UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

A GENERAL FRAMEWORK FOR p-ADIC POINT COUNTING AND APPLICATION TO ELLIPTIC CURVES ON LEGENDRE FORM

By Marc Skov Madsen

Preprint Series No.: 2

January 2004

Ny Munkegade, Bldg. 530
DK-8000 Aarhus C, Denmark

http://www.imf.au.dk
institut@imf.au.dk

A General Framework for *p*–adic Point Counting and Application to Elliptic Curves on Legendre Form

Marc Skov Madsen

January 12, 2004

Abstract

In 2000 T. Satoh gave the first *p–adic point counting* algorithm for elliptic curves over finite fields. *Satoh's algorithm* was followed by the *SST* algorithm and furthermore by the *AGM* and *MSST* algorithms for characteristic two only. All four algorithms are important to *Elliptic Curve Cryptography*.

In this paper we present a general framework for *p*–adic point counting and we apply it to *elliptic curves on Legendre form*. We show how the λ–*modular polynomial* can be used for lifting the curve and Frobenius isogeny to characteristic zero and we show how the associated *multiplier* gives the action of the lifted *Frobenius* isogeny on the invariant differential. The result is a point counting algorithm which is simpler and more practical than known algorithms for general elliptic curves. The algorithm extends the MSST algorithm to odd characteristics.

Keywords: Point Counting, Elliptic Curves, Legendre Form, Cryptography, λ–modular form.

Thanks: J.P. Hansen, N. Lauritzen, P. Gaudry, T. Satoh, B. Skjernaa.

1 Introduction

In 2000 T. Satoh gave the first *p*–adic point counting algorithm for ordinary elliptic curves over finite fields of characteristic at least five ([16]). *Satoh's Algorithm* was soon extended to characteristic two and three ([22, 5, 4]). Later Satoh's algorithm was improved by T. Satoh, B. Skjernaa and Y. Taguchi (*SST*, [18, 17]). Motivated by applications to cryptography the characteristic two case has been intensely studied and improved. This has resulted in the Arithmetic–Geometric Mean algorithm (*AGM*, [8, 15]) and Modified SST algorithm (*MSST*, [6]).

In this paper we give a presentation of the basic framework by which *p*–adic point counting algorithms can be explained. A *p*–adic point counting algorithm consists of two parts: A *lifting part* where the elliptic curve and *p*'th power Frobenius isogeny is lifted to characteristic zero and a *norm part* where trace of the *q*'th power Frobenius isogeny and the number of points on the curve is determined by a norm computation. The input to the norm computation is the action of the lifted Frobenius on the invariant differential.

We apply the basic framework for *p*–adic point counting to ordinary *elliptic curves on Legendre form*, i.e. elliptic curves on the form $\overline{E}_{\overline{\lambda}}/\mathbf{F}_q : y^2 = x(x-1)(x-\overline{\lambda})$. We find that the lifting part can be done using the λ–*modular polynomial*. Furthermore we find that the norm part is especially simple because the action of the lifted p'th power Frobenius isogeny on the invariant differential is given by the associated *multiplier*.

The resulting p–adic point counting algorithm for Legendre elliptic curves is simpler and more practical in odd characteristic than known algorithms for general elliptic curves. The algorithm may be seen as extending the MSST algorithm to odd characteristics. We include examples and data from experiments in characteristic two to nineteen.

Keywords: p–adic point counting, Elliptic Curves, Legendre Form, λ–modular form, λ–Modular Polynomial, Elliptic Curve Cryptography, Satoh's algorithm, AGM, SST, MSST.

The paper is organized as follows.

Contents

2 Background Material

This section contains the basic framework for p–adic point counting, Elliptic curves on Legendre form and the λ–modular polynomial. We assume that the reader is familiar with elliptic curves at least to the level of Silverman's book ([20, p.1-188]). We also assume the reader is familiar with the p–adic numbers and unramified extensions (See Appendix A.1, [14] or [5]).

In the following p will denote a prime and $\mathbf{F}_q$ the finite field with $q = p^n$ elements. We let $\mathbf{Q}_p$ denote the p–adic numbers and $\mathbf{Z}_p$ the ring of p–adic integers. We let $\mathbf{Q}_q$ denote an unramified field extension of $\mathbf{Q}_p$ of degree n and $\mathbf{Z}_q$ the associated ring of integers.

Elements of $\mathbf{Z}_q$ can be approximated by elements of $\mathbf{Z}_q/p^i\mathbf{Z}_q$. The precision of the approximation is given by i. As i grows the approximation improves. The elements of $\mathbf{Z}_q/p^i\mathbf{Z}_q$ can be represented by polynomials of degree at most $n-1$ with coefficients in $\mathbf{Z}/p^i\mathbf{Z}$. This means that the p–adic integers are very practical for calculations on a computer.

The surjective *reduction modulo p* morphism $\mathbf{Z}_q \to \mathbf{F}_q$ with kernel $p\mathbf{Z}_q$ links characteristic 0 and characteristic p. If $x \in \mathbf{Z}_q$ maps to $\overline{x} \in \mathbf{F}_q$ then $\overline{x}$ is called the *reduction* modulo p of x and x is called a *lift* of $\overline{x}$. We can lift other objects from characteristic p to to characteristic 0 as well: The p'th power Frobenius map $\overline{\Sigma} : \mathbf{F}_q \to \mathbf{F}_q$ can be lifted to the *Frobenius Substitution* $\Sigma : \mathbf{Q}_q \to \mathbf{Q}_q$. The Frobenius Substitution Σ is the unique element in the Galois group $\mathrm{Gal}_{\mathbf{Q}_q/\mathbf{Q}_p}$ satisfying

$$\Sigma(x) \equiv x^p \mod p$$

for all $x \in \mathbf{Z}_q$.

2.1 The Basic Framework for p–adic Point Counting

In this section we present the basic framework by which the p–adic point counting algorithms can be understood.

Let $\overline{E}/\mathbf{F}_q$ denote an ordinary elliptic curve, i.e. an elliptic curve with non–trivial p–torsion subgroup. Let $\overline{\mathrm{Fr}}_q : \overline{E} \to \overline{E}$ the q'th power Frobenius isogeny. We define the trace of the q'th power Frobenius isogeny by

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \overline{\mathrm{Fr}}_q + \widehat{\overline{\mathrm{Fr}}_q}$$

where $\widehat{\overline{\mathrm{Fr}}_q}$ is the dual of $\overline{\mathrm{Fr}}_q$. The trace is in fact an integer. The number of $\mathbf{F}_q$–rational points on the elliptic curve is related to the trace by

$$\#\overline{E}(\mathbf{F}_q) = q + 1 - \mathrm{Tr}(\overline{\mathrm{Fr}}_q). \tag{1}$$

So it is enough for point counting to determine the trace. This can be done using the invariant differential.

Let $\overline{\omega}$ denote the invariant differential on $\overline{E}$. We see that

$$\overline{\mathrm{Fr}}_q^*(\overline{\omega}) + \widehat{\overline{\mathrm{Fr}}_q}^*(\overline{\omega}) = (\overline{\mathrm{Fr}}_q + \widehat{\overline{\mathrm{Fr}}_q})^*(\overline{\omega}) = \mathrm{Tr}(\overline{\mathrm{Fr}}_q)\overline{\omega}.$$

Thus the action of the q'th power Frobenius and its dual on the invariant differential leads to information on the trace, but only modulo p since we are working in characteristic p. To overcome this difficulty we lift the situation to characteristic 0.

In practice we lift the p'th power Frobenius isogeny $\overline{\mathrm{Fr}}_p : \overline{E} \to \overline{\Sigma E}$ to the unramified extension $\mathbf{Q}_q$ of the p–adic numbers $\mathbf{Q}_p$[1]. Then we use the following Theorem.

Theorem 2.1 *Let $\overline{E}/\mathbf{F}_q$ denote an ordinary elliptic curve, $\overline{\mathrm{Fr}}_p : \overline{E} \to \overline{\Sigma E}$ the p'th power Frobenius isogeny and $\overline{\mathrm{Fr}}_q : \overline{E} \to \overline{E}$ the q'th power Frobenius isogeny. Assume $E/\mathbf{Q}_q$ is an elliptic curve reducing to $\overline{E}/\mathbf{F}_q$ modulo p and that $\mathrm{Fr}_p : E \to \Sigma E$ is an isogeny defined over $\mathbf{Q}_q$ and reducing to $\overline{\mathrm{Fr}}_p$ modulo p. Let ω denote the invariant differentials on E. Note that ω^Σ is the invariant differential on ΣE.*

There is a unique $M \in \mathbf{Q}_q$ satisfying

$$\mathrm{Fr}_p^*(\omega^\Sigma) = \frac{1}{M}\omega.$$

[1] Since $\overline{E}$ is ordinary the lift of the p'th power Frobenius isogeny exists and is unique up to isomorphism over $\mathbf{Q}_q$ (Theory of *canonical lift* [12, 13]). How this lift is found in practice is the content of the algorithms by Satoh, Skjernaa, Gaudry, Harley and Vercauteren.

Furthermore $pM \in \mathbf{Z}_q^*$ *and the action of* $\widehat{\mathrm{Fr}_p}$ *on the invariant differential* ω *is given by*

$$\widehat{\mathrm{Fr}_p}^*(\omega) = (pM)\omega^{\Sigma}.$$

Finally the trace of the q'th power Frobenius isogeny is given by

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(\frac{1}{M}) + \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(pM)$$

where $\mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p} : \mathbf{Q}_q \to \mathbf{Q}_p$ *denotes the norm.*

PROOF Appendix A.2.

The result is an integer. The formulation and proof of Theorem 2.1 is due to the author. The idea to use the norm computation was first described in the paper [18] by T.Satoh, B. Skjernaa and Y. Taguchi.

A p–adic point counting algorithm based on the above Theorem can be divided into two parts. A *lifting* part where the p'th power Frobenius isogeny is lifted to characteristic zero and a *norm part* where the trace of the q'th power Frobenius isogeny is determined by a norm computation.

We will be needing the following Lemma by Skjernaa [22] for the lifting part of our algorithm.

Lemma 2.2 *Let* $\overline{E}/\mathbf{F}_q$ *be an elliptic curve with* $j(\overline{E}) \notin \mathbf{F}_{p^2}$. *Assume that* $E/\mathbf{Q}_q$ *and* $E'/\mathbf{Q}_q$ *are elliptic curves reducing to* $\overline{E}$ *and* $\overline{\Sigma E}$ *modulo p. Assume furthermore that there exists a p-isogeny* $E \to E'$ *defined over* $\mathbf{Q}_q$. *Then the p–isogeny reduces to* ± *the p'th power Frobenius isogeny* $\overline{E} \to \overline{\Sigma E}$ *modulo p.*

2.2 Legendre Elliptic Curves

We begin this section by restating a definition and a Proposition from Silverman [20, p. 53-55].

Definition 2.3 *A Weierstrass equation is in* Legendre form *if it can be written as*

$$y^2 = x(x-1)(x-\lambda)$$

We note that a Weierstrass equation in characteristic two is not smooth. Thus an elliptic curve on Legendre form is always defined over a field of odd or zero characteristics. We also note that [20, Theorem V.4.1] gives an easy way to determine if an elliptic curve on Legendre form is ordinary.

Let $\mathbf{F}$ denote a field with $\mathrm{char}(\mathbf{F}) \neq 2$.

Proposition 2.4 *Two elliptic curves* $E_\lambda/\mathbf{F} : y^2 = x(x-1)(x-\lambda)$ *and* $E_\mu/\mathbf{F} : y^2 = x(x-1)(x-\mu)$ *on Legendre form are isomorphic over the algebraic closure* $\overline{\mathbf{F}}$ *of* $\mathbf{F}$ *if and only if*

$$\lambda \in \{\mu, \frac{1}{\mu}, 1-\mu, \frac{1}{1-\mu}, \frac{\mu}{\mu-1}, \frac{\mu-1}{\mu}\}$$

Elliptic curves on Legendre form over finite fields have recently been studied in the paper [2] by Auer and Top. We will be using the following Lemma extracted from the proof of [2, Prop.2.2]..

Lemma 2.5 *Assume* $\overline{E}_{\overline{\lambda}}/\mathbf{F}_q : y^2 = x(x-1)(x-\overline{\lambda})$ *is an elliptic curve on Legendre form. Then* $j(\overline{E}_{\overline{\lambda}}) \in \mathbf{F}_{p^2}$ *if and only if* $\overline{\lambda} \in \mathbf{F}_{p^2}$.

2.3 The λ–modular polynomial

In this section we use the concept of *modular forms* to justify the existence and properties of the λ–modular polynomial Ω_p. For an introduction to modular forms see Lang [10] or Schoeneberg [19].

It is well known that to every lattice in the complex plane there is an associated elliptic curve on Weierstrass form (Silverman [20, Chapter VI]). An elliptic curve on Weierstrass form can obviously be brought onto Legendre form by moving its 2–torsion points using some fixed algorithm (Silverman [20, Prop III.1.7]). So to every τ in the upper complex half plane $\mathbf{H}$ we have a lattice $\mathbf{Z}+\tau\mathbf{Z}$ in the complex plane and an associated elliptic curve $E_{\lambda(\tau)} : y^2 = x(x-1)(x-\lambda(\tau))$ on Legendre form. Thus we have just defined a function $\lambda : \mathbf{H} \to \mathbf{C}$. This function is rigorously defined and studied in [1, p.277-282] and [3, Chapter 4]. It is shown that λ is a modular form for the congruence subgroup modulo two.

Let p denote a fixed odd prime. Define $\mu : \mathbf{H} \to \mathbf{C}$ by $\mu(\tau) = \lambda(p\tau)$. Using the theory of Riemann Surfaces it can be shown that there exists a unique, monic and irreducible polynomial $\Omega_p(X,Y) \in \mathbf{C}(X)[Y]$ with (λ,μ) as root, i.e.

$$\Omega_p(\lambda,\mu) = 0.$$

Furthermore it can be shown that Ω_p is a symmetric polynomial in X and Y with integer coefficients. The polynomial Ω_p has degree $p+1$ in each variable and it satisfies the *Kronecker relation*

$$\Omega_p(X,Y) \equiv (X-Y^p)(X^p-Y) \mod p \tag{2}$$

We call Ω_p the λ*–modular polynomial*.

The λ–modular polynomial Ω_p can be calculated in practice for "small" values of p. See [3, p.133] for a discussion of this. F.ex.

$$\Omega_3(X,Y) \quad = \quad (Y-X)^4 - 128YX(1-Y)(1-X)(2-Y-X+2YX)$$

We will need the fact that the set of p–isogenies between elliptic curves on Legendre form (modulo isomorphism) is the affine curve given by the λ–modular polynomial Ω_p. We state this as a Theorem.

Theorem 2.6 *Let $E_\mu/\mathbf{C} : y^2 = x(x-1)(x-\mu)$ and $E_\lambda/\mathbf{C} : y^2 = x(x-1)(x-\lambda)$ be elliptic curves on Legendre form.*

There exists a p–isogeny $\psi_p : E_\mu \to E_\lambda$ if and only if the set $\{\mu, \frac{1}{\mu}, 1-\mu, \frac{1}{1-\mu}, \frac{\mu}{\mu-1}, \frac{\mu-1}{\mu}\}$ contains a root of the equation

$$\Omega_p(X,\lambda) = 0 \tag{3}$$

If μ is a root then there is an isogeny $\psi_p : E_\mu \to E_\lambda$ defined over $\mathbf{Q}(\lambda,\mu)$.

PROOF (cf. [3, Chapter 4]).

So far the above definitions and properties are analogous to the theory of the modular form j and the j–modular polynomial Φ_p used in Satoh's algorithm. Now we state a Lemma that, as far as the author knows, has no analogue when dealing with j and Φ_p.

Lemma 2.7 *Let $E_\mu/\mathbf{C} : y^2 = x(x-1)(x-\mu)$ and $E_\lambda/\mathbf{C} : y^2 = x(x-1)(x-\lambda)$ be elliptic curves on Legendre form with $\Omega_p(\mu,\lambda) = 0$. Let $\psi_p : E_\mu \to E_\lambda$ denote a p–isogeny as in Theorem 2.6. Let ω_μ (resp. ω_λ) denote the invariant differential on E_μ (resp. E_λ).*

The action of ψ_p *on the invariant differential is given by*

$$\psi_p^*(\omega_\mu) = \frac{1}{M_p}\omega_\lambda$$

where M_p *satisfies*

$$pM_p^2 = \frac{\mu(1-\mu)}{\lambda(1-\lambda)}\frac{d\lambda}{d\mu}$$

with $\frac{d\lambda}{d\mu} = -\frac{\frac{d\Omega_p}{dX}(\mu,\lambda)}{\frac{d\Omega_p}{dY}(\mu,\lambda)}$.

PROOF (cf. [3, Chapter 4]).

Remark 2.8 *There exists modular forms k and u satisfying* $\lambda(\tau) = k^2(\tau) = u^8(\tau)$. *They also induce modular polynomials having properties as above corresponding to the elliptic curves* $E_k : y^2 = x(x-1)(x-k^2)$ *and* $E_u : y^2 = x(x-1)(x-u^8)$. *The associated k– and u–modular polynomials are even simpler than the* λ*–modular polynomial. F.ex. for* $p = 3$ *the u–modular polynomial is*

$$X^4 - Y^4 + 2XY(1 - X^2Y^2)$$

3 Point Counting on Legendre Elliptic Curves

In this section we deploy the framework for p–adic point counting to ordinary elliptic curves on Legendre form. We assume odd characteristics and deal with the case of characteristic two in a remark. We give pseudo code for the algorithm and references for some of the more general and technical aspects of the algorithm. We also give examples and data from experiments.

3.1 The Algorithm

Let p denote an odd prime and $q = p^n$ a power of p. Let $\overline{E}_{\overline{\lambda}}/\mathbf{F}_q : y^2 = x(x-1)(x-\overline{\lambda})$ denote an ordinary elliptic curve on Legendre form with $\overline{\lambda} \notin \mathbf{F}_{p^2}$. Let $\overline{\mathrm{Fr}}_p : \overline{E}_{\overline{\lambda}} \to \overline{E}_{\overline{\Sigma\lambda}}$ denote the p'th power Frobenius isogeny.

Lifting Part

We will now see that the p'th power Frobenius isogeny can be lifted to characteristic zero by solving an equation involving the λ–modular polynomial $\Omega_p \in \mathbf{Z}[X,Y]$ of Section 2.3.

Using the Kronecker relation (2) we see that

$$\Omega_p(\overline{\Sigma\lambda},\overline{\lambda}) = 0 \quad \text{and} \quad \frac{\mathrm{d}\Omega_p}{\mathrm{d}X}(\overline{\Sigma\lambda},\overline{\lambda}) \neq 0 \quad \text{and} \quad \frac{\mathrm{d}\Omega_p}{\mathrm{d}Y}(\overline{\Sigma\lambda},\overline{\lambda}) = 0$$

This implies, as pointed out by Vercauteren in [4], that there is a unique $\lambda \in \mathbf{Z}_q$ satisfying

$$\Omega_p(\Sigma\lambda,\lambda) = 0 \quad \text{and} \quad \lambda \equiv \overline{\lambda} \mod p. \tag{4}$$

Then the Legendre elliptic curve $E_\lambda/\mathbf{Q}_q : y^2 = x(x-1)(x-\lambda)$ reduces to $\overline{E}_{\overline{\lambda}}/\mathbf{F}_q$ modulo p and furthermore from Theorem 2.6 we know there is a p–isogeny $E_\lambda \to E_{\Sigma\lambda}$. According to Lemma 2.2 we may assume that this is a lift of the p–th power Frobenius isogeny. We denote the lifted p'th power Frobenius by $\mathrm{Fr}_p : E_\lambda \to E_{\Sigma\lambda}$.

Norm Part

We determine the action of the lifted p'th power Frobenius isogeny on the invariant differential and the trace of the q'th power Frobenius isogeny.

Let ω and ω^{Σ} denote the invariant differentials on E_{λ} and $E_{\Sigma\lambda}$. According to Lemma 2.7 the action of Fr_p on the invariant differential ω^{Σ} is given by $\mathrm{Fr}_p^*(\omega^{\Sigma}) = \frac{1}{M_p}\omega$ where

$$(pM_p)^2 = -p\frac{\Sigma\lambda(1-\Sigma\lambda)}{\lambda(1-\lambda)}\frac{\mathrm{d}\Omega_p/\mathrm{d}X(\Sigma\lambda,\lambda)}{\mathrm{d}\Omega_p/\mathrm{d}Y(\Sigma\lambda,\lambda)}$$

It follows from Theorem 2.1 that

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(\frac{1}{M_p}) + \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(pM_p).$$

The number of $\mathbf{F}_q$–rational points on $\overline{E}_{\overline{\lambda}}$ can be found from the relation $\#\overline{E}_{\overline{\lambda}} = q+1-\mathrm{Tr}(\overline{\mathrm{Fr}}_q)$. In practice we only need to determine $\mathrm{Tr}(\overline{\mathrm{Fr}}_q)$ modulo p^N, where $N = \lceil \log_p(4\sqrt{q}+1)\rceil$. This follows from the inequality $|\mathrm{Tr}(\overline{\mathrm{Fr}}_q)| \leq 2\sqrt{q}$ (Hasse-Weil).

Pseudo code

We summarize the above by giving a pseudo code algorithm.

```
Algorithm 1: OrderLegendre
  In        : $\overline{\lambda} \in \mathbf{F}_q \setminus \mathbf{F}_{p^2}$
  Out       : The number of $\mathbf{F}_q$–rational points of $\overline{E}_{\overline{\lambda}} : y^2 = x(x-1)(x-\overline{\lambda})$.
  External: SolveModular, pAdicNorm, HasseWitt, SquareRoot
  begin
    $N = \lceil \log_p(4\sqrt{q}+1)\rceil$;
    $\lambda =$ SolveModular$(\Omega_p, \overline{\lambda}, N+1)$;
    $t_2 =$ pAdicNorm$(-p\frac{\mathrm{d}\Omega_p/\mathrm{d}X(\Sigma\lambda,\lambda)}{\mathrm{d}\Omega_p/\mathrm{d}Y(\Sigma\lambda,\lambda)}, N)$;
    $t =$ SquareRoot$(t_2,$ HasseWitt$(\overline{\lambda}), N)$;
    if $t > 2\sqrt{q}$ then
      $t = t - p^N$;
    return $q+1-t$;
  end
```

The algorithm SolveModular solves the modular equation, i.e. SolveModular determines a λ satisfying

$$\Omega_p(\Sigma\lambda,\lambda) \equiv 0 \mod p^{N+1} \quad \text{and} \quad \lambda \equiv \overline{\lambda} \mod p$$

the algorithm pAdicNorm gives the p–adic norm of elements in $\mathbf{Z}_q$, i.e.

$$t_2 = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}\left(-p\frac{\mathrm{d}\Omega_p/\mathrm{d}X(\lambda,\Sigma\lambda)}{\mathrm{d}\Omega_p/\mathrm{d}Y(\lambda,\Sigma\lambda)}\right) \mod p^N,$$

The algorithm HasseWitt calculates the trace modulo p of the q'th power Frobenius isogeny on $\overline{E}_{\overline{\lambda}}$ as described in Corollary A.15. The algorithm SquareRoot calculates the square root modulo p^N.

The algorithms `SolveModular` and `pAdicNorm` are essential to p–adic point counting so they have been given a lot of attention and different versions are at hand. Therefore we content ourselves to giving the references [18, 17, 6, 7, 11]. The algorithm `SquareRoot` can based on Newton iterations together with a trick. The trick is to calculate the inverse of the square root first, because then we avoid inversions.

Remark on characteristic two

We end this section by relating our algorithm to the MSST algorithm in characteristic two. In characteristic two a Weierstrass equation on Legendre form is not a smooth curve and therefore not an elliptic curve. Instead (See [2]) we should consider ordinary elliptic curves on the form

$$\overline{E}_{\overline{a}_6}/\mathbf{F}_q : y^2 + xy = x^3 + \overline{a}_6$$

In [6] Gaudry describes the MSST algorithm which is an algorithm for point counting on ordinary elliptic curves on the form

$$\overline{E}_{\overline{a}_2,\overline{a}_6}/\mathbf{F}_q : y^2 + xy = x^3 + \overline{a}_2 x + \overline{a}_6$$

The MSST algorithm can be described in the same way as Algorithm 3.1. It uses the k–modular polynomial[2] for the lifting part and the associated multiplier for the norm part.

3.2 Examples

Example 3.1 *Our setup is* $p = 3$, $n = 7$, $\mathbf{F}_q = \mathbf{F}_p[x]/(x^7 + x^6 + 2x^5 + x^4 + x^3 + 1)$ *and* $\mathbf{Z}_q = \mathbf{Z}_p[x]/(x^7 + x^6 + 2x^5 + x^4 + x^3 + 1)$. *We let* $\overline{\alpha} = [x] \in \mathbf{F}_q$ *and* $\alpha = [x] \in \mathbf{Z}_q$. *We study the elliptic curve*

$$\overline{E}_{\overline{\lambda}}/\mathbf{F}_q : Y^2 = X(X-1)(X-\overline{\lambda})$$

with $\overline{\lambda} = 2\overline{\alpha}^3 + \overline{\alpha}^2 + \overline{\alpha} + 2$. *From [3, p.105] we find*

$$\Omega_3(X,Y) \quad = \quad (X-Y)^4 - 128XY(1-X)(1-Y)(2-X-Y+2XY)$$

The calculations of the algorithm gives

$$\begin{aligned} N &= 5 \\ \lambda &\equiv 399\alpha^6 + 633\alpha^5 + 3\alpha^4 + 116\alpha^3 + 121\alpha^2 + 55\alpha + 29 \mod p^{N+1} \\ t_2 &\equiv 157 \mod p^N \\ \mathrm{Tr}(\overline{\mathrm{Fr}}_q) &= 20 \\ \#\overline{E}_{\overline{\lambda}}(\mathbf{F}_q) &= 2168 \end{aligned}$$

Example 3.2 *In the Tables below we give some timings for our implementation*[3] . *We used a 600MHz Thinkpad X20 laptop running Linux version 2.4.18-14. The implementation was done in C++ using the gcc compiler and the libraries NTL*[4] *and Gnu MP*[5].

[2] k is a modular form satisfying $k^2 = \lambda$. See [3, Chapter 4]

[3] In characteristic two we are using the MSST algorithm without any special optimizations for characteristic two. In odd characteristic the dominant step of the norm computation is the Teichmuller lift which is not needed in characteristic two. This explains the big increase when going from characteristic two to three.

[4] Number Theory Library. http://www.shoup.net.

[5] http://www.swox.com/gmp/.

We used the descriptions in [17] for the `SolveModular` *and* `pAdicNorm` *algorithms. We remark that asymptotically faster algorithms have been proposed ([7, 11]).*

The λ–modular polynomials where found in [3, p.127ff+Exercise 4.6.4a]. The size of the field $\mathbf{F}_q$ *is given by the number of "bits", where* $q \sim 2^{bits}$.

p	50bits	100bits	150bits	200bits	300bits	500bits
2	0.04s	0.275s	0.915s	1.995s	6.56s	17.415s
3	0.04s	0.16s	0.54s	1.02s	3.31s	14.14s
5	0.03s	0.1s	0.3s	0.62s	2.21s	7.88s
7	0.02s	0.1s	0.23s	0.62s	1.64s	8.25s
11	0.02s	0.13s	0.27s	0.51s	1.84s	9.14s
13	0.02s	0.09s	0.3s	0.56s	2.05s	8.9s
17	0.03s	0.11s	0.36s	0.68s	2.48s	6.83s
19	0.04s	0.12s	0.41s	0.78s	2.89s	7.8s

Table 1: Lifting part

p	50bits	100bits	150bits	200bits	300bits	500bits
2	0.04s	0.15s	0.49s	0.665s	2.085s	4.67s
3	0.08s	0.31s	0.94s	1.565s	4.795s	20.085s
5	0.065s	0.235s	0.63s	1.17s	3.31s	10.335s
7	0.03s	0.25s	0.45s	1.2s	2.215s	9.44s
11	0.03s	0.175s	0.48s	0.755s	2.315s	9.525s
13	0.04s	0.185s	0.52s	0.78s	2.41s	9.535s
17	0.04s	0.2s	0.6s	0.89s	2.69s	6.11s
19	0.045s	0.225s	0.65s	0.975s	2.93s	6.61s

Table 2: Norm part

The tables shows that the algorithm is practical for cryptographic applications.

3.3 Final Remarks

In this paper we have given the basic framework for *p*–adic point counting and applied this to elliptic curves on Legendre form. This results in an efficient algorithm for point counting on these curves using the λ–modular polynomial. It would be interesting to be able to compute the λ–modular polynomial for higher values of *p* than described in the literature ([3, p. 133]) and thus extending the values of *p* for which the algorithm is practical.

Even though the *Canonical Lift* may be avoided in the explanation of many *p*–adic point counting algorithms it lies beneath all of them. So it would be interesting to have a better understanding of it. F.ex. it would be interesting to have elementary proofs for the existence and uniqueness of the canonical lift for ordinary elliptic curves.

A Appendix

A.1 The p–Adic Numbers and Unramified Extensions

In this section we provide the reader with an introduction to the p–adic numbers, unramified extensions and the Frobenius substitution. The presentation is very much inspired by the excellent treatment in Neukirch [14].

Let p denote a prime.

A.1.1 The p–Adic Numbers

Every $x \in \mathbf{Q} \setminus \{0\}$ can be written uniquely as $x = \frac{u}{v} p^i$ where $u, v \in \mathbf{Z} \setminus (p)$ and $i \in \mathbf{Z}$. We define

$$v_p(x) := i.$$

Furthermore we let $v_p(0) := \infty$. We call $v_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ the *p–adic valuation* of $\mathbf{Q}$. It has the following properties

1. $v_p(x) = \infty \Leftrightarrow x = 0$.
2. $v_p(xy) = v_p(x) + v_p(y)$.
3. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, with equality if $v_p(x) \neq v_p(y)$.

The *p–adic absolute value* $|\cdot|_p : \mathbf{Q} \to \mathbf{R}$ is defined by

$$|x|_p = p^{-v_p(x)}.$$

It is a called a *non–archimedian absolute value* since it satisfies

1. $|x|_p \geq 0$ for all $x \in \mathbf{Q}$ with equality iff $x = 0$.
2. $|xy|_p = |x|_p |y|_p$ for all $x, y \in \mathbf{Q}$.
3. $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ with equality if $|x|_p \neq |y|_p$.

Imitating the construction of $\mathbf{R}$ as the completion of $\mathbf{Q}$ with respect to the ordinary absolute value $|\cdot|$ on $\mathbf{Q}$ we can define the p–adic numbers $\mathbf{Q}_p$ as the completion of $\mathbf{Q}$ with respect to the p–adic absolute value $|\cdot|_p$.

To be more explicit let R denote the set of Cauchy sequences in $\mathbf{Q}$ with respect to $|\cdot|_p$ and N the set of null sequences, i.e. sequences converging to 0. R is a ring and N a maximal ideal in R. Let

$$\mathbf{Q}_p := R/N$$

Then $\mathbf{Q}_p$ is a field with $\mathbf{Q} \subseteq \mathbf{Q}_p$ since every element $x \in \mathbf{Q}$ can be viewed as the constant sequence $(x)_n \in R$. The p–adic valuation and absolute value are extended to elements $x = (x_i) \in \mathbf{Q}_p$ by

$$\begin{aligned} v_p(x) &= \lim_{i \to \infty} v_p(x_i) \\ |x|_p &= \lim_{i \to \infty} |x_i|_p \end{aligned}$$

Note that $|x|_p = p^{-v_p(x)}$ for all $x \in \mathbf{Q}_p$. As for the field of real numbers one proves

Proposition A.1 *The field $\mathbf{Q}_p$ is complete with respect to $|\cdot|_p$ and $\mathbf{Q}$ is a dense subset.*

Let $\mathbf{Z}_p := \{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}$. This easily seen to be a ring and the closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ with respect to $|\cdot|_p$. The elements of $\mathbf{Z}_p$ are called *p–adic integers*. We note that the set of units is $\mathbf{Z}_p^* = \{x \in \mathbf{Z}_p \mid |x|_p = 1\}$ and that $p\mathbf{Z}_p = \{x \in \mathbf{Z}_p \mid |x|_p < 1\}$. We also note that $v_p(x) = \max\{i \in \mathbf{N} \mid x \in p^i\mathbf{Z}_p\}$ for all $x \in \mathbf{Z}_p$. So a number is small with respect to $|\cdot|_p$ if it is divisible by a high power of p.

Proposition A.2

$$\mathbf{Z}/p^n\mathbf{Z} \simeq \mathbf{Z}_p/p^n\mathbf{Z}_p$$

for all $n \geq 1$.

PROOF The injectivity of the canonical map is clear. The surjectivity follows from the following argument: Let $x \in \mathbf{Z}_p$ be given. Since $\mathbf{Z}_p$ is the closure of $\mathbf{Z}$ there exists $a \in \mathbf{Z}$ such that $|x-a|_p \leq p^{-n}$. I.e. $x - a \in p^n\mathbf{Z}_p$.

The surjective *reduction modulo p* morphism $\mathbf{Z}_p \to \mathbf{F}_p$ with kernel $p\mathbf{Z}_p$ links characteristic 0 and characteristic p. If $x \in \mathbf{Z}_p$ maps to $\overline{x} \in \mathbf{F}_p$ then $\overline{x}$ is called the *reduction* modulo p of x and x is called a *lift* of $\overline{x}$.

Lemma A.3 *A series $\sum_i x_i$ in $\mathbf{Q}_p$ is convergent iff $\lim_{i\to\infty}|x_i|_p = 0$.*

PROOF

$\Rightarrow$: Well known.

$\Leftarrow$: if $M > N$ then

$$|\sum_{i=0}^{M} x_i - \sum_{i=0}^{N} x_i|_p = |\sum_{i=N+1}^{M} x_i|_p \leq \max_{N+1\leq i\leq M}\{|x_i|_p\}$$

So $(\sum_{i=0}^{N} x_i)_N$ is a Cauchy sequence in $\mathbf{Q}_p$ and therefore convergent.

Corollary A.4 *Every element $z \in \mathbf{Z}_p$ has a unique expression as a* Taylor series *in p*

$$z = \sum_{i=0}^{\infty} a_i p^i$$

with $a_i \in \{0,1,\ldots,p-1\}$.

Every element $z \in \mathbf{Q}_p$ has a unique expression as a Laurent series *in p*

$$z = \sum_{i=-N}^{\infty} a_i p^i$$

with $a_i \in \{0,1,\ldots,p-1\}$.

Proposition A.2 and Corollary A.4 are essential for the practical understanding of $\mathbf{Z}_p$. An element $\sum_{i=0}^{\infty} a_i p^i \in \mathbf{Z}_q$ as above is approximated by the element $\sum_{i=0}^{N-1} a_i p^i \in \mathbf{Z}/p^N\mathbf{Z}$. Notice that the part we throw away has p–adic norm at most p^{-N}. So the greater the N the better the approximation. Furthermore the ring $\mathbf{Z}/p^N\mathbf{Z}$ is very easy to implement on a computer. The reader should compare this to the situation when we represent the real number system on a computer. We can only handle a finite number of decimals so we cut off from a certain point. But the more decimals we use the better the approximation.

A.1.2 Unramified Extensions

Proposition A.5 *Let $\mathbf{Q}_p \subset K$ be a finite field extension of degree n. Then $|\cdot|_p$ on $\mathbf{Q}_p$ may be extended uniquely to a non–archimedian absolute value on K. The extension is given by the formula*

$$|\alpha|_p = \sqrt[n]{\mathrm{N}_{K/\mathbf{Q}_p}(\alpha)} \qquad ,\forall \alpha \in K$$

Furthermore K is complete with respect to $|\cdot|_p$.

PROOF [14, Prop.II.4.8].

For a finite field extension $\mathbf{Q}_p \subseteq K$ we define

$$\begin{aligned} \mathcal{O}_K &:= \{x \in K \mid |x|_p \leq 1\} \\ \mathcal{O}_K^* &:= \{x \in \mathcal{O}_K \mid |x|_p = 1\} \\ \mathcal{M}_K &:= \{x \in \mathcal{O}_K \mid |x|_p < 1\} \\ \Gamma_K &:= \mathcal{O}_K/\mathcal{M}_K \end{aligned}$$

We note that $\mathcal{O}_K^*$ is the set of units in $\mathcal{O}_K$ and $\mathcal{M}_K$ is a maximal ideal in $\mathcal{O}_K$. Γ_K is a field and since $\mathbf{F}_p \simeq \mathbf{Z}_p/p\mathbf{Z}_p$ we have a field extension

$$\mathbf{F}_p \subseteq \Gamma_K.$$

Definition A.6 *A finite field extension $\mathbf{Q}_p \subseteq K$ of degree n is* unramified *if the field extension $\mathbf{F}_p \subseteq \Gamma_K$ (is separable and) has degree n.*

Proposition A.7 *Every unramified extension K of $\mathbf{Q}_p$ of degree n is on the form*

$$K \simeq \mathbf{Q}_p[x]/(f(x))$$

where $f \in \mathbf{Z}[x]$ is a monic polynomial of degree n and the reduction $\overline{f} \in \mathbf{F}_p[x]$ is irreducible. Furthermore $\mathcal{O}_K \simeq \mathbf{Z}_p[x]/(f(x))$, $M_K = (p)$ and $\Gamma_K \simeq \mathbf{F}_p[x]/(\overline{f}(x))$.

Conversely a finite extension of $\mathbf{Q}_p$ on the above form is unramified.

PROOF Since $\mathbf{F}_p \subseteq \Gamma_K$ is a separable field extension of degree n there exists a monic, irreducible polynomial $\overline{f} \in \mathbf{F}_p[x]$ of degree n such that

$$\Gamma_K = \mathbf{F}_p[x]/(\overline{f}(x))$$

Let $f \in \mathbf{Z}[x]$ denote a monic lift of $\overline{f}$, i.e. f is monic and reduces to $\overline{f}$ mod p. A small exercise shows that that $f \in \mathbf{Q}_p[x]$ is irreducible.

Since $\mathcal{O}_K/\mathcal{M}_K \simeq \mathbf{F}_p[x]/(\overline{f}(x))$ there exists $\theta \in \mathcal{O}_K$ such that $f(\theta) \in \mathcal{M}_K$. By Hensel's Lemma ([14, II.4.6]) there exists $\psi \in \mathcal{O}_K$ such that $f(\psi) = 0$ and $\psi \equiv \phi \mod \mathcal{M}_K$. Since $\mathbf{Q}_p \subseteq \mathbf{Q}_p[x]/(f(x))$ has degree n we find that $K = \mathbf{Q}_p[\psi] \simeq \mathbf{Q}_p[x]/(f(x))$.

Every $x \in \mathcal{O}_K \setminus \{0\}$ can now be written

$$p^n x = \sum_{i=0}^{n-1} a_i \psi^i$$

with $n \geq 0$, $a_i \in \mathbf{Z}_p$ and at least one $a_i \in \mathbf{Z}_p^*$. Assume $n > 0$. Reducing mod p we see that

$$0 = \sum_{i=0}^{n-1} \overline{a}_i \overline{\psi}^i$$

But since $\overline{\psi}$ is a root of the irreducible polynomial $\overline{f} \in \mathbf{F}_p[x]$ of degree n all the $\overline{a}_i$'s must be zero (Contradiction). I.e. $n = 0$.

If $x \in M_K$ a similar argument shows that $x \in (p)$.

Corollary A.8 *There exists (up to isomorphism) exactly one unramified extension of $\mathbf{Q}_p$ of degree n. It is denoted by $\mathbf{Q}_q$ where $q = p^n$. The corresponding ring of integers is denoted by $\mathbf{Z}_q$.*

PROOF Let K and L be unramified extension of $\mathbf{Q}_p$ of degree n. Since every every finite field of degree $q = p^n$ is uniquely determined we know that $\Gamma_L \simeq \Gamma_K \simeq \mathbf{F}_p[x]/(\overline{f}(x))$ for some monic, irreducible polynomial $\overline{f} \in \mathbf{F}_p[x]$ of degree n. If $f \in \mathbf{Z}[x]$ is a monic lift of $\overline{f}$ of degree n then it follows directly from the proof of Proposition A.7 that

$$K \simeq \mathbf{Q}_q[x]/(f(x)) \simeq L$$

For the rest of this section we assume $\mathbf{Q}_q$ is given as in Proposition A.7 by a polynomial $f \in \mathbf{Z}[x]$ monic of degree n and with irreducible reduction modulo p and we let $\alpha = x + (f) \in \mathbf{Q}_q$.

Corollary A.9

$$\mathbf{Z}_q/p^n\mathbf{Z}_q \simeq (\mathbf{Z}/p^n\mathbf{Z})[x]/(f(x))$$

for all $n \geq 1$.

The surjective *reduction modulo p* morphism $\mathbf{Z}_q \to \mathbf{F}_q$ with kernel $p\mathbf{Z}_q$ links characteristic 0 and characteristic p. If $x \in \mathbf{Z}_q$ maps to $\overline{x} \in \mathbf{F}_q$ then $\overline{x}$ is called the *reduction* modulo p of x and x is called a *lift* of $\overline{x}$.

Corollary A.10 *Every element $z \in \mathbf{Z}_q$ has a unique expression as a* Taylor series *in p*

$$z = \sum_{i=0}^{\infty}\Big(\sum_{j=0}^{n-1} a_{i,j}\alpha^j\Big)p^i$$

with $a_{i,j} \in \{0, 1, \ldots, p-1\}$.

Every element $z \in \mathbf{Q}_p$ has a unique expression as a Laurent series *in p*

$$z = \sum_{i=-N}^{\infty}\Big(\sum_{j=0}^{n-1} a_{i,j}\alpha^j\Big)p^i$$

with $a_{i,j} \in \{0, 1, \ldots, p-1\}$.

Corollary A.9 and A.10 are essential for the practical understanding of $\mathbf{Z}_q$. An element $\sum_{i=0}^{\infty}(\sum_{j=0}^{n-1} a_{i,j}\alpha^j)p^i \in \mathbf{Z}_q$ as above is approximated by the element $\sum_{i=0}^{N-1}(\sum_{j=0}^{n-1} a_{i,j}\alpha^j)p^i \in (\mathbf{Z}/p^N\mathbf{Z})[x]/(f(x))$. Notice that the part we throw away has p–adic norm at most p^{-N}. So the greater the N the better the approximation. Furthermore the ring $(\mathbf{Z}/p^N\mathbf{Z})[x]/(f(x))$ is very easy to implement on a computer. The reader should compare this to the situation when we represent the real number system on a computer. We can only handle a finite number of decimals so we cut off from a certain point. But the more decimals we use the better the approximation.

A.1.3 The Frobenius Substitution

Corollary A.11 *Let $\overline{\Sigma} : \mathbf{F}_q \to \mathbf{F}_q$ denote the p'th power Frobenius. The Galois group* $\mathrm{Gal}_{\mathbf{Q}_q/\mathbf{Q}_p}$ *is cyclic of degree n generated by the unique element $\Sigma : \mathbf{Q}_q \to \mathbf{Q}_q$ making the following diagram commutative*

$$\begin{tikzcd}
\mathbf{Z}_q \arrow[r, "\Sigma"] \arrow[d] & \mathbf{Z}_q \arrow[d] \\
\mathbf{F}_q \arrow[r, "\overline{\Sigma}"] & \mathbf{F}_q .
\end{tikzcd}$$

(The vertical map is reduction mod p).

Definition A.12 Σ *is called the* Frobenius substitution.

PROOF Write $\mathbf{Q}_q = \mathbf{Q}_p[x]/(f(x))$ with f as in the Proposition. Then $\mathbf{F}_q = \mathbf{F}_p[x]/(\overline{f}(x))$. Let $\theta = X + (f)$ and $\overline{\theta} = X + (\overline{f})$. The roots of $\overline{f}$ are $\overline{\theta}, \overline{\Sigma}(\overline{\theta}), \ldots, \overline{\Sigma}^{n-1}(\overline{\theta})$. It follows from Hensel's Lemma that for each $i \geq 1$ there exists a unique $\psi_i \in \mathbf{Z}_q$ such that $f(\psi_i) = 0$ and $\psi_i \equiv \overline{\Sigma}^i(\theta) \mod p$. We define $\Sigma \in \mathrm{Gal}_{\mathbf{Q}_q/\mathbf{Q}_p}$ by

$$\begin{array}{rcl} \Sigma : \mathbf{Q}_q & \to & \mathbf{Q}_q \\ \theta & \to & \psi_1 \end{array}$$

Then since $f(\Sigma^i(\theta)) = \Sigma^i f(\theta) = 0$ and $\Sigma^i(\theta) \equiv \theta^{p^i}$ we see that $\Sigma^i(\theta) = \psi_i$. It follows that $\mathrm{Gal}(\mathbf{Q}_q/\mathbf{Q}_p) =< \Sigma >$ and the diagram is commutative.

A.2 Proof of the Main Theorem of p–adic Point Counting

Theorem A.13 *Let $\overline{E}/\mathbf{F}_q$ denote an ordinary elliptic curve, $\overline{\mathrm{Fr}}_p : \overline{E} \to \overline{\Sigma E}$ the p'th power Frobenius isogeny and $\overline{\mathrm{Fr}}_q : \overline{E} \to \overline{E}$ the q'th power Frobenius isogeny. Assume $E/\mathbf{Q}_q$ is an elliptic curve reducing to $\overline{E}/\mathbf{F}_q$ modulo p and that $\mathrm{Fr}_p : E \to \Sigma E$ is an isogeny defined over $\mathbf{Q}_q$ and reducing to $\overline{\mathrm{Fr}}_p$ modulo p. Let ω and ω^Σ denote the invariant differentials on E and ΣE.*

There is a unique $M \in \mathbf{Q}_q$ satisfying

$$\mathrm{Fr}_p^*(\omega^\Sigma) = \frac{1}{M}\omega$$

Furthermore $pM \in \mathbf{Z}_q^*$ and the action of $\widehat{\mathrm{Fr}_p}$ on the invariant differential ω is given by

$$\widehat{\mathrm{Fr}_p}^*(\omega) = (pM)\omega^\Sigma.$$

Finally the trace of the q'th power Frobenius isogeny is given by

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(\frac{1}{M}) + \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(pM) \tag{5}$$

where $\mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p} : \mathbf{Q}_q \to \mathbf{Q}_p$ denotes the norm.

PROOF An elliptic curve is a genus 1 curve and therefore the associated $\overline{\mathbf{Q}_q}$–vector space of holomorphic differentials is 1–dimensional. This implies that the set consisting of the invariant differential is a basis. So the existence and uniqueness of $M \in \mathbf{Q}_q$ is clear (The action of Fr_p^* is not zero since characteristic 0).

The action of $\widehat{\mathrm{Fr}_p}$ on the invariant differential is given by the following calculation where we use the fact that Fr_p is a p–isogeny (degrees are invariant under reduction ([21, Prop. II.4.4])).

$$p\omega^{\Sigma} = (\mathrm{Fr}_p \circ \widehat{\mathrm{Fr}_p})^*(\omega^{\Sigma}) = \widehat{\mathrm{Fr}_p}^*(\mathrm{Fr}_p^*(\omega^{\Sigma})) = \frac{1}{M}\widehat{\mathrm{Fr}_p}^*(\omega)$$

Since the elliptic curve E and the isogeny Fr_p is defined over $\mathbf{Q}_q$ we can apply the Frobenius substitution to them. Thus we are able to draw the following commutative diagram where the vertical arrows denote reduction modulo p.

$$\begin{tikzcd}
E \arrow[r, "\mathrm{Fr}_p"'] \arrow[rrrr, bend left, "\mathrm{Fr}_q"] \arrow[d] & \Sigma E \arrow[r, "\Sigma\mathrm{Fr}_p"'] \arrow[d] & \cdots \arrow[r, "\Sigma^{n-2}\mathrm{Fr}_p"'] & \Sigma^{n-1}E \arrow[r, "\Sigma^{n-1}\mathrm{Fr}_p"'] \arrow[d] & E \arrow[d] \\
\overline{E} \arrow[r, "\overline{\mathrm{Fr}}_p"] \arrow[rrrr, bend right, "\overline{\mathrm{Fr}}_q"'] & \overline{\Sigma E} \arrow[r, "\overline{\mathrm{Fr}}_p"] & \cdots \arrow[r, "\overline{\mathrm{Fr}}_p"] & \overline{\Sigma}^{n-1}\overline{E} \arrow[r, "\overline{\mathrm{Fr}}_p"] & \overline{E}
\end{tikzcd}$$

The isogeny Fr_q is the composition of the lifted p'th power Frobenius isogenies. We see that it reduces to the q'th power Frobenius isogeny modulo p. The action of Fr_q on the invariant differential can be found by the following calculation where we use the fact that the Galois group for the field extension $\mathbf{Q}_q/\mathbf{Q}_p$ is generated by the Frobenius substitution.

$$\mathrm{Fr}_q^*(\omega) = \mathrm{Fr}_p^* \circ \Sigma\mathrm{Fr}_p^* \circ \cdots \circ (\Sigma^{n-1}\mathrm{Fr}_p^*)(\omega) = \frac{1}{M}\cdot\frac{1}{\Sigma M}\cdots\frac{1}{\Sigma^{n-1}M}\omega = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(\frac{1}{M})\omega$$

In the same way we find that $\widehat{\mathrm{Fr}}_q^*(\omega) = \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(pM)$. Therefore

$$\mathrm{Tr}(\mathrm{Fr}_q)\omega = (\mathrm{Fr}_q + \widehat{\mathrm{Fr}}_q)^*\omega = \left(\mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(\frac{1}{M}) + \mathrm{N}_{\mathbf{Q}_q/\mathbf{Q}_p}(pM)\right)\omega$$

Combining [20, Prop V.2.3] and [21, Prop II.4.4] we see that $\mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \mathrm{Tr}(\mathrm{Fr}_q)$ and so Equation (5) follows.

A small argument using Equation (5) shows $\frac{1}{M} \in \mathbf{Z}_q$. So reducing modulo p we find $\overline{\mathrm{Fr}}_p^*(\overline{\omega}^{\overline{\Sigma}}) = \overline{(\frac{1}{M})}\overline{\omega}$. Since $\overline{\mathrm{Fr}}_p$ is inseparable it follows from [20, II.4.2.c] that $\overline{(\frac{1}{M})} = 0$ and thus $\frac{1}{M} \in p\mathbf{Z}_q$. An argument as before shows that $pM \in \mathbf{Z}_q$ and using the fact that $\widehat{\overline{\mathrm{Fr}}}_p$ is separable ($\overline{E}$ is ordinary) it follows that $\overline{(pM)} \neq 0$ and thus $pM \in \mathbf{Z}_q^*$.

A.3 The Hasse–Witt Matrix

In point counting we are often able to find the square of the trace of the q'th power Frobenius isogeny. In order to extract the trace itself by Newton iterations we need the trace modulo p. In odd characteristic we can find this by using the Hasse–Witt matrix as stated in Manin [9]. In point counting this is an often mentioned but never clearly stated fact. So we think its time to give an elementary proof. The proof is an extension of the simple case $q = p$ for elliptic curves as found in Manin [9].

Let p denote an odd prime and $q = p^n$.

Proposition A.14 *Let $E/\mathbf{F}_q : y^2 = f(x)$ denote an elliptic curve on Weierstrass form and $\overline{\mathrm{Fr}}_q : E \to E$ the q'th power Frobenius isogeny. Let a_{p-1} denote the x^{p-1} coefficient of $f(x)^{\frac{p-1}{2}}$. Then*

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) \equiv \mathrm{N}_{\mathbf{F}_q/\mathbf{F}_p}(a_{p-1}) \mod p$$

PROOF We see that

$$1 + q - \mathrm{Tr}(\overline{\mathrm{Fr}}_q) = \#E(\mathbf{F}_q) = 1 + q + \sum_{\alpha\in\mathbf{F}_q} \left(\frac{f(\alpha)}{p}\right)$$

where the brackets denote the Legendre symbol. So $\mathrm{Tr}(\overline{\mathrm{Fr}}_q) \equiv -\sum_{\alpha\in\mathbf{F}_q} f(\alpha)^{\frac{q-1}{2}} \mod p$. If we write $f(x)^{\frac{q-1}{2}} = \sum_{i=0}^{3\frac{q-1}{2}} b_i x^i$ we see that $\sum_{\alpha\in\mathbf{F}_q} f(\alpha)^{\frac{q-1}{2}} = \sum_{i=0}^{3\frac{q-1}{2}} b_i \sum_{\alpha\in\mathbf{F}_q} \alpha^i$. Using the fact that $\mathbf{F}_q^*$ is cyclic it is easy to see

$$\sum_{\alpha\in\mathbf{F}_q} \alpha^i = 0 \quad (i \not\equiv 0 \mod q-1) \quad \text{and} \quad \sum_{\alpha\in\mathbf{F}_q} \alpha^{m(q-1)} = -1 \quad (m \geq 1).$$

So

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) \equiv b_{q-1} \mod p$$

Now we find b_{q-1}. We see that

$$f(x)^{\frac{q-1}{2}} = \prod_{i=0}^{n-1} (f(x)^{\frac{p-1}{2}})^{p^i}$$

If $f(x)^{\frac{p-1}{2}} = \sum_{j=0}^{3\frac{p-1}{2}} a_j x^j$ then $(f(x)^{\frac{p-1}{2}})^{p^i} = \sum_{j=0}^{3\frac{p-1}{2}} a_j^{p^i} x^{jp^i}$. Since the only solution of

$$m_0 + m_1 p + \ldots + m_{n-1} p^{n-1} = q - 1$$

with $0 \leq m_i \leq 3\frac{p-1}{2}$ is $\{m_i = p-1\}_i$ it follows that

$$b_{q-1} = \prod_{i=0}^{n-1} a_{p-1}^{p^i} = \mathrm{N}_{\mathbf{F}_q/\mathbf{F}_p}(a_{p-1})$$

Corollary A.15 *Let $E_{\overline{\lambda}}/\mathbf{F}_q : y^2 = x(x-1)(x-\overline{\lambda})$ denote an elliptic curve on Legendre form. Then*

$$\mathrm{Tr}(\overline{\mathrm{Fr}}_q) \equiv (-1)^m H_p(\overline{\lambda}) \mod p$$

where $H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$ and $m = \frac{p-1}{2}$.

PROOF Use Silverman [20, Proof of V.4.1.b].

A.4 Bibliography

References

[1] L. V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.

[2] R. Auer and J. Top. Legendre elliptic curves over finite fields. *J. Number Theory*, 95(2):303–312, 2002.

[3] J. M. Borwein and P. B. Borwein. *Pi and the AGM*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1987. A study in analytic number theory and computational complexity, A Wiley-Interscience Publication.

[4] J. V. F. Vercauteren, B. Preneel. *A Memory Efficient Version of Satoh's Algorithm.*, pages 1–13. Lecture Notes in Computer Science 2045. Springer, 2001.

[5] M. Fouquet, P. Gaudry, and R. Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15(4):281–318, 2000.

[6] P. Gaudry. A comparison and a combination of sst and agm algorithms for counting points of elliptic curves in characteristic 2. Asiacrypt'2002.

[7] R. Harley. Assymptotically optimal p-adic point-counting. In an email to NMBRTHRY list 13. january 2003.

[8] R. Harley, J.-F. Mestre, and P. Gaudry. Counting points with the Arithmetic-Geometric Mean. Eurocrypt 2001, Rump session, 2001.

[9] Ju.I.Manin. The hasse-witt matrix of an algebraic curve. *American Mathematical Society Translations*, 45:245–264, 1965.

[10] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

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

[12] J. Lubin, J. P. Serre, and J. Tate. Elliptic curves and formal groups. In Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 21, 1964. Found at http://www.ma.utexas.edu/users/voloch/1st.html, 1964.

[13] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Springer-Verlag, Berlin, 1972. Lecture Notes in Mathematics, Vol. 264.

[14] J. Neukirch. *Algebraic number theory*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[15] J.-F. M. rédigé par David Lubicz. Algorithmes pour compter des points en petite caractéristique en genre 1 et 2. March 2002.

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

[17] T. Satoh. *On p-adic point counting algorithms for elliptic curves over finite fields*, pages 43–66. Lect. Notes in Comput. Sci. Vol. 2369(2002). Springer, 2002.

[18] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields Appl.*, 9(1):89–101, 2003.

[19] B. Schoeneberg. *Elliptic modular functions: an introduction*. Springer-Verlag, New York, 1974. Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

[20] J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 199? Corrected reprint of the 1986 original.

[21] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[22] B. Skjernaa. Satoh's algorithm in characteristic 2. *Math. Comp.*, 72(241):477–487 (electronic), 2003.