0 \bmod p^N, \qquad \alpha \equiv x_0.$$

Following the complexity estimates found in Cohen et al. (2006), it is easily shown that if the degree of ψ is fixed, the algorithm runs in time $\widetilde{\mathcal{O}}(nN)$ and space $\mathcal{O}(nN)$.

Write $F = F(\gamma)$ as $\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$ with all f_i in $\mathbb{Z}_q$ and consider the system of equations

$$\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \mu \begin{pmatrix} 1 \\ \alpha^\sigma \end{pmatrix}, \quad \text{or} \quad \begin{cases} f_1 + \alpha f_2 = \mu, \\ f_3 + \alpha f_4 = \mu \alpha^\sigma. \end{cases} \tag{9}$$

It is clear that if we can find a solution $(\alpha, \mu) \in \mathbb{Z}_q \times \mathbb{Z}_q^\times$ for (9), this yields a factorization of $F = (C^\sigma) D C^{-1}$, which is of the kind that we are looking for. Here C and D can e.g. be taken as

$$C = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} \mu & f_2 \\ 0 & f_4 - \alpha^\sigma f_2 \end{pmatrix}.$$

Eliminating μ from the system of Eqs. (9) gives

$$\alpha(\alpha^\sigma f_2 - f_4) + (\alpha^\sigma f_1 - f_3) = 0. \tag{10}$$

If $f_1 \equiv f_2 \equiv 0$, certainly one of f_3, f_4 will not be zero modulo p, as $\operatorname{ord}(\det(F)) = 1$. In this case we can work with the eigenvector $(\alpha \;\; 1)^T$ instead of $(1 \;\; \alpha)^T$. So we can suppose that at least one of f_1 or f_2 is nonzero modulo p. Let

$$x_0^\sigma := \left(\frac{f_4 \bmod p}{f_2 \bmod p} \right), \quad \text{or} \quad x_0^\sigma := \left(\frac{f_3 \bmod p}{f_1 \bmod p} \right).$$

If both definitions make sense, $\det(F) \equiv 0$ implies that they are equal modulo p. Computing the corresponding x_0 is easy finite field arithmetic. We define the polynomial $\psi(X, Y)$ by

$$\psi(X, Y) := X(Yf_2 - f_4) + (Yf_1 - f_3) \quad \in \mathbb{Z}_q[X, Y].$$

Our choice of x_0^σ guarantees that $\psi(x_0, x_0^\sigma) \equiv 0$ and also

$$\frac{\partial}{\partial X} \psi(x_0, x_0^\sigma) = x_0^\sigma f_2 - f_4 \equiv 0.$$

Note that this last inequality holds even if $f_2 \equiv 0$. We will show immediately that $\frac{\partial}{\partial Y} \psi(x_0, x_0^\sigma) \not\equiv 0$ follows from nonsupersingularity. The algorithm from the beginning of this section allows us now to compute $\alpha \in \mathbb{Z}_q$ (with $\alpha \equiv x_0$) and hence also μ, both with precision $N = \mathcal{O}(n)$, in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$. Indeed, denote with $\beta \in \mathbb{Z}_q$ the exact solution of $\psi(\beta, \beta^\sigma) = 0$ and $\beta \equiv x_0$. Then the above algorithm computes α as an approximation of β such that $\psi(\alpha, \alpha^\sigma) \equiv 0 \bmod p^N$. Writing $\alpha = \beta + \beta'$ we know that $\beta' \equiv 0$. If we substitute $\beta + \beta'$ in $\psi(\alpha, \alpha^\sigma)$, we find

$$[\beta^\sigma(\beta f_2 + f_1) - (\beta f_4 + f_3)] + \beta'^\sigma(\beta f_2 + f_1) + \beta' \left[\beta^\sigma f_2 + \beta'^\sigma f_2 - f_4 \right] \equiv 0 \bmod p^N.$$

The sum between the first square brackets is zero, and as $\beta f_2 + f_1$ is a unit in $\mathbb{Z}_q$ (see below) and the last sum between square brackets is zero modulo p, a trivial induction argument shows that $p^N | \beta'^{\sigma}$ and hence $\beta' \equiv 0 \bmod p^N$. This implies that α is indeed computed with precision N. In addition, eliminating α from (9) yields

$$\mu(f_4 - \alpha^{\sigma} f_2) = f_1 f_4 - f_2 f_3,$$

which equals $\det(F)$ and has valuation 1. As $f_4 - \alpha^{\sigma} f_2 \equiv 0$, it is impossible that $\operatorname{ord}(\mu) > 0$ as well, whence $\mu \in \mathbb{Z}_q^{\times}$.

Suppose that $0 \equiv \frac{\partial}{\partial Y}\psi(x_0, x_0^{\sigma}) = x_0 f_2 + f_1$. If $f_2 \equiv 0$ this would imply $f_1 \equiv 0$, which we excluded. Define $f_i' := f_i/f_2$; then

$$f_1' \equiv -x_0, \quad f_4' \equiv x_0^{\sigma} \equiv x_0^p, \quad f_3' \equiv f_1' f_4' \equiv -x_0^{p+1}.$$

As a consequence

$$F \equiv f_2 \begin{pmatrix} -x_0 & 1 \\ -x_0^{p+1} & x_0^p \end{pmatrix} \quad \text{and} \quad F^{\sigma} \cdot F \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

This implies that the trace of $\mathcal{F}$ is congruent to zero modulo p, and hence the curve under consideration is supersingular.

6. Conclusion and implementation results

Combining all steps explained in Sections 2–5 above, we have found a deterministic algorithm that for every nonsupersingular elliptic curve over $\mathbb{F}_{p^n}$ — given by a Weierstrass equation — can compute its zeta function in time $\widetilde{\mathcal{O}}(n^2)$ and space $\mathcal{O}(n^2)$. We will now give a list of the main steps of the algorithm. For ease of exposition we assume that we are working in odd characteristic and with an 'integral basis' for the Monsky–Washnitzer cohomology H^1_{MW}. We do not mention in the algorithm that we only compute approximations modulo a certain power of p and Γ of the objects involved; both precisions are $\mathcal{O}(n)$. If p^n is so small that $N > n$ in (8), we can use a naive point counting algorithm.

`INPUT:` A finite field $\mathbb{F}_{p^n}$ and a monic squarefree degree 3 polynomial $Q(X) \in \mathbb{F}_{p^n}[X]$.

`OUTPUT:` The zeta function of the elliptic curve $Y^2 = Q(X)$ over $\mathbb{F}_{p^n}$.

`STEP 1:` Put the curve in a one-parameter family $Y^2 = Q(X, \bar{\gamma})$ with $\bar{\gamma} \in \mathbb{F}_{p^n}$, as explained in Section 2. In particular, $Q(X, \Gamma) \in \mathbb{F}_p[X, \Gamma]$. This step could require a quadratic twist. Determine $\bar{\varphi}(x) \in \mathbb{F}_p[x]$, the minimal polynomial of $\bar{\gamma}$, as in Shoup (1999) and define $\mathbb{F}_{p^m} := \mathbb{F}_p[x]/\bar{\varphi}(x)$.

`STEP 2:` Determine and solve the differential equation and find $F(\Gamma) \in \mathbb{Z}_p[[\Gamma]]^{2\times 2}$ modulo a sufficiently large power of Γ.

`STEP 3:` Lift $\bar{\varphi}(x)$ to a Teichmüller modulus $\varphi(x)$ so that $\mathbb{Z}_{p^m} = \mathbb{Z}_p[x]/\varphi(x)$ and $x = \gamma$.

`STEP 4:` Compute $F(\gamma)$ by substituting γ in $F(\Gamma)$.

`STEP 5:` Compute a solution (α, μ) with $\operatorname{ord}(\mu) = 0$ for one of the equations

$$F(\gamma) \cdot \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \mu \begin{pmatrix} 1 \\ \alpha^{\sigma} \end{pmatrix} \qquad \text{or} \qquad F(\gamma) \cdot \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \mu \begin{pmatrix} \alpha^{\sigma} \\ 1 \end{pmatrix}.$$

`STEP 6:` Compute the rational integer $t_1 \equiv \mathcal{N}_{\mathbb{Q}_{p^m}/\mathbb{Q}_p}(\mu)$ modulo an appropriate power of p, such that $|t_1| < 2\sqrt{p^m}$. Compute then the resultant

$$p^n T^2 - tT + 1 = \operatorname{Res}_X(p^m X^2 - t_1 X + 1; X^{n/m} - T).$$

`STEP 7:` Change the sign of t if a quadratic twist was required and return

$$\frac{p^n T^2 - tT + 1}{(1-T)(1-p^n T)}.$$

We now present a few timing results obtained with an implementation of this algorithm. We note that we did *not* use Harley's $\widetilde{\mathcal{O}}(n^2)$ norm algorithm for Step 6, but instead the — far easier to implement

and in practice probably faster for reasonable n — algorithm of Satoh et al. (2003). This method runs in time $\widetilde{\mathcal{O}}(n^{2.5})$ given some precomputations. These precomputations require time $\widetilde{\mathcal{O}}(n^3)$, but are completely integer arithmetic and hence extremely fast. In our algorithm we cannot consider them as precomputation (they depend on $\bar{\varphi}(x)$, the minimal polynomial of the parameter $\bar{\gamma}$), so our implementation has as theoretical complexity $\widetilde{\mathcal{O}}(n^3)$. In Step 2 the matrix $F(0)$ as boundary condition for the differential equation is computed using an implementation of Kedlaya's algorithm made by Michael Harrison for odd characteristic, and using our own non-optimized implementation of Denef and Vercauteren's algorithm for characteristic 2. We note that in this last case all Frobenius matrices turn out to be integral, which simplifies the algorithm a lot.

The implementation has been made for the computational algebra system Magma V2.13-15, and the timing results were obtained on an AMD Opteron 875 Dual Core, running at 2.2 MHz and with 32 GB of physical memory available. The author wants to thank Alan Lauder for making this machine available. The algorithm received as input a random elliptic curve over $\mathbb{F}_{p^n}$, given by its Weierstrass equation. For $p = 2$ a random curve with Eq. (6) was given. All times are in seconds.

$p\backslash n$	50	100	250	500	1000	2000	4000	8000
2	.13	.30	1.35	4.85	20	94	528	3199
3	.15	.40	1.98	7.49	33	151	771	4807
5	.46	1.12	5.39	22.54	93	485	2 228	—
7	1.54	3.97	27.71	129.70	675	3713	19 167	—

It is interesting to note that for $n \gg 0$ almost all computation time goes to Steps 3, 5 and 6, the last two being roughly comparable in required time. For example, for $p^n = 3^{4000}$ we have as total time 771 seconds, where Step 5 uses 209 seconds and Step 6 uses 438 seconds. For $p^n = 7^{4000}$ the computation of $\varphi(x)$ takes 17082 seconds. A conclusion that could be drawn from this is that for such big fields our algorithm should work faster than Harley's — as long as in either algorithm the same norm algorithm and no precomputation is used — because Harley's algorithm needs a computation similar to Step 5 but with an equation ψ of higher degree involving a lot more monomials, and exactly the same field polynomial and norm computation.

Step 2 can be considered as precomputation, meaning that it depends only on the field size (and the structure of the family in which the curve lives). For n large enough this step is of minor influence, but for fields of cryptographic size it is worth looking at the time needed for just one curve, ignoring the precomputation. The following table gives some of these times for some small field sizes, hence ignoring the time for Step 2 of the algorithm.

p^n	2^{50}	2^{100}	2^{250}	3^{50}	3^{100}	3^{250}	5^{50}	5^{100}	5^{250}	7^{50}	7^{100}
Time	.07	.18	.82	.08	.26	1.59	.18	0.61	4.05	1.08	3.14

Harley's algorithm for computing the Teichmüller modulus is only practical for $p \leq 7$. For larger primes we have therefore used an algorithm of Satoh (2002), which is reasonably fast in practice although it runs in time $\widetilde{\mathcal{O}}(n^3)$. Below are some results for such higher characteristic.

p^n	11^{100}	11^{500}	17^{100}	17^{500}	29^{100}	29^{500}	101^{100}	1009^{100}
Time	5.27	369	6.65	495	10.99	647	59.62	4076

To conclude, we compare for a few field sizes the time needed for each step of the algorithm separately. The second column in the following table gives a more precise complexity estimate of each step (based on a closer inspection of the algorithms behind the step), where $M(X)$ denotes the time required to multiply two elements of X.

		2^{100}	2^{1000}	3^{100}	3^{1000}	5^{100}	5^{1000}	17^{100}
1	$\mathcal{O}(n^2)$	.00	.04	.00	.46	.01	.78	.02
2	$\mathcal{O}(n \cdot M(\mathbb{Z}_p[X]_{\leq n} \bmod p^{\lceil n \log n \rceil}))$	.12	7.16	.14	2.11	.51	7.23	2.48
3	$\mathcal{O}(\log n \cdot M(\mathbb{Z}_{p^n} \bmod p^n))$	.04	1.89	.05	4.50	.26	40.88	3.24
4	$\mathcal{O}(M(\mathbb{Z}_{p^n} \bmod p^n))$	.01	.59	.02	1.11	.04	5.10	.19
5	$\mathcal{O}(\log n \cdot M(\mathbb{Z}_{p^n} \bmod p^n))$	.07	4.70	.08	10.29	.13	15.74	.30
6	$\mathcal{O}(\log n \cdot M(\mathbb{Z}_{p^n} \bmod p^n))$	.06	5.42	.11	14.40	.17	23.64	.41

Acknowledgements

The author wants to thank Jan Denef for his help on the problem of finding an integral matrix of Frobenius in characteristic 2 and Denef, Wouter Castryck and the anonymous referees for their helpful comments. Fréderik Vercauteren provided some crucial help with the implementation in characteristic 2.

References

Bernstein, D.J., 2003. Fast multiplication and its applications. Buhler–Stevenhagen's Algorithmic number theory (in press) URL: http://cr.yp.to/papers.html#multapps.
Birch, B.J., Swinnerton-Dyer, H.P.F., 1965. Notes on elliptic curves. II. J. Reine Angew. Math. 218, 79–108.
Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F., 2006. Handbook of elliptic and hyperelliptic curve cryptography. In: Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL.
Denef, J., Vercauteren, F., 2006. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. J. Cryptology 19 (1), 1–25. erratum available as Denef and Vercauteren (2007).
Denef, J., Vercauteren, F., 2007. Errata for "An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2", and related papers. Available on http://wis.kuleuven.be/algebra/denef_papers/ErrataPointCounting.pdf.
Diffie, W., Hellman, M.E., 1976. New directions in cryptography. IEEE Trans. Inform. Theory IT-22 (6), 644–654.
Dwork, B., 1963. A deformation theory for the zeta function of a hypersurface. In: Proc. Internat. Congr. Mathematicians (Stockholm, 1962). Inst. Mittag–Leffler, Djursholm, pp. 247–259.
Edixhoven, B., 2003. Point counting after Kedlaya. EIDMA—Stieltjes Graduate course, Leiden.
ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Advances in Cryptology (Santa Barbara, Calif., 1984). In: Lecture Notes in Computer Science, vol. 196. Springer, Berlin, pp. 10–18.
Gerkmann, R., 2008. Relative rigid cohomology and point counting on families of elliptic curves. J. Ramanujan Math. Soc. 23 (1).
Harley, R., 2002. Asymptotically optimal p-adic point-counting. E-mail to NMBRTHRY list.
Hubrechts, H., 2007. Point counting in families of hyperelliptic curves in characteristic 2. LMS J. Comput. Math. 10, 207–234 (electronic).
Hubrechts, H., 2008. Point counting in families of hyperelliptic curves. Found. Comput. Math. 8 (1), 137–169.
Kedlaya, K.S., 2001. Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology. J. Ramanujan Math. Soc. 16 (4), 323–338.
Kedlaya, K.S., 2004. Computing zeta functions via p-adic cohomology. In: Algorithmic Number Theory. In: Lecture Notes in Computer Science, vol. 3076. Springer, Berlin, pp. 1–17.
Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput. 48 (177), 203–209.
Lauder, A.G.B., 2004. Deformation theory and the computation of zeta functions. Proc. London Math. Soc. (3) 88 (3), 565–602.
Mestre, J.-F., 2000. Lettre adressée à Gaudry et Harley. Available on http://www.math.jussieu.fr/~mestre/.
Millennium Prize Problems, 2000. http://www.claymath.org/millennium/.
Miller, V.S., 1986. Use of elliptic curves in cryptography. In: Advances in Cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985). In: Lecture Notes in Computer Science, vol. 218. Springer, Berlin, pp. 417–426.
Satoh, T., 2000. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc. 15 (4), 247–270.
Satoh, T., 2002. On p-adic point counting algorithms for elliptic curves over finite fields. In: Algorithmic Number Theory (Sydney, 2002). In: Lecture Notes in Comput. Sci., vol. 2369. Springer, Berlin, pp. 43–66.
Satoh, T., Skjernaa, B., Taguchi, Y., 2003. Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields Appl. 9 (1), 89–101.
Shoup, V., 1999. Efficient computation of minimal polynomials in algebraic extension of finite fields. In: Proc. 1999 International Symposium on Symbolic and Algebraic Computation.
Silverman, J.H., 1992. The arithmetic of elliptic curves. In: Graduate Texts in Mathematics, vol. 106. Springer-Verlag, New York, corrected reprint of the 1986 original.
Vercauteren, F., 2003. Computing zeta functions of curves over finite fields. Ph.D. Thesis, KULeuven, Belgium.
Vercauteren, F., Preneel, B., Vandewalle, J., 2001. A memory efficient version of Satoh's algorithm. In: Advances in Cryptology—EUROCRYPT 2001 (Innsbruck). In: Lecture Notes in Computer Science, vol. 2045. Springer, Berlin, pp. 1–13.
von zur Gathen, J., Gerhard, J., 2003. Modern Computer Algebra. Cambridge University Press, Cambridge.
Waterhouse, W.C., 1969. Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4) 2, 521–560.