A SIMPLE POINT COUNTING ALGORITHM FOR HESSIAN ELLIPTIC CURVES IN CHARACTERISTIC THREE

TROND STØLEN GUSTAVSEN AND KRISTIAN RANESTAD

Abstract. Given an ordinary elliptic curve on Hesse form over a finite field of characteristic three, we give a sequence of elliptic curves which leads to an effective construction of the canonical lift, and obtain an algorithm for computing the number of points. Our methods are based on the study of an explicitly and naturally given 3-isogeny between elliptic curves on Hesse form.

1. Introduction

Following ideas of Satoh, we deduce by elementary methods a simple algorithm for computing the number of points of an Hessian elliptic curve defined over a finite field of characteristic three. The algorithm has the same complexity as the AGM algorithm in characteristic two.

Schoof's algorithm, see [13], was the first polynomial time algorithm for point counting on elliptic curves over finite fields. In [11] Satoh introduced a new method based on the modular polynomial and the canonical lift. Soon after Mestre gave a more elementary approach, valid in characteristic two, based on the arithmetic-geometric mean (AGM), see [9].

In this paper we give an AGM-like algorithm in characteristic three that uses special properties of Hessian elliptic curves. Our work is independent of the paper [6] of D. Kohel and the thesis [1] of R. Carls, that generalizes both Satoh's method and the AGM algorithm. The key to these generalizations are modular curves and deformations respectively. Our approach is more elementary and gives, like the AGM-approach, a comparably simpler algorithm. In contrast to the approaches of Kohel and Carls, it relies completely on elementary calculations.

The Hessian elliptic curves are those which can be given by an equation of the form $x^3 + y^3 + z^3 = dxyz$ in projective coordinates. The cryptographic features of Hessian elliptic curves are investigated in several papers, see [5], [14], [15], and properties of Hessian elliptic curves in characteristic three are investigated in [15]. According to [10] and [4] field arithmetic in characteristic three may be efficiently implemented in hardware and software, and since our algorithm is relatively easy to implement, it may contribute to the use of elliptic curves over fields of characteristic three in cryptography.

Date: October 26, 2005.

1991 *Mathematics Subject Classification.* [2000] Primary 11G20, 11T71; Secondary 11G07, 14H52.

Key words and phrases. elliptic curve, finite field, point counting, cryptography.

Acknowledgment. We have used the PARI system for testing implementations, see [16]. In understanding aspects of the AGM algorithm in characteristic two, unpublished notes, see [8], on the AGM algorithm by Marc Skov Madsen have been to some help. We thank Anders Høyer Berg, Eivind Eriksen and Runar Ile for helpful remarks.

The point counting method that we propose, proceeds by finding a sequence of elliptic curves in Hesse form over a certain 3-adic ring R leading to an effective construction of the canonical lift. Using Newton iterations we compute the sequence from a recurrence relation in R. Since cubing can be done very efficiently in characteristic three, the computational cost of the recurrence relation is essentially two multiplications. Thus our algorithm compares closely to the AGM-algorithm in characteristic two. Using a proposition of Satoh, we compute the trace of Frobenius by passing to the formal group. As for the AGM-algorithm this results in a norm computation.

2. Preliminaries

2.1. **Notation.** We will denote by $\mathbb{F}_q$ the finite field with $q = 3^n$ elements. We fix an unramified extension K over $\mathbb{Q}_p$ of degree n. The valuation ring of K is denoted by R. We have $R/3R \cong \mathbb{F}_q$, and if $r \in R$ we will denote by $r \bmod 3$ the canonical image in $\mathbb{F}_q$.

The 3-power Frobenius will be denoted by $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, and we denote by $\Sigma : K \to K$ the (little) Frobenius substitution reducing to σ. If E is an elliptic curve over $\mathbb{F}_q$, we denote by $F : E \to E$ the q-Frobenius map given in projective coordinates as $(x, y, z) \mapsto (x^q, y^q, z^q)$. By a slight abuse of notation we will denote also by σ the 3-Frobenius $E \to \sigma E$ given by $(x, y, z) \mapsto (x^3, y^3, z^3)$ where σE is the elliptic curve obtained by applying σ to the coefficients of the defining equation for E. Similarly, if $\mathcal{E}$ is an elliptic curve over K, we will denote by $\Sigma\mathcal{E}$ the elliptic curve obtained by applying Σ to the coefficients of the defining equation for $\mathcal{E}$, and using Σ on the coordinates of a point in $\mathcal{E}$, we also get a map $\mathcal{E} \to \Sigma\mathcal{E}$ which will be denoted by Σ as well.

2.2. **Elliptic curves in Hesse form in characteristic three.** We denote by E_d the curve in $\mathbb{P}^2$ given by the equation $x^3 + y^3 + z^3 = dxyz$. In characteristic three this curve is a non-singular elliptic curve if $d \neq 0$. The addition law on E with $O = (1, -1, 0)$ as the zero element is given as follows. Set $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$. Then we have

$$-P = (y_1, x_1, z_1)$$

$$P + Q = (y_1^2 x_2 z_2 - y_2^2 x_1 z_1, x_1^2 y_2 z_2 - x_2^2 y_1 z_1, z_1^2 y_2 x_2 - z_2^2 y_1 x_1) \tag{2.1}$$

$$[2]P = (y_1(z_1^3 - x_1^3), x_1(y_1^3 - z_1^3), z_1(x_1^3 - y_1^3)) \tag{2.2}$$

In characteristic 3 the relationship to the Weierstrass form is given as follows.

Proposition 1. *A non supersingular elliptic curve E over $\mathbb{F}_q$ may be written in Hesse form if and only if it has a non trivial $\mathbb{F}_q$-rational 3-torsion point. If E has a rational non trivial 3-torsion point, it may be written as $Y^2 = X^3 + X^2 + a_6$ on affine Weierstrass form and as $x^3 + y^3 + 1 = dxy$ in affine Hesse form. Here $a_6 = -1/d^3$ ($d^3 = -1/a_6$ has a unique solution in $\mathbb{F}_q$). The isomorphism is given by $X \mapsto -(1/d)(x + y)$ and $Y \mapsto -(1/d)(x - y)$ and $j(E) = -1/a_6 = d^3$.*

Proof. See [15, Lemma 1]. □

2.3. **Point counting and the canonical lift.** Let E be an elliptic curve over $\mathbb{F}_q$. The number of $\mathbb{F}_q$ rational points is given by $\#E(\mathbb{F}_q) = q + 1 - t$ where $t = \mathrm{Tr}(F)$ is the trace of Frobenius. By Hasse's theorem, $|t| \leq 2\sqrt{q}$.

Satoh introduced the idea of computing the number of points of an elliptic curve over a finite field by lifting the Verschiebung $\widehat{F}$ to R. The canonical lift $\mathcal{E}$ of an ordinary elliptic curve E defined over $\mathbb{F}_q$ is an elliptic curve over K satisfying the properties that (1) the reduction of $\mathcal{E} \pmod 3$ is E and (2) that $\mathrm{End}(\mathcal{E}) \cong \mathrm{End}(E)$.

Deuring [2] has shown that the canonical lift exist and is unique up to isomorphism. Denote by $\mathcal{F} : \mathcal{E} \to \mathcal{E}$ the lift of F. The idea of Satoh is to compute the trace by passing to the formal group using the following proposition:

Proposition 2. *Let $\mathcal{E}$ be an elliptic curve over K and let $f \in \mathrm{End}_K(\mathcal{E})$ be of degree d. Denote by τ the formal parameter of $\mathcal{E}$ at O and assume that the reduction $\pi(f)$ of f modulo 3 is separable and that $f(\ker\pi) \subseteq \ker\pi$. Let $\hat{f}(\tau) = c\tau + O(\tau^2)$ be the homomorphism induced by f on the formal group $\mathcal{E}$. Then $\mathrm{Tr}(f) = c + \frac{d}{c}$.*

However; since the Frobenius endomorphism is inseparable, one cannot apply the proposition to $\mathcal{F}$ directly, but for a non-supersingular elliptic curve, the dual of Frobenius is separable, and we have that $\mathrm{Tr}(F) = \mathrm{Tr}(\widehat{F}) = \mathrm{Tr}(\widehat{\mathcal{F}})$.

3. Computing the canonical lift

For $d \in \mathbb{F}_q$ we denote by $E = E_d$ the corresponding elliptic curve $x^3 + y^3 + z^3 = dxyz$ in Hesse form. We will assume that $d \notin \mathbb{F}_{3^2}$. In this section we will show how to obtain the canonical lift from a sequence $\{D_i\}$ solving a particular recurrence relation in R. To proceed it is convenient to assure that the recurrence relation has a solution in R :

Lemma 1. *Given $D_i \in R$ lifting d^{3^i}, there exists uniquely a $D_{i+1} \in R$ satisfying*

$$(D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3 = 0$$

and $D_{i+1} \bmod 3 = d^{3^{i+1}}$.

Proof. Let $f(z) = (z+6)^3 - (z^2+3z+9)D_i^3$. We get $f'(z) = 3(z+6)^2 + (2z+3)D_i^3$. Let $z_1 \in R$ be any lift of $d^{3^{i+1}}$. Then $f(z_1) \bmod 3 = (d^{3^{i+1}})^3 - (d^{3^{i+1}})^2(d^{3^i})^3 = d^{3^{i+2}} - d^{2\cdot 3^{i+1}+3^{i+1}} = 0 \bmod 3$ and $f'(z_1) \bmod 3 = 2d^{3^{i+1}}(d^{3^i})^3 = 2d^{2\cdot 3^{i+1}} \neq 0$. By Hensel's lemma there exists a unique $D_{i+1} = z_\infty \in R$ such that $D_{i+1} \bmod 3 = d^{3^{i+1}}$ and $f(z_\infty) = 0$ in R. □

In order to define a 3-isogeny $E_{D_{i+1}} \to E_{D_i}$ we consider the map $\mathbb{P}^2_R \to \mathbb{P}^3_R$ given by

$$(x, y, z) \mapsto (y^2z + z^2x + x^2y, y^2x + z^2y + x^2z, xyz, x^3 + y^3 + z^3)$$

where (x, y, z) is sent to the four polynomials u, v, w and t which are invariant under a cyclic permutation of the variables. Note that

$$u^3 + 9w^3 - 6uvw + v^3 + 3w^2t + uvt + wt^2 = 0 \tag{3.1}$$

and that the sub-group $\Lambda = \{(1, -1, 0), (0, 1, -1), (-1, 0, 1)\} \subseteq E[3]$ of 3-torsion points, are mapped to a single point. Assume that $x^3 + y^3 + z^3 = D_{i+1}xyz$. Then we have $t = D_{i+1}v$. Substituting this into (3.1) and using Lemma 1, we get

$$u^3 + v^3 + \left(\frac{D_{i+1} + 6}{D_i}w\right)^3 - (D_{i+1} + 6)uvw = 0.$$

Setting $r = \frac{D_{i+1}+6}{D_i}w$ we get $u^3 + v^3 + r^3 = D_iuvr$. In fact, we have

Proposition 3. *The map above gives a* 3*-isogeny* $\phi_i : E_{D_{i+1}} \to E_{D_i}$ *reducing to the dual* $\widehat{\sigma} : E_{d^{3^{i+1}}} \to E_{d^{3^i}}$ *of the* 3*-Frobenius over* $\mathbb{F}_q$*, such that* $\ker \phi_i = \Lambda$.

Proof. From the above we get a map $E_{D_{i+1}} \to E_{D_i}$ given by

$$(x, y, z) \mapsto (y^2z + z^2x + x^2y, y^2x + z^2y + x^2z, \frac{D_{i+1} + 6}{D_i} xyz).$$

Reducing to $\mathbb{F}_q$ and composing with the 3-Frobenius we get

$$(x, y, z) \mapsto (y^6z^3 + z^6x^3 + x^6y^3, y^6x^3 + z^6y^3 + x^6z^3, d^{2\cdot 3^i} x^3y^3z^3).$$

On the other hand one calculates from (2.1) and (2.2) that multiplication by 3 is given by

$$\begin{aligned}(x, y, z) \mapsto (&y^6z^3 + y^3x^6 + z^6x^3, y^3z^6 + y^6x^3 + z^3x^6 \\ &xyz \left(x^6 + y^6 + z^6 - y^3z^3 - y^3x^3 - z^3x^3\right)),\end{aligned}$$

To see that these two maps are equal we calculate

$$\begin{aligned} d^{2\cdot 3^i} x^3y^3z^3 &= d^{2\cdot 3^i} (xyz)((1/d^{3^i})(x^3 + y^3 + z^3))^2 \\ &= xyz(x^6 + y^6 + z^6 + 2y^3z^3 + 2y^3x^3 + 2z^3x^3) \\ &= xyz(x^6 + y^6 + z^6 - x^3y^3 - x^3z^3 - y^3z^3) \end{aligned}$$

Since degree is invariant under reduction it follows that $E_{D_{i+1}} \to E_{D_i}$ has degree 3. Since $3 = \deg \phi_i \geq \# \ker \phi_i$ and since $\Lambda \subseteq \ker \phi_i$, we have $\ker \phi_i = \Lambda$. □

Let $\mathcal{E}$ denote the canonical lift of E_d and denote by $\mathcal{E}^{(i)} := \Sigma^i \mathcal{E}$ the elliptic curve obtained by applying Σ^i to the coefficients of the equation defining $\mathcal{E}$. Note that $\mathcal{E}^{(nk)} \cong \mathcal{E}$ since $\Sigma^n = \mathrm{id}$. By the following corollary we can compute the j-invariant of the canonical lift and its conjugates $\mathcal{E}^{(i)}$ to arbitrary precision.

Corollary 1. *Assume that* $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$*. Then* $j(E_{D_i}) \equiv j(\mathcal{E}^{(i)}) \bmod 3^{i+1}$.

Moreover; there exists D_i^∞ *such that* $j(E_{D_i^\infty}) = j(\mathcal{E}^{(i)})$, $D_i \equiv D_i^\infty \bmod 3^i$ *and* $D_i^\infty = D^\infty_{i \bmod n}$.

Proof. Note that $j(E_{D_{i+1}}) \bmod 3 = d^{3^{i+1}}$ and that $j(E_{D_i}) \bmod 3 = d^{3^i}$. The proof is by induction. Since the case $i = 0$ is clear, we assume that $j(E_{D_i}) \equiv j(\mathcal{E}^{(i)}) \bmod 3^{i+1}$. From proposition 3 there is a 3-isogeny $E_{D_{i+1}} \to E_{D_i}$. From Theorem 5.3.5 in [7] we have $\Phi_3(j(E_{D_{i+1}}), j(E_{D_i})) = 0$ where Φ_3 is the modular polynomial of degree 3. We also have $\Phi_3(j(\mathcal{E}^{(i+1)}), j(\mathcal{E}^{(i)})) = 0$. Note that $j(E_{D_{i+1}}) \equiv j(\mathcal{E}^{(i+1)}) \bmod 3$. By using the Kronecker relation for Φ_3 we get $\partial\Phi_3/\partial X = X^3 - Y \bmod 3$, $\partial\Phi_3/\partial Y = Y^3 - X \bmod 3$, and $(\partial\Phi_3/\partial X)\left(j(E_{D_{i+1}}), j(E_{D_i})\right) \equiv j(E_{D_{i+1}})^3 - j(E_{D_i}) \equiv (d^{3^{i+1}})^3 - d^{3^i} \equiv (d^9)^{3^i} - d^{3^i} \bmod 3$. Since we have unique third roots in $\mathbb{F}_q$ we have $(d^9)^{3^i} - d^{3^i} = 0$ if and only if $d^9 - d = 0$ if and only if $d \in \mathbb{F}_{3^2}$. Thus by assumption, we have $(\partial\Phi_3/\partial X)\left(j(E_{D_{i+1}}), j(E_{D_i})\right) \not\equiv 0 \bmod 3$. On the other hand we have $(\partial\Phi_3/\partial Y)\left(j(E_{D_{i+1}}), j(E_{D_i})\right) \equiv j(E_{D_i})^3 - j(E_{D_{i+1}}) \equiv (d^{3^i})^3 - d^{3^{i+1}} \equiv 0 \bmod 3$. Now Proposition 2 in [17] show that $j(E_{D_{i+1}}) \equiv j(\Sigma^{i+1}\mathcal{E}) \bmod 3^{i+2}$.

For the second part, we note that for any $t \in K$,

$$j(E_t) = \frac{t^3(t^3 - 216)^3}{t^9 + 81t^6 + 2187t^3 + 19683},$$

see [3]. From the equation $j(E_t) = j(\mathcal{E}^{(i)})$, we get by multiplying with the denominator a polynomial $h_i(t) \in R[t]$. We find that $h_i'(t) = 3t^{11} \bmod 3^2$ and we get

$h_i'(D_{i+n(k+1)}) \not\equiv 0 \bmod 3^2$. Since $h_i(D_i) \equiv 0 \bmod 3^{i+1}$, by Hensel's lemma ($i > 1$) there exists a unique D_i^∞ such that $h_i(D_i^\infty) = 0$ and $D_i \equiv D_i^\infty \bmod 3^i$. We note that $D_i^\infty = D_{i \bmod n}^\infty$ since $h_i(t) = h_{i \bmod n}(t)$. □

4. Computing the trace of Frobenius

To find the trace of Frobenius, we consider the canonical lift to R and pass to the formal group. We will approximate the canonical lift by the E_{D_i} defined in the previous section, and the lift of the dual of σ will be approximated by $E_{D_{i+1}} \to E_{D_i}$. We compute the induced morphism on the formal group up to first order:

Lemma 2. *The completion of the local ring of E_{D_i} (over K) in $O = (1, -1, 0)$ is given as $K[[\tau]]$ where $\frac{y}{x} = \tau - 1$ and $\frac{z}{x} = -\frac{3\tau}{D_i} + O(\tau^3)$. The isogeny $E_{D_{i+1}} \to E_{D_i}$ induces $K[[\tau_i]] \to K[[\tau_{i+1}]]$ given by $\tau_i \mapsto \left(1 + \frac{6}{D_{i+1}}\right)\tau_{i+1} + O(\tau_{i+1}^2)$.*

Proof. We substitute $\frac{y}{x} = \tau - 1$ and $\frac{z}{x} = -3\tau/D$ in $\frac{y^3}{x^3} + \frac{z^3}{x^3} + 1 - D\frac{y}{x}\frac{z}{x}$:

$$1 + (\tau - 1)^3 + (-3\tau/D)^3 - D(\tau - 1)(-3\tau/D) \equiv 0 \bmod(\tau^3).$$

From the map (see proof of Proposition 3)

$$(x, y, z) \mapsto (y^2z + z^2x + x^2y, y^2x + z^2y + x^2z, \frac{D_{i+1} + 6}{D_i}xyz)$$

we calculate

$$\begin{aligned}\tau_i &= \frac{y^2x + z^2y + x^2z}{y^2z + z^2x + x^2y} + 1 = \frac{\left(\frac{y}{x}\right)^2 + \left(\frac{z}{x}\right)^2\frac{y}{x} + \frac{z}{x}}{\left(\frac{y}{x}\right)^2\frac{z}{x} + \left(\frac{z}{x}\right)^2 + \frac{y}{x}} + 1 \\ &= \frac{(\tau_{i+1} - 1)^2 + (-3\tau_{i+1}/D_{i+1})^2(\tau_{i+1} - 1) + (-3\tau_{i+1}/D_{i+1})}{(\tau_{i+1} - 1)^2(-3\tau_{i+1}/D_{i+1}) + (-3\tau_{i+1}/D_{i+1})^2 + (\tau_{i+1} - 1)} + 1 \\ &= 1 + \frac{6}{D_{i+1}}\tau_{i+1} + O(\tau_{i+1}^2)\end{aligned}$$

□

Consider the canonical lift $\mathcal{E}$ of $E = E_d$ given by $x^3 + y^3 + z^3 = dxyz$ over $\mathbb{F}_q$ where $q = 3^n$ and $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$. To compute the trace of Frobenius $\mathrm{Tr}(F)$, we consider the dual $\widehat{\mathcal{F}}$, see Section 2.3, as the composition

$$\mathcal{E} = \Sigma^n\mathcal{E} \to \Sigma^{n-1}\mathcal{E} \to \cdots \to \Sigma^2\mathcal{E} \to \Sigma\mathcal{E} \to \mathcal{E}.$$

We can approximate the map $\widehat{\Sigma} : \Sigma^{i+1}\mathcal{E} \to \Sigma^i\mathcal{E}$ by the map $E_{D_{i+1+nk}} \to E_{D_{i+nk}}$, where $\{D_i\}_{i=0}^\infty$ are in R such that $D_i \bmod 3 = d^{3^i}$, see Lemma 1. By Corollary 1, Proposition 2 and Lemma 2 we get that (setting $k = 1$),

$$\mathrm{Tr}(F) \equiv \prod_{i=1}^n (1 + 6/D_{i+n}) \bmod q.$$

From Corollary 1, we also have that $\Sigma^i D_{nk} \equiv D_{i+nk} \bmod q^k$ and we get

$$\mathrm{Tr}(F) \equiv \prod_{i=1}^n \Sigma^i(1 + 6/D_n) \equiv N_{K/\mathbb{Q}_3}(1 + \frac{6}{D_n}) \bmod q.$$

From Hasse's Theorem, $|\operatorname{Tr}(F)| \leq 2\sqrt{q}$, so this is sufficient to determine $\operatorname{Tr}(F)$. In fact, it suffice to compute $\operatorname{Tr}(F)$ modulo 3^m where $m = \lceil \frac{n}{2} \rceil + 2$, using

$$\operatorname{Tr}(F) \equiv \prod_{i=0}^{n-1}(1 + 6/D_{i+m}) \equiv \prod_{i=0}^{n-1}\Sigma^i(1 + 6/D_m) \equiv N_{K/\mathbb{Q}_3}(1 + \frac{6}{D_m}) \bmod 3^m.$$

In the next section we consider possible algorithms for counting the number of points on the elliptic curve using these identities.

5. Algorithm

The observations above leads to the algorithms 1 and 2 which we will explain in this section.

Algorithm 1 Calculate the trace of Frobenius of a Hessian elliptic curve over $\mathbb{F}_q$

```
Require: An elliptic curve on Hesse form over $\mathbb{F}_q$ given by $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$, and a lift
  $D_0 \in \mathbb{Z}_q$ of $d$.
Ensure: The trace of Frobenius $t = \#E(\mathbb{F}_q) - q + 1$.
  $m \leftarrow \lceil \frac{n}{2} \rceil + 2$
  for $i = 1$ to $m$ do
    $D_i \leftarrow \text{NewtonSolve}((D_i + 6)^3 - (D_i^2 + 3D_i + 9)D_{i-1}^3 = 0) \bmod 3^i$
  end for
  $t \leftarrow (1 + 6/D_m)$
  for $i = m + 1$ to $n + m - 1$ do
    $D_i \leftarrow \text{NewtonSolve}((D_i + 6)^3 - (D_i^2 + 3D_i + 9)D_{i-1}^3 = 0) \bmod 3^m$
    $t \leftarrow t \cdot (1 + 6/D_i) \bmod 3^{m+1}$
  end for
  if $t > 2\sqrt{3^n}$ then
    $t \leftarrow t - 3^m$
  end if
```

Algorithm 2 Calculate the trace of Frobenius of a Hessian elliptic curve over $\mathbb{F}_q$

```
Require: An elliptic curve on Hesse form over $\mathbb{F}_q$ given by $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$, and a lift
  $D_0 \in \mathbb{Z}_q$ of $d$.
Ensure: The trace of Frobenius $t = \#E(\mathbb{F}_q) - q + 1$.
  $m \leftarrow \lceil \frac{n}{2} \rceil + 2$
  for $i = 1$ to $m$ do
    $D_i \leftarrow \text{NewtonSolve}((D_i + 6)^3 - (D_i^2 + 3D_i + 9)D_{i-1}^3 = 0) \bmod 3^i$
  end for
  $t \leftarrow N_{K/\mathbb{Q}_3}(1 + 6/D_m) \bmod 3^m$
  if $t > 2\sqrt{3^n}$ then
    $t \leftarrow t - 3^m$
  end if
```

5.1. **Brief explanation of the algorithms.** In both algorithms, the operation NewtonSolve$((D_i+6)^3-(D_i^2+3D_i+9)D_{i-1}^3=0) \bmod 3^{i+1}$ solves the cubic equation with respect to D_i by Newton iterations with the function

$$f(z)=(z+6)^3-(z^2+3z+9)D_{i-1}^3,$$

starting with any lifting of d^i. In the first algorithm we use $t \equiv \prod_{i=0}^{n-1}(1+6/D_{i+m}) \bmod 3^m$ and in the second algorithm we use $t \equiv N_{K/\mathbb{Q}_3}(1+\frac{6}{D_m}) \bmod 3^{m+1}$. Since $1+\frac{6}{D_m} \in 1+3R$ in the notation of [12, Section 3], we may use [12, Algorithm 2] to compute $N_{K/\mathbb{Q}_3}(1+\frac{6}{D_m})$ efficiently. This algorithm is based on the identity

$$N_{K/\mathbb{Q}_3}(x)=\exp(\mathrm{Tr}_{K/\mathbb{Q}_3}(\log x))$$

when $x \in 1+3R$. Note however that [12, Algorithm 2] is not as efficient in characteristic three as in characteristics two.

5.2. **Complexity.** Optimally, one needs $O(n)$ multiplications in R in algorithm 1. Each multiplication in R needs $O(n^{2\mu})$ bit operations where μ depends on the implementation. This gives totally $O(n^{2\mu+1})$ bit operations. See [10] and [4] for possible values of μ for practical implementations of field arithmetic in characteristic three. Algorithm 2 has the same total complexity but may be more efficient due to fast norm computation, see [12]. We remark that taking the third power can be done very efficiently in characteristic three, so the computational cost of the recurrence relation in the algorithm is essentially two multiplications.

Thus the computational cost compares very closely to the AGM-algorithm in characteristic two, if we use field arithmetic optimized for characteristic three, see [10] and [4].

5.3. **Comparison with other algorithms.** D. Kohel, see [6], and R. Carls, see [1], also give p-adic point counting algorithms that generalizes Mestres AGM algorithm. D. Kohel gives an interpretation of the AGM algorithm in characteristic two and finds generalizations to other low characteristics. He uses modular curves and consider what he calls an oriented modular correspondence.

R. Carls gives a generalized algebraic geometric mean (GAGM) sequence for abelian varieties, and he deduce a point counting algorithm for elliptic curves based on the computation of the GAGM. His algorithm works for ordinary elliptic curves over fields of characteristic $p>2$ and he shows that the algorithm is of the same complexity as the AGM algorithm in characteristic two.

Kohel's paper does not give a complexity bound, it seems however that his methods leads to algorithms in characteristic three of the same complexity as the AGM algorithm in characteristic two. Thus our algorithm has the same complexity as the algorithms of Kohel and of Carls. However; our approach differs from the methods of Kohel and Carls in that it is simpler and more elementary. The recurrence relation that we use are deduced by simple calculations involving the addition law on the elliptic curve. The other parts of the algorithm are exactly the same as in characteristic two. Since Hessian elliptic curves over fields of characteristic three has gained some interest in elliptic curve cryptography (see [5], [14], [15]), we believe it is worthwhile to observe that the special properties of the Hesse form in characteristic three, by elementary considerations, lead to a p-adic point counting algorithm.

To summarize the comparison with the work of Kohel and Carls, we conclude that, although their methods are more general, our approach has the advantage that it is more elementary. We believe that both the deduction of the algorithm and the proof of its correctness, it easier to access. We also consider our algorithm to be easier to implement.

6. An example

To give a simple example, we consider $\mathbb{F}_{3^4}$ represented as $\mathbb{F}_3[x]/(x^4+x^2+2)$, and consider the curve defined by $d = c^3+c+1$, where c is the class of x. We get:

D_0	c^3+c+1
D_1	$(1+2\cdot 3^3)c^3+(3+2\cdot 3^2)c^2+(2+3+2\cdot 3^3)c+(1+3+2\cdot 3^2)$
D_2	$(2+3+3^2)c^3+(2\cdot 3+3^2+2\cdot 3^3)c^2+(2+3+3^2+3^3)c+(1+3+2\cdot 3^2)$
D_3	$(2+2\cdot 3+3^2)c^3+(3+3^2+2\cdot 3^3)c^2+(1+3+2\cdot 3^2+3^3)c+(1+2\cdot 3)$
D_4	$(1+3+3^2+3^3)c^3+(2\cdot 3+3^2)c^2+(1+3+3^2+3^3)c+(1+3+2\cdot 3^2)$
D_5	$(1+3^2+2\cdot 3^3)c^3+(3+3^2+2\cdot 3^3)c^2+(2+3+3^3)c+(1+2\cdot 3)$
D_6	$(2+3+3^2+3^3)c^3+(2\cdot 3+3^2)c^2+(2+3+3^2+3^3)c+(1+3+2\cdot 3^2)$
D_7	$(2+2\cdot 3+3^2)c^3+(3+3^2+2\cdot 3^3)c^2+(1+3+2\cdot 3^2+3^3)c+(1+2\cdot 3)$
D_8	$(1+3+3^2+3^3)c^3+(2\cdot 3+3^2)c^2+(1+3+3^2+3^3)c+(1+3+2\cdot 3^2)$

We compute

$$\begin{aligned}&(1+\frac{6}{D_4})(1+\frac{6}{D_5})(1+\frac{6}{D_6})(1+\frac{6}{D_7}) \bmod q\\ &= 1+2\cdot 3+2\cdot 3^2+2\cdot 3^3 \bmod q\\ &= 79 \bmod q\end{aligned}$$

From the Theorem of Hasse we conclude that $t = 79-3^4 = -2$. This gives

$$\#E = q+1-t = 81+1-(-2) = 84$$

References

1. R. Carls, *A generalized arithmetic geometric mean*, Ph.D. thesis, 2004, http://www.maths.usyd.edu.au/u/carls/thesis.pdf.
2. M. Deuring, *Die Typen der Multiplikatorringe Elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.
3. H. R. Frium, *The group law on elliptic curves on Hesse form*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 123–151.
4. K. Harrison, D. Page, and N. P. Smart, *Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems*, LMS J. Comput. Math. **5** (2002), 181–193 (electronic).
5. M. Joye and J.-J. Quisquater, *Hessian elliptic curves and side-channel attacks*, Cryptographic hardware and embedded systems—CHES 2001 (Paris), Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 402–410.
6. D. R. Kohel, *The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Advances in cryptology—ASIACRYPT 2003 (Taipei, Taiwan) (Berlin), Lecture Notes in Comput. Sci., vol. 2894, Springer, 2003, pp. 124–136.
7. S. Lang, *Elliptic functions*, second ed., Springer-Verlag, New York, 1987.
8. M. S. Madsen, *The AGM-method of point counting on ordinary elliptic curves over finte fields of characteristic 2.*, 2002, http://home.imf.au.dk/marc.
9. J.-F. Mestre, *Lettre adressé à Gaudry et Harley*, http://www.math.jussieu.fr/˜mestre, 2000.

10. D. Page and N. P. Smart, *Hardware implementation of finite fields of characteristic three*, Cryptographic Hardware and Embedded Systems - CHES 2002 (B. S. Kaliski Jr., . K. Ko, and C. Paar, eds.), Springer-Verlag, February 2003, pp. 529–539.
11. T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. (2000), no. 4, 247–270.
12. T. Satoh, B. Skjernaa, and Y. Taguchi, *Fast computation of canonical lifts of elliptic curves and its application to point counting*, Finite Fields and Their Applications **9** (2003), 89–101.
13. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494.
14. N. P. Smart, *The Hessian form of an elliptic curve*, Cryptographic Hardware and Embedded Systems CHES 2001 (C. Paar C.K. Koc, D. Naccache, ed.), Lecture Notes in Comput. Sci., no. 2162, Springer Verlag, 2001, pp. 118–126.
15. N. P. Smart and E. J. Westwood, *Point multiplication on ordinary elliptic curves over fields of characteristic three*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 6, 485–497.
16. The PARI Group, Bordeaux, *PARI/GP, Version 2.1.5*, 2000, available from `http://www.parigp-home.de/`.
17. F. Vercauteren, B. Preneel, and J. Vandewalle, *A memory efficient version of Satoh's algorithm*, Advances in cryptology—EUROCRYPT 2001 (Innsbruck) (Berlin), Lecture Notes in Comput. Sci., vol. 2045, Springer, 2001, pp. 1–13.

University of Oslo, Dept. of Mathematics, P.O. Box 1053, 0316 Oslo, Norway
E-mail address: `stolen@math.uio.no`

University of Oslo, Dept. of Mathematics, P.O. Box 1053, 0316 Oslo, Norway
E-mail address: `ranestad@math.uio.no`