

# Quasi-quadratic elliptic curve point counting using rigid cohomology

Hendrik Hubrechts \*

Department of mathematics, Katholieke Universiteit Leuven

Celestijnenlaan 200B, 3001 Leuven (Belgium)

`Hendrik.Hubrechts@wis.kuleuven.be`

May 7, 2007

## Abstract

We present a deterministic algorithm that computes the zeta function of a nonsupersingular elliptic curve  $E$  over a finite field with  $p^n$  elements 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.

## Extended abstract

### The point counting problem

In modern cryptography, the discrete logarithm problem in finite groups holds a central position. One of the best suited type of groups for this purpose turn out to be elliptic curves over finite fields, as they allow a fast group operation and seem to have strong security properties. An important parameter of such a cryptographic scheme is the size of the curve, i.e. its number of points. Let a curve  $E$  over the finite field  $\mathbb{F}_q$  with  $q$  elements be given, then its number of points (including the point at infinity) equals  $q + 1 - t$ , with  $t$  the *trace of Frobenius*. A lot of research has been done on the subject of the design of algorithms that compute  $t$  for a given curve as fast as possible. If  $q = p^n$ , with  $p$  a small prime, then the fastest algorithm to date is due to Harley, an algorithm that requires  $\tilde{\mathcal{O}}(n^2)$  bit operations and  $\mathcal{O}(n^2)$  bit space. In these complexities we ignore the dependency on  $p$ . This result of Harley has evolved through a number of articles by different authors from an algorithm of Satoh and uses the canonical lift of the curve. In the current paper we present a deterministic algorithm that has the same time and space complexities, but uses a rigid lift of the elliptic curve. Note that the algorithms based on the canonical lift as well as the one described in this paper work only for nonsupersingular curves.

### An $\tilde{\mathcal{O}}(n^2)$ algorithm using rigid cohomology

In [14], Kedlaya described how to use Monsky-Washnitzer cohomology in order to compute the zeta function of hyperelliptic and elliptic curves in odd characteristic and in [5] Denef and Vercauteren extended this to characteristic 2. Both algorithms work in time  $\tilde{\mathcal{O}}(n^3)$ . Our algorithm

---

\*Research Assistant of the Research Foundation - Flanders (FWO - Vlaanderen).

computes, just as these algorithms, the matrix of the  $q$ th power Frobenius on this finite dimensional vector space over  $\mathbb{Q}_q$ . In order to do this in quasi-quadratic time, we use deformation as considered in our papers [12] and [13], see also [17].

A first step in the algorithm is to find for a given elliptic curve an equation that can be placed in a suitable one dimensional family. The result is that — excluding supersingular curves and ignoring some special cases — up to a quadratic twist every elliptic curve in characteristic  $p \geq 5$  can be given by an equation  $Y^2 = X^3 + \bar{\gamma}X + \bar{\gamma}$ , in characteristic 3 we find  $Y^2 = X^3 + X^2 + \bar{\gamma}$  and in even characteristic  $Y^2 + XY + X(X^2 + \bar{\gamma}) = 0$ . In all these equations the parameter  $\bar{\gamma}$  is in the same field  $\mathbb{F}_q$  as over which the original curve was defined. The Monsky-Washnitzer cohomology  $H_{MW}^-$  that we need is a 2-dimensional  $p$ -adic vector space, and using the above form of the curve, the matrix  $F$  of the  $p$ th power Frobenius can be found very efficiently with sufficient  $p$ -adic precision. Indeed, in [12] and [13] we have shown that  $F(\Gamma)$ , the generic matrix of Frobenius for the whole family given by e.g.  $Y^2 = X^3 + \Gamma X + \Gamma$ , satisfies a certain efficiently solvable differential equation

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma)G(\Gamma) = p\Gamma^{p-1}G^\sigma(\Gamma^p)F(\Gamma),$$

$\sigma : \mathbb{Q}_q \rightarrow \mathbb{Q}_q$  being the Frobenius automorphism. Using a well-chosen representation of the field  $\mathbb{Q}_q$  we have also that the matrix  $F = F(\gamma)$ , with  $\gamma$  a Teichmüller lift of  $\bar{\gamma}$ , can be rapidly computed. A complication is that we need an integral matrix of Frobenius, we will explain below how to achieve this.

For the next step of the algorithm we have that with (recall that  $q = p^n$ )

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

the trace of this matrix  $\mathcal{F}$  is precisely the trace of Frobenius  $t$ . Computing  $\mathcal{F}$  from the product (1) will not yield an efficient algorithm, but further on it is briefly explained how we can compute  $t \equiv \text{Tr}(\mathcal{F})$  modulo  $p^N$  with  $N \simeq n/2$ . Having done this, a classical trick using the Hasse-Weil bound  $|t| \leq 2\sqrt{p^n}$  allows us to conclude our algorithm by returning  $q + 1 - t$  as the number of points on the curve.

## Finding an integral Frobenius matrix $F$

For our algorithm it is very important to have a  $p$ -adic integral matrix of Frobenius. In odd characteristic a good basis of  $H_{MW}^-$  does exist that can be used throughout the algorithm, but in characteristic 2 things are — as they seem to be quite often in rigid cohomology — more complicated. We show that we can compute an approximation of a matrix  $B$  of a change of basis, where the new basis does give an integral matrix of Frobenius. The main points in order to be able to do this fast enough are that we have to prove valuation bounds on this matrix  $B$  and its inverse, and that we can show that we need  $B$  only with precision  $\mathcal{O}(1)$  instead of  $\mathcal{O}(n)$ .

## Finding the trace of the $q$ th power Frobenius

Computing  $\mathcal{F}$  directly from the product (1) is not a good idea, although for higher genus it is by now the only way. For nonsupersingular elliptic curves we can however solve the system

$$F \cdot \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \mu \begin{pmatrix} 1 \\ \alpha^\sigma \end{pmatrix}$$

for  $\alpha \in \mathbb{Z}_q$ ,  $\mu \in \mathbb{Z}_q^\times$  — all modulo a certain power of  $p$  — which yields a factorization  $F = C^\sigma DC^{-1}$  over  $\mathbb{Q}_q$  with  $D$  equal to  $\begin{pmatrix} \mu & x \\ 0 & y \end{pmatrix}$  for some  $x, y$  in  $\mathbb{Q}_q$ . As a consequence we have that

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

and the norm  $\lambda := \mathcal{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\mu)$  of  $\mu$  is an eigenvalue of  $\mathcal{F}$ . This eigenvalue  $\lambda$  is a unit in  $\mathbb{Z}_q$ , which implies that  $\text{Tr}(\mathcal{F}) = \lambda + q/\lambda$  and  $q/\lambda \equiv 0 \pmod{p^n}$ . In order to recover the trace of  $\mathcal{F}$ , we only need to compute the norm of  $\mu \in \mathbb{Z}_q$  up to a  $p$ -adic precision of roughly  $n/2$ . This can be done using an algorithm of Harley.

## Implementation results

We have implemented a variant of this algorithm in Magma — only for odd characteristic — and the results are quite good. For a random elliptic curve over  $\mathbb{F}_{3^{100}}$  we can compute its zeta function in about half a second and a curve over  $\mathbb{F}_{3^{1000}}$  takes 46 seconds. Also results in characteristic 5 and 7 are presented.

# 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 [2], a solution of which is worth a million dollar [19]. In recent times elliptic curves over finite fields have drawn the attention of cryptographers, as Koblitz [16] and Miller [20] suggested to exploit the group structure on such curves for creating a trapdoor one way function. The motivation for this proposal is that computing discrete logarithms is considered to be very hard for most elliptic curves, while computing the group operation can be done very fast. A very broad exposition can be found in the book [3]. Such one way functions can be used in many cryptographic protocols, as for example Diffie-Hellman key exchange [6] or ElGamal encryption [9]. An important parameter needed for estimating the security level of these applications 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.

## 1.1 The zeta function and supersingular curves

Let  $E$  be an elliptic curve defined over the finite field  $\mathbb{F}_q$  with  $q$  elements, then we can define its zeta function 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  $E$  (where  $E$  is seen as a projective curve). It is well known that  $Z(T)$  is actually a rational function, more precisely

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

A proof of this theorem of Hasse and Weil can be found for example in [24, §V.2]. The integer  $t$  in the zeta function is called the *trace of Frobenius*, 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  $t \equiv 0 \pmod{p}$  are called *supersingular*, and in [24, §V.4] an easy criterion is given for deciding whether a given curve is supersingular. There are only a few possible values for the trace of a supersingular curve, a list with a proof can be found in [28]. 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  $Z_k(T)$  equals the following resultant:

$$Z_k(T) = \text{Res}_X(Z_1(X); X^k - T). \tag{2}$$

## 1.2 Point counting algorithms

In the following overview we limit our exposition to elliptic curves over finite fields with  $p^n$  elements, where  $p$  is a small prime number (e.g.  $p \leq 7$ ) and for the complexities only  $n$  is taken into account. For the complexity estimates — which are always meant bitwise — we use the classical Big-Oh notation  $\mathcal{O}$ , together with the Soft-Oh notation  $\tilde{\mathcal{O}}$  as defined in [27,

Definition 25.8] that ignores logarithmic factors. Using the above remark we also ignore the dependency on  $p$  of the algorithms, being irrelevant for very small primes. In all complexity estimates asymptotically fast arithmetic is assumed, see [1]. 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 [3] by Cohen, Frey e.a. 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 time  $\tilde{\mathcal{O}}(n^4)$  and requires  $\mathcal{O}(n^2)$  memory. It is often called ‘ $\ell$ -adic’, because it works by computing the trace of Frobenius modulo prime numbers  $\ell \neq p$ . Having done this for enough small primes  $\ell$ , 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  $\mathbb{Q}_q$  which has an endomorphism ring that is isomorphic to the one of  $E$ , with the isomorphism given by reduction modulo  $p$ . The idea is then to approximate the  $j$ -invariant  $J$  of this canonical lift modulo an appropriate power of  $p$  and afterwards analyzing the action of the  $q$ th 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 an equation  $\psi(J, J^\sigma) = 0$  over  $\mathbb{Q}_q$ , where  $J$  is congruent modulo  $p$  to the  $j$ -invariant of  $E$  and  $\sigma : \mathbb{Q}_q \rightarrow \mathbb{Q}_q$  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 [21] worked in time  $\tilde{\mathcal{O}}(n^3)$  and required  $\mathcal{O}(n^3)$  memory space. After a lot of improvements by Vercauteren [26], the AGM of Mestre [18], Satoh, Skjernaa and Taguchi (SST) [22] and others, a computation time of  $\tilde{\mathcal{O}}(n^{2.5})$  and space  $\mathcal{O}(n^2)$  was achieved. The fastest method however, working for all finite fields of small characteristic, is the patented algorithm of Harley, as described in his e-mail [11]. It requires time  $\tilde{\mathcal{O}}(n^2)$  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  $aX^\sigma + bX + c = 0$  over  $\mathbb{Q}_q$  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 [25].

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

In this paper we describe a new algorithm that has the same complexity as Harley’s result, but is based on a different approach. In [14], Kedlaya gave an algorithm to compute the zeta function of a hyperelliptic curve of genus  $g$  in odd characteristic in time  $\tilde{\mathcal{O}}(g^4 n^3)$  and space  $\mathcal{O}(g^3 n^3)$ . It does not use the canonical lift (for genus one 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 degrees) we can effectively compute in this Monsky-Washnitzer cohomology due to it being isomorphic to the de Rham cohomology of the algebraic lift. Second, by cutting out Weierstrass points, the action of the  $p$ th power Frobenius is readily computable. And third, factoring the  $q$ th power Frobenius in repeated applications of the  $p$ th power Frobenius makes sure that the appearing power series converge good enough. Later on Denef and Vercauteren extended Kedlaya’s method to the technically more challenging case of characteristic 2 in [5].

In [17], Lauder used deformation in order to compute the zeta function of higher dimensional varieties. This works by putting the variety in a well-chosen one parameter family, say with formal parameter  $\Gamma$ , and computing the general matrix  $F(\Gamma)$  of the  $p$ th power Frobenius. As

shown by Dwork in [7] such a matrix satisfies a differential equation, the Picard-Fuchs equation of the deformation, and this equation allows fast recovery of  $F(\Gamma)$  modulo a certain power of  $\Gamma$ . 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  $q$ th power Frobenius yields then the zeta function. In [12] and [13] we followed a suggestion of Denef and Lauder to try to combine such a deformation with Kedlaya's and Denef and Vercauteren's algorithm, which resulted in an  $\tilde{O}(n^{2.667})$  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 put in a good family and that we can reduce the last problem to computing 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 briefly sketch the structure of this paper. In Section 2 we describe how to place a general 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 [12] and [13] allows us to compute the matrix of the  $p$ th power Frobenius for curves in such a family. In addition we explain how to recover an integral matrix of this Frobenius operator, which is not guaranteed by the original algorithms of [12] and [13]. In the fifth section is shown how to compute the trace of the  $q$ th 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.

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 and Wouter Castryck for their comments on an earlier version of this paper.

## 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. We will show in this section how to reduce efficiently the equation of  $E$  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 to the original curve or to its quadratic twist, which we denote by  $\text{Twist}(E)$ . It is well known (and easily proven) that the trace of Frobenius  $t$  of  $E$  equals minus the trace of Frobenius of  $\text{Twist}(E)$ , and hence it suffices to work with  $E'$ . Note that it will be clear in each case which of the two isomorphisms  $E' \cong E$  or  $E' \cong \text{Twist}(E)$  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  $E'$  is an important part of a concrete implementation of the algorithm.

### 2.1 Odd characteristic

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

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

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  $E' \cong \text{Twist}(E)$ .

PROOF. Let  $d$  be a nonsquare in  $\mathbb{F}_q$  if  $b/c \notin (\mathbb{F}_q)^2$ , and  $d := 1$  otherwise. Then there exists  $\lambda \in \mathbb{F}_q$  such that  $\lambda^2 = \frac{b}{cd}$ , and the change of variables  $Y \mapsto \lambda^{-3}Y$ ,  $X \mapsto \lambda^{-2}X$  transforms  $Y^2 = X^3 + bd^2X + cd^3$  into  $Y^2 = X^3 + (b^3/c^2)X + b^3/c^2$ . If  $d$  is a nonsquare the equation  $Y^2 = X^3 + bd^2X + cd^3$  gives precisely the quadratic twist of  $E$ . ■

Now we consider the case  $p = 3$ . If  $a = 0$  in (3)<sup>1</sup>, we can again use Proposition 1, and if  $a \neq 0$  the translation  $X \mapsto X - \frac{b}{2a}$  removes the term with  $X$  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  $E' \cong \text{Twist}(E)$ .

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 in odd characteristic, 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  $\Gamma$  and it suffices to compute the zeta function of  $Y^2 = Q(X, \bar{\gamma})$ . In addition, this can be done very fast. Indeed, the complexity is dominated by verifying whether  $b/c$  (or  $a$ ) is a square in  $\mathbb{F}_q$  and as  $x \in (\mathbb{F}_q)^2$  is equivalent to  $x^{(q-1)/2} = 1$ , this can certainly be done in time  $\tilde{O}(n^2)$  and space  $\mathcal{O}(n)$ . However, in Section 11.3.5 of [3] a much faster algorithm can be found.

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  $\Gamma$  of the resultant  $\text{Res}_X(Q(X, \Gamma); \frac{\partial}{\partial X}Q(X, \Gamma))$  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 second degree resultant. Although this requires the computation of a square root in  $\mathbb{F}_q$ , it might still be advantageous in the end.

## 2.2 Characteristic 2

We now take  $q = 2^n$  and  $E$  a nonsupersingular curve over  $\mathbb{F}_q$  given by

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

The fact that  $E$  is not supersingular is easily seen to be equivalent to  $a \neq 0$ . The translation  $X \mapsto X + b$  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  $Y \mapsto a^3Y$  and  $X \mapsto a^2X$  gives the form

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

as 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  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 0$ . If this trace equals 1 we can take  $\alpha$  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  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 0$ , otherwise we have  $E' \cong \text{Twist}(E)$ . As we did not find a relevant reference, we prove the following lemma that implies that in the second case the sum of the traces of Frobenius of  $E$  and  $E'$  is zero.

<sup>1</sup>All such curves are in fact supersingular because their  $j$ -invariant is zero.

**Lemma 3** *The equations  $Y^2 + XY = X(X^2 + AX + B)$  and  $Y^2 + XY = X(X^2 + B)$ , where  $A, B \in \mathbb{F}_q$  and  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A) = 1$ , have together precisely  $2q$  affine solutions.*

PROOF. We show that for every  $x \in \mathbb{F}_q^\times$  one of the equations has two solutions and the other has none. If  $x = 0$  both have one solution. Choose  $x \in \mathbb{F}_q^\times$ . Replacing  $Y$  by  $xY$  yields as equation  $Y^2 + Y = x + B/x + A$ , which has (two) solutions if and only if  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x + B/x + A) = 0$ . The linearity of the trace concludes the proof.  $\blacksquare$

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

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

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

where  $H(X), Q_f(X, \Gamma) \in \mathbb{F}_2[X, \Gamma]$  and  $\bar{\gamma} \in \mathbb{F}_q$ . In order to get an elliptic curve for  $Y^2 + H(X)Y = H(X)Q_f(X, 0)$  as well, we only have to translate  $\Gamma \mapsto \Gamma + 1$ , as  $Y^2 + XY = X(X^2 + 1)$  does define an elliptic curve. Again, the above transformations can be done very fast in practice. The most time consuming step is computing  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(A)$ , which can certainly be done in time  $\tilde{\mathcal{O}}(n^2)$ . The memory requirements are only  $\mathcal{O}(n)$ .

### 3 $p$ th power Frobenius in odd characteristic

Now that we have put our elliptic curve — up to a twist — in a linear family, we will show how to compute the matrix of the  $p$ th power Frobenius on its Monsky-Washnitzer cohomology. This cohomology was first considered by Kedlaya in [14] in an algorithm to count the number of points on hyperelliptic curves in odd characteristic. We have worked out this deformation approach in great detail in [12] and we will give a short summary in this section, specified to genus 1 and with  $\mathbb{F}_p$  as base field. More details can hence be found in [12].

#### 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  $\bar{\gamma} \in \bar{\mathbb{F}}_p$  is the parameter such that we need the zeta function of  $E : Y^2 = \bar{Q}(X, \bar{\gamma})$  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  $\mathbb{F}_p$ .

**Note 4** The general case can indeed be reduced to this. Suppose that the curve is defined over a bigger field  $\mathbb{F}_{p^m}$  than  $\mathbb{F}_q = \mathbb{F}_{p^n}$ , then [23] shows how to compute the minimal polynomial of  $\bar{\gamma}$  over  $\mathbb{F}_p$  in time  $\tilde{\mathcal{O}}(m^2)$ , with which we can denote  $\mathbb{F}_q$  in the form explained above. Having computed the zeta function over  $\mathbb{F}_q$ , we can use formula (2) 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  $\mathbb{Q}_q$ , a lift of  $x \mapsto x^p$  on  $\mathbb{F}_q$ , is denoted by  $\sigma$ . The valuation on  $\mathbb{Q}_q$  is written as ord, normalized to  $\text{ord}(p) = 1$ .

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

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

then we find that  $\bar{r}(0)$  and  $\bar{r}(\bar{\gamma})$  (where  $\bar{\cdot}$  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  $\rho'$  be the largest index  $i$  such that  $\text{ord}(r_i) = 0$ . 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  $R(\Gamma) \equiv r(\Gamma) \pmod{p}$ . Define the ring  $S := \mathbb{Q}_p[\Gamma, 1/R(\Gamma)]^\dagger$ , where  $\dagger$  denotes the overconvergent completion, and the  $S$ -module

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

On  $T$  act two differential operators, namely  $d : T \rightarrow TdX : v \mapsto \frac{\partial v}{\partial X} dX$  and the connection  $\nabla : T \rightarrow Td\Gamma : v \mapsto \frac{\partial v}{\partial \Gamma} d\Gamma$  satisfying  $\nabla X = 0$ . The submodule  $H_{MW}^-$  of  $TdX/dT$  is defined as the eigenspace corresponding to the eigenvalue  $-1$  under the elliptic involution and is a free  $S$ -module of rank 2. With  $F_p$  the  $p$ th power Frobenius map on  $H_{MW}^-$ , we find the following commutative diagram:

$$\begin{array}{ccc} H_{MW}^- & \xrightarrow{\nabla} & H_{MW}^- d\Gamma \\ \downarrow F_p & & \downarrow F_p \\ H_{MW}^- & \xrightarrow{\nabla} & H_{MW}^- d\Gamma. \end{array} \quad (4)$$

The basis used in [12] for  $H_{MW}^-$  is the pair  $\{dX/\sqrt{Q}, XdX/\sqrt{Q}\}$ , and the diagram (4) gives the differential equation

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

for the matrix  $F(\Gamma)$  of  $F_p$  with respect to this basis. Here  $G(\Gamma)$  is the matrix of the connection  $\nabla$ . Let  $\gamma$  be the Teichmüller lift of  $\bar{\gamma}$  in  $\mathbb{Z}_q$ , then the matrix  $F(\gamma)$  is precisely the matrix of the  $p$ th power Frobenius on the Monsky-Washnitzer cohomology as found by Kedlaya in [14].

## 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 [12] 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 integral, which is a priori only guaranteed with our chosen basis if  $p > 3$  (see [15, Section 3.5]). Two possible solutions emerge. We can imitate the proofs of [12], but now with the basis  $\{dX/\sqrt{Q^3}, XdX/\sqrt{Q^3}\}$ , which does give an integral matrix, see [15]. The complexity estimates will all remain the same in this case; this is the solution used in the implementation 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 multiplying with  $p$  and is easily retrieved using Kedlaya's reduction algorithm of [14]. Transforming  $F(\gamma)$  using this matrix yields then an integral version of  $F(\gamma)$ .

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 simply that both polynomials are equal 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  $\gamma$  of  $\bar{\gamma}$ . In [3, Section 12.1.2] a very efficient algorithm for computing  $\varphi(x)$  is given, originally due to Harley, that computes  $\varphi(x)$  modulo  $p^n$  in time  $\tilde{\mathcal{O}}(n^2)$  and space  $\mathcal{O}(n^2)$ .

## 4 2nd power Frobenius in characteristic 2

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

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

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 in [5] how to do this in time  $\tilde{\mathcal{O}}(n^3)$  and space  $\mathcal{O}(n^3)$ , and in [13] 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 [13].

## 4.1 Computing the matrix of Frobenius

We suppose as in the previous section that  $\mathbb{F}_q$  is given by  $\mathbb{F}_2[x]$  divided out by the minimal polynomial of  $\bar{\gamma}$ . Define  $\mathbb{Q}_2, \mathbb{Q}_q, \mathbb{Z}_2, \mathbb{Z}_q$  and  $\sigma$  as before and let  $H(X) := X$  and  $Q_f(X, \Gamma) := X^2 + \Gamma + 1$ . The polynomial  $c(\Gamma)$  from [13] is just equal to 1 in our case. The resultant needed is  $r(\Gamma) = \text{Res}_X(H; Q_f \frac{\partial}{\partial X} H) = \Gamma + 1$  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  $S$  is defined by  $S := \mathbb{Q}_2[\Gamma, 1/(\Gamma + 1)]^\dagger$  and the  $S$ -module  $T$  by

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

Using the definitions of  $d, \nabla, H_{MW}^-$  as before we find again diagram (4), with  $\mathcal{B} := \{YdX, XYdX\}$  as basis for  $H_{MW}^-$ . Here too we get  $F(\gamma)$ , using the Teichmüller modulus representation of  $\mathbb{Q}_q$ , with precision  $N = \mathcal{O}(n)$ . However, in order to get an integral matrix our chosen basis does not suffice, indeed, from the proof of Proposition 11 from [13] follows that only  $2^6 \cdot F(\gamma)$  is guaranteed to be integral. We will show in the next subsection how to solve this problem. The conclusion will be that we have to compute  $F(\gamma)$  modulo  $2^{N+13}$ , and can transform it afterwards into a matrix of Frobenius modulo  $2^N$  with integral coefficients. As follows from the algorithm of [13], we can find this approximation of  $F(\gamma)$  in time  $\tilde{\mathcal{O}}(n^2)$  and space  $\mathcal{O}(n^2)$ .

We would like to mention that in [10] Gerkmann 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  $q$ th power Frobenius map are the reciprocal zeroes of the numerator of the zeta function, and hence integral. This implies that a  $\mathbb{Z}_q$ -submodule of  $H_{MW}^-$  does exist that is stable under this map. In [8, Proposition 5.3.1], Edixhoven showed how to find a basis for this submodule and in [4] Denef and Vercauteren applied this to their characteristic 2 situation. It turns out that  $\mathcal{D} := \left\{ \frac{dX}{2Y+X}, \frac{XdX}{2Y+X} \right\}$  is such an ‘integral basis’. It might be possible to reconstruct the algorithm explained above using this basis, but here 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 [4], specialized to our situation. The modules  $H_1$  and  $H_1^-$  are as defined in Denef and Vercauteren’s paper [5], essentially they are the modules  $TdX/dT$  and  $H_{MW}^-$  above 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  $E \setminus \{P_\infty\}$  is affine, with  $P_\infty$  the point at infinity of  $E$ . Let  $D = kP_\infty$  be a divisor on  $E$  with  $k \geq 2$ . We define the  $\mathbb{Z}_q$ -module  $L$  as consisting of those differentials  $\omega$  on  $E \setminus \{P_\infty\}$  satisfying the following two conditions. First, we require that  $\text{div}(\omega) + D \geq 0$ , and second, each term with valuation less than  $-1$  in the local expansion of  $\omega$  at  $P_\infty$  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  $p$ th power Frobenius, and  $L$  generates  $H_1$ . Hence we have also that  $L \cap H_1^-$  generates  $H_1^-$ , and  $\mathcal{D}$  will be a basis for  $L \cap H_1^-$  as  $\mathbb{Z}_q$ -module.

First we need a lower bound on the valuation of the matrix of change of basis and its inverse. The differential forms  $YdX$  and  $XYdX$  from  $\mathcal{B}$  have a pole of order 6 respectively 8 at the point

$P_\infty$ . If we take  $D = 8P_\infty$ , both forms satisfy the condition  $\text{div}(\omega) + D \geq 0$ , and  $4\omega$  for  $\omega \in \mathcal{B}$  will also satisfy the second condition on the integrability. Indeed, during integration only  $-7, \dots, -1$  can appear as denominators, and 4 divided by one of these is always integral in  $\mathbb{Z}_2$ . This implies that both  $4YdX$  and  $4XYdX$  are in the  $\mathbb{Z}_q$ -module  $L$ , 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 the Lemmata 2 and 3 of [5]. As

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

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

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

Computing this last matrix, denoted with  $B$ , modulo  $2^M$  with  $M = \mathcal{O}(n)$  is easy using the reduction formulae in [5], but this would require time  $\tilde{\mathcal{O}}(n^3)$ . We can see however that we do not need  $B$  modulo such high 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  $B' \equiv B \pmod{2^\alpha}$  for some  $\alpha$ , then if  $(B'^{-1})^\sigma$  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 [5] allows us to compute  $B'$  in time  $\tilde{\mathcal{O}}(n^2)$  and space  $\mathcal{O}(n^2)$ .

From the valuation bound  $-2$  on  $B^{-1}$  above we see that  $\text{ord}(\det B)$  is not larger than 4, and hence working with  $\alpha \geq 5$  suffices already to be able to invert  $B'$  (which has to be done to the full precision  $2^{N+13}$ ). It is not hard to verify that  $B'^{-1} \equiv B^{-1} \pmod{2^{\alpha-4}}$ . 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  $\alpha := 13 = \mathcal{O}(1)$  suffices. The loss in precision in this product is at most  $2+6+4 \leq 13$ , hence we have to compute  $F(\gamma)$  modulo  $2^{N+13}$ .

## 5 An eigenvalue of the $q$ th power Frobenius

In this section we will first show that it suffices to compute an approximation of an eigenvalue of the matrix of the  $q$ th power Frobenius, and we reduce this to computing an ‘eigenvalue’ of  $F(\gamma)$ , in fact an eigenvalue of the  $\sigma$ -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 curve over  $\mathbb{F}_q$ , where  $q = p^n$ , and  $F = F(\gamma)$  is the matrix of the  $p$ th power Frobenius on its Monsky-Washnitzer cohomology over  $\mathbb{Q}_q$ , as explained in the two previous sections. For

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

the matrix of the  $q$ th power Frobenius, Kedlaya [14] and Denef and Vercauteren [5] showed that we have, with  $Z(T)$  the zeta function of  $E$  over  $\mathbb{F}_q$ ,

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

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

$$N := \lceil \log_p(4\sqrt{q}) \rceil = \lceil n/2 + \log_p(4) \rceil = \mathcal{O}(n), \quad (6)$$

which is smaller than  $n$  if  $n$  is not too small. To conclude, it suffices to compute  $\lambda_1$  modulo  $p^N$  in order to find the zeta function of  $E$ : the trace  $t$  is then the unique integer congruent to  $\lambda_1$  modulo  $p^N$  that satisfies  $|t| < 2\sqrt{q}$ .

If we have matrices  $C$  and  $D$  over  $\mathbb{Z}_q$  such that  $F = C^\sigma DC^{-1}$  with  $D$  in uppertriangular 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  $\mu$  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  $\mu$  with valuation 0 can always be found efficiently if  $E$  is not supersingular. It is easily seen that a factorization  $F = C^\sigma DC^{-1}$  over  $\mathbb{Q}_q$  cannot exist if the curve is supersingular: the product of the two diagonal elements has valuation one, and their sum has then valuation at least one. This is clearly impossible as the valuation is a map from  $\mathbb{Q}_q$  to the integers.

Having found  $\mu$  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 Teichmüller modulus, and  $\mu(x) \in \mathbb{Z}_p[x]/\varphi(x)$ , then

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

A complete description of the algorithm has been given by Vercauteren and can be found in [25, Section 3.10.3]. It requires  $\tilde{\mathcal{O}}(n^2)$  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’ $\mu$ 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 [3]. Note that this algorithm requires  $\mathbb{Z}_q$  to be given as  $\mathbb{Z}_p[x]$  modulo a Teichmüller modulus.

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

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

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

$$\psi(\alpha, \alpha^\sigma) \equiv 0 \pmod{p^N}, \quad \alpha \equiv x_0.$$

Following the complexity estimates found in [3], it is easily shown that if the degree of  $\psi$  is fixed, the algorithm runs in time  $\tilde{\mathcal{O}}(nN)$  and space  $\mathcal{O}(nN)$ .

<sup>2</sup>In fact, the Hasse-Weil bound shows that  $|t| \leq 2\sqrt{q}$ , but equality can only occur for supersingular curves.

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

$$\begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \mu \begin{pmatrix} 1 \\ \alpha^\sigma \end{pmatrix}, \quad \text{or} \quad \begin{cases} f_1 + \alpha f_2 = \mu, \\ f_3 + \alpha f_4 = \mu \alpha^\sigma. \end{cases} \quad (7)$$

It is clear that if we can find a solution  $(\alpha, \mu) \in \mathbb{Z}_q \times \mathbb{Z}_q^\times$  for (7), this yields a factorization of  $F = (C^\sigma)DC^{-1}$ , which is of the kind that we are looking for. Here  $C$  and  $D$  can e.g. be taken as

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

Eliminating  $\mu$  from the system of equations (7) gives

$$\alpha(\alpha^\sigma f_2 - f_4) + (\alpha^\sigma f_1 - f_3) = 0. \quad (8)$$

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

$$x_0^\sigma := \begin{pmatrix} f_4 \bmod p \\ f_2 \bmod p \end{pmatrix}, \quad \text{or} \quad x_0^\sigma := \begin{pmatrix} f_3 \bmod p \\ f_1 \bmod p \end{pmatrix}.$$

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

$$\psi(X, Y) := X(Y f_2 - f_4) + (Y f_1 - f_3) \in \mathbb{Z}_q[X, Y].$$

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

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

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  $\mu$ , both with precision  $N = \mathcal{O}(n)$ , in time  $\tilde{\mathcal{O}}(n^2)$  and  $\mathcal{O}(n^2)$ . Indeed, if we denote with  $\beta \in \mathbb{Z}_q$  the exact solution of  $\psi(\beta, \beta^\sigma) = 0$  and  $\beta \equiv x_0$ , then we can write  $\alpha = \beta + \beta'$  with  $\beta' \equiv 0$  and it is not hard to verify that then actually  $\beta' \equiv 0 \pmod{p^N}$ . This implies that  $\alpha$  is indeed computed with precision  $N$ . In addition, eliminating  $\alpha$  from (7) 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  $\text{ord}(\mu) > 0$  as well, whence  $\mu \in \mathbb{Z}_q^\times$ .

Suppose that  $\frac{\partial}{\partial Y} \psi(x_0, x_0^\sigma) = x_0 f_2 + f_1 \equiv 0$ . 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

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

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

## 6 Conclusion and implementation results

Combining all steps explained in Sections 2, 3, 4 and 5 above, we have found a deterministic algorithm that for every elliptic curve over  $\mathbb{F}_{p^n}$  given by its Weierstrass equation, can compute its zeta function in time  $\tilde{\mathcal{O}}(n^2)$  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  $H_{MW}^-$ . We do not mention in the algorithm that we only compute *approximations* of the objects involved. If  $p^n$  is so small that  $N > n$  in (6), we can use a naive point counting algorithm.

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

**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  $Y^2 = Q(X, \bar{\gamma})$ , where  $\bar{\gamma} \in \mathbb{F}_{p^n}$ , as explained in Section 2. In particular,  $Q(X, \Gamma) \in \mathbb{F}_p[X, \Gamma]$ .

**STEP 2:** Compute the matrix of Frobenius  $F(0)$  of the curve defined by  $Y^2 = Q(X, 0)$  and determine the differential equation for  $F(\Gamma)$ .

**STEP 3:** Solve the differential equation and find  $F(\Gamma) \in \mathbb{Z}_p[[\Gamma]]^{2 \times 2}$ .

**STEP 4:** Determine  $\bar{\varphi}(x) \in \mathbb{F}_p[x]$ , the minimal polynomial of  $\bar{\gamma}$ , and define  $\mathbb{F}_{p^m} := \mathbb{F}_p[x]/\bar{\varphi}(x)$ . 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 5:** Compute  $F(\gamma)$  by reducing  $F(\Gamma)$  modulo  $\varphi(\Gamma)$ .

**STEP 6:** Compute a solution  $(\alpha, \mu)$  with  $\text{ord}(\mu) = 0$  for one of the equations

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

**STEP 7:** Compute  $t_1 \equiv \mathcal{N}_{\mathbb{Q}_{p^m}/\mathbb{Q}_p}(\mu)$  modulo an appropriate power of  $p$ , such that  $|t_1| < 2\sqrt{p^m}$ . Compute then the resultant

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

**STEP 8:** Return

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

We have implemented this algorithm in odd characteristic and present a few timing results obtained with it. We note that we do *not* use Harley’s  $\tilde{\mathcal{O}}(n^2)$  norm algorithm for Step 7, but instead the — far easier to implement and in practice probably faster for reasonable  $n$  — algorithm of Satoh, Skjernaas and Taguchi [22]. This method runs in time  $\tilde{\mathcal{O}}(n^{2.5})$  given some precomputations. These precomputations require time  $\tilde{\mathcal{O}}(n^3)$ , 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  $\tilde{\mathcal{O}}(n^3)$ . In Step 2 the matrix  $F(0)$  is computed using an implementation of Kedlaya’s algorithm by Michael Harrison.

The implementation has been made in the computational algebra system Magma V2.13-10, and the timing results were obtained on an AMD Athlon 64 3000+, using 1GB of physical memory. The algorithm received as input a random elliptic curve over  $\mathbb{F}_{p^n}$ , given by its Weierstrass equation. All times in the following table are in seconds.

$p \setminus n$	50	100	250	500	1000	2000	4000
3	.18	.50	2.55	10.05	46	229	1246
5	.58	1.38	6.48	27.08	117	610	-
7	2.16	5.51	34.13	156.21	800	4454	-

It is interesting to see that for  $n \gg 0$  almost all computation time goes to Steps 6, 7 and the computation of the Teichmüller modulus in Step 4, the first two being comparable in required time. E.g. for  $p^n = 3^{4000}$  we have as total time 1246 seconds, where Step 6 uses 411 seconds and Step 7 uses 683 seconds. For  $p^n = 7^{2000}$  the computation of  $\varphi(x)$  takes 3913 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 6 but with an equation  $\psi$  of higher degree, and exactly the same field polynomial and norm computation.

Steps 2 and 3 can be considered as precomputation, meaning that they depend only on the field size (and the structure of the family in which the curve lives). For  $n$  big enough these steps are 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 these times for the field sizes as above, hence ignoring the time for Steps 2 and 3 of the algorithm.

$p \setminus n$	50	100	250	500	1000	2000	4000
3	.10	.35	2.10	9.03	43	221	1221
5	.25	.77	4.99	23.36	109	587	-
7	1.67	4.60	31.81	150.82	787	4415	-

## References

- [1] BERNSTEIN, D. J. Fast multiplication and its applications. URL: <http://cr.yp.to/papers.html#multapps>. To appear in Buhler-Stevenhagen's *Algorithmic number theory*.
- [2] BIRCH, B. J., AND SWINNERTON-DYER, H. P. F. Notes on elliptic curves. II. *J. Reine Angew. Math.* 218 (1965), 79–108.
- [3] COHEN, H., FREY, G., AVANZI, R., DOCHE, C., LANGE, T., NGUYEN, K., AND VERCAUTEREN, F., Eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [4] DENEFF, J., AND VERCAUTEREN, F. Errata for “An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2”, and related papers. Available on [http://www.wis.kuleuven.be/algebra/denef\\_papers/ErrataPointCounting.pdf](http://www.wis.kuleuven.be/algebra/denef_papers/ErrataPointCounting.pdf).
- [5] DENEFF, J., AND VERCAUTEREN, F. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology* 19, 1 (2006), 1–25. Erratum available as [4].
- [6] DIFFIE, W., AND HELLMAN, M. E. New directions in cryptography. vol. IT-22. 1976, pp. 644–654.
- [7] DWORK, B. A deformation theory for the zeta function of a hypersurface. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. Inst. Mittag-Leffler, Djursholm, 1963, pp. 247–259.
- [8] EDIXHOVEN, B. *Point counting after Kedlaya*. EIDMA-Stieltjes Graduate course, Leiden, September 2003.
- [9] ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, vol. 196 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1985, pp. 10–18.

- [10] GERKMANN, R. Relative rigid cohomology and point counting on families of elliptic curves. Preprint, available on <http://www.mathematik.uni-mainz.de/~gerkmann/>.
- [11] HARLEY, R. Asymptotically optimal  $p$ -adic point-counting. E-mail to NMBRTHRY list.
- [12] HUBRECHTS, H. Point counting in families of hyperelliptic curves. To appear in Foundations of Computational Mathematics.
- [13] HUBRECHTS, H. Point counting in families of hyperelliptic curves in characteristic 2. Submitted, available on <http://wis.kuleuven.be/algebra/hubrechts/>.
- [14] KEDLAYA, K. S. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.* 16, 4 (2001), 323–338.
- [15] KEDLAYA, K. S. Computing zeta functions via  $p$ -adic cohomology. In *Algorithmic number theory*, vol. 3076 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2004, pp. 1–17.
- [16] KOBLITZ, N. Elliptic curve cryptosystems. *Math. Comp.* 48, 177 (1987), 203–209.
- [17] LAUDER, A. G. B. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc.* (3) 88, 3 (2004), 565–602.
- [18] MESTRE, J.-F. Lettre adressée à Gaudry et Harley. Available on <http://www.math.jussieu.fr/~mestre/>.
- [19] MILLENIUM PRIZE PROBLEMS. <http://www.claymath.org/millennium/>.
- [20] MILLER, V. S. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, vol. 218 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1986, pp. 417–426.
- [21] SATOH, T. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* 15, 4 (2000), 247–270.
- [22] SATOH, T., SKJERNAA, B., AND TAGUCHI, Y. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields Appl.* 9, 1 (2003), 89–101.
- [23] SHOUP, V. Efficient Computation of Minimal Polynomials in Algebraic Extension of Finite Fields. *Proc. 1999 International Symposium on Symbolic and Algebraic Computation.*
- [24] SILVERMAN, J. H. *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
- [25] VERCAUTEREN, F. *Computing zeta functions of curves over finite fields.* PhD thesis, KULeuven, Belgium, 2003.
- [26] VERCAUTEREN, F., PRENEEL, B., AND VANDEWALLE, J. A memory efficient version of Satoh's algorithm. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, vol. 2045 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2001, pp. 1–13.
- [27] VON ZUR GATHEN, J., AND GERHARD, J. *Modern computer algebra.* Cambridge University Press, Cambridge, 2003.
- [28] WATERHOUSE, W. C. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.* (4) 2 (1969), 521–560.