

AN AGM-LIKE ELLIPTIC CURVE POINT COUNTING ALGORITHM 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 on Hesse form leading 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

In this paper we give a simple algorithm for computing the number of points of an Hessian elliptic curve defined over a finite field of characteristic three. The algorithm is inspired by the method of Satoh ([7]) and the AGM algorithm in characteristic two, [2]. It has the same complexity as the AGM algorithm in characteristic two. Our methods are based on the explicit computation of a naturally given 3-isogeny between elliptic curves on Hesse form.

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, [4], [10], [9], and the properties of Hessian elliptic curves in characteristic three are investigated in [9]. According to [6] and [3] field arithmetic may be efficiently implemented in hardware and software. Since our algorithm is very easy to implement and of same complexity as the AGM algorithm in characteristic two, it may contribute to the use of characteristic three elliptic curves in cryptography.

The point counting method that we propose, proceed by finding a sequence of elliptic curves on 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. However, we will not discuss this part of the algorithm, but one may use the fast norm computation of [8].

Date: December 1, 2003.

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

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

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 $R/(3)R \cong \mathbb{F}_q$, 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 $\sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q$. We denote by $\Sigma : K \rightarrow K$ the Frobenius substitution. If E is an elliptic curve over $\mathbb{F}_q$, we denote by $F : E \rightarrow E$ 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 $E \rightarrow E$ given by $(x, y, z) \mapsto (x^3, y^3, z^3)$.

2.2. Elliptic curves on 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 $Q = (x_2, y_2, z_2)$ we have

$$\begin{aligned} -P &= (y_1, x_1, z_1) \\ P + Q &= (y_1^2 x_2 z_2 - y_2^2 x_1 z_1, x_1^2 y_2 z_2 - x_2^2 y_1 z_1, z_1^2 y_2 x_2 - z_2^2 y_1 x_1) \\ [2]P &= (y_1(z_1^3 - x_1^3), x_1(y_1^3 - z_1^3), z_1(x_1^3 - y_1^3)) \end{aligned}$$

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

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

Proof. See [9, 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 $t = \text{Tr}(F)$ 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 Verschöbung $\hat{F}$ 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 $\text{End}(\mathcal{E}) \cong \text{End}(E)$.

Deuring [1] has shown that the canonical lift exist and is unique up to isomorphism. We will denote by $\mathcal{F} : \mathcal{E} \rightarrow \mathcal{E}$ 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 $f \in \text{End}_K(\mathcal{E})$ 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 $\text{Tr}(f) = c + \frac{d}{c}$.*

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 $\text{Tr}(F) = \text{Tr}(\hat{F}) = \text{Tr}(\hat{\mathcal{F}})$.

3. COMPUTING THE CANONICAL LIFT

For $d \in \mathbb{F}_q$ we denote by $E = E_d$ the corresponding elliptic curve $x^3 + y^3 + z^3 = dxyz$ on 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. *Let $D_0 \in R$ is any lift d . Then given $D_i \in R$ 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 $D_{i+1} = d^{3^{i+1}} \pmod{3}$.

Proof. Let $f(z) = (z+6)^3 - (z^2 + 3z + 9)D_i^3$. We get $f'(z) = 3(z+6) + (2z+3)D_i^3$. Let $z_1 \in R$ be any lift of $d^{3^{i+1}}$. Then $f(z_1) \equiv (d^{3^{i+1}})^3 - (d^{3^{i+1}})^2(d^{3^i})^3 = d^{3^{i+2}} - d^{2 \cdot 3^{i+1} + 3^{i+1}} = 0 \pmod{3}$ and $f'(z_1) \equiv 2d^{3^{i+1}}(d^{3^i})^3 \equiv 2d^{2 \cdot 3^{i+1}} \not\equiv 0 \pmod{3}$. By Hensels lemma there exists a unique $D_{i+1} = z_\infty \in R$ such that $f(z_\infty) = 0$ in R . $\square$

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

$$(3.1) \quad u^3 + 9w^3 - 6uvw + v^3 + 3w^2t + uvt + wt^2 = 0$$

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 $u^3 + v^3 + r^3 = D_{i+1}uvr$. In fact, we have

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

Proof. From the above, we have the map

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

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

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

On the other hand the multiplication by 3 is given by

$$(x, y, z) \mapsto (y^6z^3 + y^3x^6 + z^6x^3, y^3z^6 + y^6x^3 + z^3x^6, xyz(x^6 + y^6 + z^6 - y^3z^3 - y^3x^3 - z^3x^3)).$$

To see that these two maps are equal we calculate

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

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

By the following corollary this allow us to compute the j -invariant of the canonical lift and its conjugates to arbitrary precession.

Corollary 1. *Assume that $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$, and denote by $\mathcal{E}$ the canonical lift of E_d . Then $j(E_{D_i}) \equiv j(\Sigma^i \mathcal{E}) \pmod{3^{i+1}}$.*

Proof. Note that $j(E_{D_{i+1}}) \pmod{3} = d^{3^{i+1}}$ and that $j(E_{D_i}) = d^{3^i} \pmod{3}$. The proof is by induction. Since the case $i = 0$ is clear, we assume that $j(E_{D_i}) \equiv j(\Sigma^i \mathcal{E}) \pmod{3^{i+1}}$. From proposition 3 there is a 3-isogeny $E_{D_{i+1}} \rightarrow E_{D_i}$. From Theorem 5.3.5 in [5] 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 $\Phi_3(j(\Sigma^{i+1} \mathcal{E}), j(\Sigma^i \mathcal{E})) = 0$. Note that $j(E_{D_{i+1}}) = j(\Sigma^{i+1} \mathcal{E}) \pmod{3}$. By using the Kronecker relation for Φ_3 we get

$$\frac{\partial \Phi_3}{\partial X} = X^3 - Y \pmod{3} \text{ and } \frac{\partial \Phi_3}{\partial Y} = Y^3 - X \pmod{3}$$

We get

$$\begin{aligned} \frac{\partial \Phi_3}{\partial X} (j(E_{D_{i+1}}), j(E_{D_i})) &= \frac{\partial \Phi_3}{\partial X} (j(E_{D_{i+1}})^3, j(E_{D_i})) \\ &= j(E_{D_i})^9 - j(E_{D_i}) \pmod{3} \\ &= (d^{3^i})^9 - d^{3^i} = (d^9)^{3^i} - d^{3^i} \end{aligned}$$

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 $(\partial \Phi_3 / \partial X) (j(E_{D_{i+1}}), j(E_{D_i})) \not\equiv 0 \pmod{3}$. On the other hand we have

$$\begin{aligned} \frac{\partial \Phi_3}{\partial Y} (j(E_{D_{i+1}}), j(E_{D_i})) &= \frac{\partial \Phi_3}{\partial Y} (j(E_{D_i}), j(E_{D_i})^3) \\ &= j(E_{D_i})^3 - j(E_{D_i})^3 \pmod{3} = 0 \end{aligned}$$

Now we may use Proposition 2 in [11] to show that $j(E_{D_{i+1}}) = j(\Sigma^{i+1} \mathcal{E}) \pmod{3^{i+2}}$. $\square$

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; the lift of the dual of σ will be approximated by $E_{D_{i+1}} \rightarrow E_{D_i}$. We compute the induced morphism on the formal group up to first order:

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

$$1 + (\tau - 1)^3 + (-3\tau/D)^3 - D(\tau - 1)(-3\tau/D) = 0 \pmod{\tau^3}.$$

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

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

□

Assume that $E = E_d$ is given by $x^3 + y^3 + z^3 = dxyz$ over $\mathbb{F}_q$ where $q = 3^n$ and $d \in \mathbb{F}_q \setminus \mathbb{F}_{3^2}$. By Lemma 1 there exist a sequence $\{D_i\}_{i=0}^\infty$ of elements in R such that $D_i = d^{3^i} \pmod{3}$ and such that $(D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3 = 0$. To compute the trace of Frobenius, we consider the dual $\widehat{\mathcal{F}}$ as the composition

$$\mathcal{E} = \Sigma^n \mathcal{E} \rightarrow \Sigma^{n-1} \mathcal{E} \rightarrow \dots \rightarrow \Sigma^2 \mathcal{E} \rightarrow \Sigma \mathcal{E} \rightarrow \mathcal{E}.$$

We approximate the map $\widehat{\Sigma} : \Sigma^{i+1} \mathcal{E} \rightarrow \Sigma^i \mathcal{E}$ by the map $E_{D_{i+1+n_k}} \rightarrow E_{D_{i+n_k}}$. By Corollary 1 this holds modulo 3^{i+1+n_k} . (In fact, since

$$j(E_D) = \frac{D^3(D^3 - 216)^3}{D^9 + 81D^6 + 2187D^3 + 19683}$$

we may solve a polynomial equation resulting from $j(E_D) = j(\mathcal{E}_D)$ (where $\mathcal{E}_D$ is the canonical lift of E_D) by Newton's method to find D reducing to D_i and thus assume that E_{D_i} is obtained as reduction $(\pmod{3^{i+1}})$ of the canonical lift.) From Section 2.3, Proposition 2 and from Lemma 2 we get that for $k = 1$,

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

We also have that $\Sigma^i D_{nk} \equiv D_{i+n_k}$ and we get

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

We may in fact do better: Because of Hasse's Theorem, it suffice to compute t modulo 3^m where $m = \lceil \frac{n}{2} \rceil + 2$. In fact we may use

$$t \equiv \prod_{i=m}^{m+n} \Sigma^i (1 + 6/D_i) \pmod{3^m} \equiv N_{K/\mathbb{Q}_3} (1 + \frac{6}{D_m}) \pmod{3^m}.$$

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

Algorithm 1 Calculate the trace of Forbenius of an 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 Forbenius $t = \#E(\mathbb{F}_q) - q + 1$.

$m \leftarrow \lceil \frac{n}{2} \rceil + 2$

for $i = 1$ to m **do**

$\text{solve}((D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3, D_{i+1}) \bmod 3^{i+2}$

end for

$t \leftarrow (1 + 6/D_m)$

for $i = m$ to $n + m - 1$ **do**

$\text{solve}((D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3, D_{i+1}) \bmod 3^{m+2}$

$t \leftarrow t \cdot (1 + 6/D_i) \bmod 3^{m+2}$

end for

if $t > 2\sqrt{3^n}$ **then**

$t \leftarrow -t$

end if

Algorithm 2 Calculate the trace of Forbenius of an 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 Forbenius $t = \#E(\mathbb{F}_q) - q + 1$.

$m \leftarrow \lceil \frac{n}{2} \rceil + 2$

for $i = 1$ to m **do**

$\text{solve}((D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3, D_{i+1}) \bmod 3^{i+2}$

end for

$t \leftarrow N_{K/\mathbb{Q}_3}(1 + (6/(D_m))) \bmod 3^m$

if $t > 2\sqrt{3^n}$ **then**

$t \leftarrow -t$

end if

5. ALGORITHM

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

5.1. Brief explanation of the algorithms. In both algorithms, the operation $\text{solve}((D_{i+1} + 6)^3 - (D_{i+1}^2 + 3D_{i+1} + 9)D_i^3, D_{i+1}) \bmod 3^{i+2}$ is done by Newton iterations with the function $f(z) = (z + 6)^3 - (z^2 + 3z + 9)D_i^3$ starting with any lifting of d^{i+1} . In the first algorithm we use $t \equiv \prod_{i=m}^{m+n} \Sigma^i(1 + 6/D_i) \bmod 3^m$ and in the second algorithm we use $N_{K/\mathbb{Q}_3}(1 + \frac{6}{D_m}) \bmod 3^m$. We refer to [8] on how to compute $t = N_{K/\mathbb{Q}_3}(1 + \frac{6}{D_m})$ efficiently.

5.2. Comments on the complexity. Optimally done, 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. With Schönhage multiplication this gives $O(n^{3+\epsilon})$. Algorithm 2 will have the same total complexity but may be more efficient due to fast norm computation, see [8].

6. EXAMPLES

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 have $j = d^3 = c^3 + 2c + 1$. This gives $j^8 = c^3 + 2c + 1 \neq 1$ which ensures $j \notin \mathbb{F}_{3^2}$. We get:

$$\begin{aligned} D_0 & c^3 + c + 1 \\ D_1 & (1 + 2 \cdot 3^3)c^3 + (3 + 2 \cdot 3^2)c^2 + (2 + 3 + 2 \cdot 3^3)c + (1 + 3 + 2 \cdot 3^2) \\ D_2 & (2 + 3 + 3^2)c^3 + (2 \cdot 3 + 3^2 + 2 \cdot 3^3)c^2 + (2 + 3 + 3^2 + 3^3)c + (1 + 3 + 2 \cdot 3^2) \\ D_3 & (2 + 2 \cdot 3 + 3^2)c^3 + (3 + 3^2 + 2 \cdot 3^3)c^2 + (1 + 3 + 2 \cdot 3^2 + 3^3)c + (1 + 2 \cdot 3) \\ D_4 & (1 + 3 + 3^2 + 3^3)c^3 + (2 \cdot 3 + 3^2)c^2 + (1 + 3 + 3^2 + 3^3)c + (1 + 3 + 2 \cdot 3^2) \\ D_5 & (1 + 3^2 + 2 \cdot 3^3)c^3 + (3 + 3^2 + 2 \cdot 3^3)c^2 + (2 + 3 + 3^3)c + (1 + 2 \cdot 3) \\ D_6 & (2 + 3 + 3^2 + 3^3)c^3 + (2 \cdot 3 + 3^2)c^2 + (2 + 3 + 3^2 + 3^3)c + (1 + 3 + 2 \cdot 3^2) \\ D_7 & (2 + 2 \cdot 3 + 3^2)c^3 + (3 + 3^2 + 2 \cdot 3^3)c^2 + (1 + 3 + 2 \cdot 3^2 + 3^3)c + (1 + 2 \cdot 3) \\ D_8 & (1 + 3 + 3^2 + 3^3)c^3 + (2 \cdot 3 + 3^2)c^2 + (1 + 3 + 3^2 + 3^3)c + (1 + 3 + 2 \cdot 3^2) \end{aligned}$$

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

$$\begin{aligned} \#E & = q + 1 - t \\ & = 81 + 1 - (-2) \\ & = 84 \end{aligned}$$

We consider $\mathbb{F}_{3^5}$ represented as $\mathbb{F}_3[x]/(x^5 + 2x + 2)$. We get

$$\prod_{i=5}^9 \left(1 + \frac{6}{D_i}\right) \bmod q = 1 + 3 + 2 \cdot 3^3 + 2 \cdot 3^4 = 220$$

We have $q = 3^5 = 243$ and $2\sqrt{3^5} = 18\sqrt{3} = 31.177$. We conclude that $t = 220 - 243 = -23$. Hasse says:

$$213 = q + 1 - 31 < \#E < q + 1 + 32 = 276$$

We get

$$\#E = q + 1 - t = 243 + 1 + 23 = 267$$

REFERENCES

- [1] M. Deuring. Die typen der multiplikatorringe elliptischer funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941.
- [2] R. Harley and P. G. J. F. Mestre. Counting points with arithmetic-geometric mean. Eurocrypt 2001, Rump session.
- [3] K. Harrison, D. Page, and N. P. Smart. Software implementation of finite fields of characteristic three. Preprint, 2002.
- [4] M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In D. N. C.K. Koc and C. Paar, editors, *Cryptographic Hardware and Embedded Systems CHES 2001*, number 2162 in Lecture Notes in Computer Science, pages 402–410. Springer Verlag, 2001.
- [5] S. Lang. *Elliptic Functions*. Springer-Verlag, New York, second edition, 1987.

- [6] D. Page and N. P. Smart. Hardware implementation of finite fields of characteristic three. In *Cryptographic Hardware and Embedded Systems - CHES 2002*, 2002. Springer LNCS ????
- [7] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, (no. 4):247–270, 2000.
- [8] T. Satoh, B. Skjærnaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications*, 9:89–101, 2003.
- [9] N. Smart and J. Westwood. Point multiplication on ordinary elliptic curves over fields of characteristic three. Cryptology ePrint Archive, Report 2002/114, 2002. <http://eprint.iacr.org/>.
- [10] N. P. Smart. The hessian form of an elliptic curve. In D. N. C.K. Koc and C. Paar, editors, *Cryptographic Hardware and Embedded Systems CHES 2001*, number 2162 in Lecture Notes in Computer Science, pages 118–126. Springer Verlag, 2001.
- [11] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of satoh’s algorithm. In *EUROCRYPT 2001, LNCS 2045*, pages 1–13. Springer-Verlag Berlin Heidelberg, 2001.

AGDER COLLEGE, DEPT. OF INFORMATION AND COMMUNICATION TECHNOLOGY, 4876 GRIMSTAD, NORWAY

E-mail address: `trond.gustavsen@hia.no`

UNIVERSITY OF OSLO, DEPT. OF MATHEMATICS, P.O. Box 1053, 0316 OSLO, NORWAY

E-mail address: `ranestad@math.uio.no`