MATHEMATICS OF COMPUTATION
Volume 72, Number 241, Pages 477–487
S 0025-5718(02)01434-5
Article electronically published on March 22, 2002

SATOH'S ALGORITHM IN CHARACTERISTIC 2

BERIT SKJERNAA

Abstract. We give an algorithm for counting points on arbitrary ordinary elliptic curves over finite fields of characteristic 2, extending the $O(\log^5 q)$ method given by Takakazu Satoh, giving the asymptotically fastest point counting algorithm known to date.

Introduction

The mathematical aspects of elliptic curves have been studied during the 20th century, and have been used in connection with factorization and primality testing, and were a key ingredient in Wiles' proof of Fermat's last theorem.

Since elliptic curves were suggested for cryptography independently by N. Koblitz [Kob87] and V. Miller [Mil86] in 1985, a lot of work has been carried out to find methods to construct suitable curves. A requirement to avoid certain attacks on the cryptosystem is that the curve chosen has group order divisible by a large prime. Several attempts at choosing special kinds of curves where the group order is easily computable have proven to give insecure curves. Even though some special kinds might still be secure, using the full space of elliptic curves is widely recommended as the best method. However, even with Schoof's pioneering method [Sch85], it was not practically possible to count points on curves of cryptographic interest, before it was improved by Elkies and Atkin for the case of large characteristic, and by Couveignes for characteristic 2.

In 1999, T. Satoh [Sat00] gave a new method for counting points on an arbitrary elliptic curve over a field $\mathbb{F}_q$ of small characteristic p greater than 5. The algorithm runs in $O(\log^5 q)$ with straightforward arithmetic but is heavily dependent on p, whereas the improvements of Schoof's method runs in $O(\log^6 q)$ with reasonable assumptions. Thus, for fixed characteristic, the asymptotic behavior of Satoh's algorithm is faster than for previously known algorithms.

In this paper, we will generalize the results of Satoh to the characteristic 2 case, which is the most interesting case for applications. We will start by giving an outline of the algorithm, before proceeding with the details. After the conclusions, we will give a small illustrative example, and discuss the performance for curves of cryptographic interest.

Received by the editor September 4, 2000 and, in revised form, March 15, 2001.
2000 *Mathematics Subject Classification.* Primary 11G20, 11T71; Secondary 11G07, 14H52.
Key words and phrases. Satoh's algorithm, elliptic curves, finite fields, order counting.
Research supported in part by a Ph.D. grant from CRYPTOMAThIC.

1. Outline

Let $\overline{E}:\ y^2+xy=x^3+\overline{a}_6$ be an elliptic curve defined over the finite field $\mathbb{F}_{2^N}$, with $j(\overline{E})\notin\mathbb{F}_4$. We want to count the number of points in $\overline{E}(\mathbb{F}_{2^N})$.

As in Schoof's algorithm, our aim is to calculate the trace of the 2^N'th power Frobenius: $\mathrm{Fr}_{2^N}\in\mathrm{End}(\overline{E})$, since $\#\overline{E}(\mathbb{F}_{2^N})=2^N+1-\mathrm{Tr}(\mathrm{Fr}_{2^N})$. To do this we split the Frobenius into N small Frobenius maps, giving rise to the following sequence:

$$\overline{E}\xrightarrow{\mathrm{Fr}_2}\overline{E}_1\xrightarrow{\mathrm{Fr}_2}\cdots\xrightarrow{\mathrm{Fr}_2}\overline{E}_N=\overline{E}.$$

Let $\mathbb{Q}_2$ denote the 2-adic numbers, and let K be the unramified extension of $\mathbb{Q}_2$ of degree N given by $\mathbb{Q}_2[X]/f(X)\mathbb{Q}_2[X]$, where $f(X)\in\mathbb{Z}_2[X]$ is the polynomial with only 0's and 1's as coefficients, whose reduction modulo 2 is used to define $\mathbb{F}_{2^N}$. Denote by R the valuation ring of K. We want to simultaneously lift the j-invariants of the above curves to R, in such a way that the small Frobenius maps can all be lifted to isogenies between the lifted curves. Thus having lifted the j-invariants modulo 2^M for a well chosen value M, we will use the fact that the trace of an endomorphism is not altered by reduction, to get an explicit formula for $\mathrm{Tr}(\mathrm{Fr}_{2^N})^2 \mod 2^{M-9}$. Now using Hensel's Lemma we can find $\pm\mathrm{Tr}(\mathrm{Fr}_{2^N}) \mod 2^{M-10}$, by lifting a square root modulo 8. Finally, we determine $\mathrm{Tr}(\mathrm{Fr}_{2^N})$ by using $\#\overline{E}(\mathbb{F}_{2^N})\equiv 0 \mod 4$ and $|\mathrm{Tr}(\mathrm{Fr}_{2^N})|\le 2\sqrt{2^N}$.

Note that all calculations will be carried out in $R \mod 2^M$ for some M, and that this ring can be represented as polynomials of degree less than N, with coefficients in $\mathbb{Z}/2^M\mathbb{Z}$.

Throughout the paper, a bar over an object (e.g., an elliptic curve or an element) will denote that it is over the finite field. A bar over an object of R denotes the reduction modulo the prime in question (mostly 2).

Where no other references are given, the theory can be found in [Sil86].

2. Preliminaries

First note that none of the restrictions in the outline are crucial. If $j(\overline{E})\in\mathbb{F}_4$, then $\#\overline{E}(\mathbb{F}_{2^N})$ is easily found from $\#\overline{E}(\mathbb{F}_4)$ ([Eng99, Theorem 3.66]). If $\overline{E}$ is the curve given by $y^2+xy=x^3+\overline{a}_2x^2+\overline{a}_6$, either $\overline{E}$ is isomorphic to $\overline{E}':\ y^2+xy=x^3+\overline{a}_6$ (if $\mathrm{Tr}(\overline{a}_2)=0$), or $\overline{E}'$ is the twist of $\overline{E}$ by $\overline{a}_2$, and $\#\overline{E}'(\mathbb{F}_{2^N})+\#\overline{E}(\mathbb{F}_{2^N})=2^N+2$ (see [Eng99, Section 3.10]).

In this text we will always choose the form $y^2+xy=x^3-\frac{36}{j(E)-1728}x-\frac{1}{j(E)-1728}$ for our elliptic curves ([Sil86, p. 52]). Note that if an elliptic curve E over an unramified extension of $\mathbb{Q}_2$ has good reduction mod 2 to a nonsupersingular elliptic curve, then the chosen form is a minimal Weierstrass equation, i.e., the 2-valuation of the discriminant is 0.

To lift the j-invariants in such a way that the small Frobenius maps can be lifted, we use the 2nd modular polynomial, Φ_2, which, by [Coh93, p. 379], is given by

$$\begin{aligned}\Phi_2(X,Y)\ &= X^3+Y^3-X^2Y^2+2^4 3\cdot 31(X^2Y+XY^2)-2^4 3^4 5^3(X^2+Y^2)\\ &\quad+3^4 5^3 4027XY+2^8 3^7 5^6(X+Y)-2^{12}3^9 5^9.\end{aligned}$$

Recall that the n'th modular polynomial, Φ_n, is a symmetric polynomial in 2 variables with the property that two curves E and E', over a field of characteristic zero, have an n-isogeny iff $\Phi_n(j(E),j(E'))=0$ [Lan87, Theorem 5.3.5, p. 59].

We want to lift a solution $(z_0, z_1, ..., z_{N-1})$ of the system of equations

$$\begin{cases} \Phi_2(z_0, z_1) \equiv \Phi_2(z_1, z_2) \equiv \cdots \equiv \Phi_2(z_{N-1}, z_0) \equiv 0 \mod 2, \\ \overline{z_i} = j(\overline{E}_i),\ i = 0, \ldots, N-1, \end{cases}$$

to a solution $(w_0, w_1, ..., w_{N-1})$ in K of the system of equations

$$\begin{cases} \Phi_2(w_0, w_1) = \Phi_2(w_1, w_2) = \cdots = \Phi_2(w_{N-1}, w_0) = 0, \\ \overline{w_i} = j(\overline{E}_i),\ i = 0, \ldots, N-1, \end{cases}$$

thus giving us j-invariants for which 2-isogenies exist between the corresponding curves.

The following theorem now shows that this allows us to lift the small Frobenius maps.

Theorem 2.1. *Let $\overline{E}$ be an ordinary elliptic curve defined over a finite field of characteristic $p > 0$, with $j(\overline{E}) \notin \mathbb{F}_{p^2}$, and let $\overline{E}^{(p)}$ be the curve obtained from E by applying the small Frobenius, Fr_p, to its coefficients. If E and E' are two curves reducing to $\overline{E}$ and $\overline{E}^{(p)}$ respectively, and there exists a p-isogeny between E and E', then Fr_p can be lifted to an isogeny between E and E'.*

Proof. Let f be a p-isogeny between E and E'; then its reduction $\overline{f}$ has degree p (degrees are invariant under reduction), and since it cannot be separable (by going to duals this is easily seen to imply $\overline{E} \cong \overline{E}^{(p^2)}$), it must be of the form $\overline{f} = \lambda \circ \mathrm{Fr}_p$, where λ is an automorphism. Thus $\lambda = [\pm 1]$, and Fr_p is the reduction of either f or of $-f$. □

Remark. The above theorem implies that we can avoid the theory of the canonical lift.

To find out more about the trace of Frobenius, we will use the following proposition:

Proposition 2.2. *Let $\mathcal{E}/_K$ be an elliptic curve, and let $f \in \mathrm{End}_K(\mathcal{E})$ be of degree d. Let $\tau = -\frac{X}{Y}$ be the local parameter at $\mathcal{O}$, and assume that the reduction $\overline{f}$ of f modulo p is separable. Then $\mathrm{Tr}(f) = c_1 + \frac{d}{c_1}$, where $\tau \circ f = \sum_{n=1}^{\infty} c_n \tau^n$.*

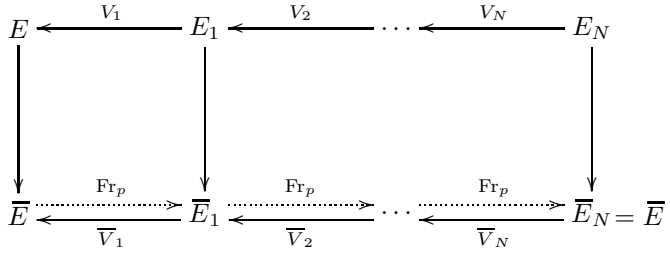
Proof. $f \circ f - f \circ [\mathrm{Tr}(f)] + [d] = [0]$ in $\mathrm{End}(\mathcal{E})$; thus $(c_1^2 - c_1 \mathrm{Tr}(f) + d)\tau + O(\tau^2) = 0$ in the formal group $\widehat{\mathcal{E}}$. Hence the coefficient of τ must vanish. Since $\overline{f}$ is separable, c_1 must be nonzero, and $\mathrm{Tr}(f) = c_1 + \frac{d}{c_1}$. □

Since the Frobenius map is not itself separable, we will have to work with its dual. Fortunately, the dual of the lift is precisely equal to the lift of the dual, and it is composed of the lifts of the duals of the small Frobenius maps. We will denote the dual of the small Frobenius $\mathrm{Fr}_2 \in \mathrm{Isog}(\overline{E}_{i-1}, \overline{E}_i)$, $i = 1, \ldots, N$, by $\overline{V}_i$, and its lift by V_i. We will later need the fact that $\mathrm{Ker}\, V_i$ is a group of order 2, thus

$$\{\mathcal{O}\} \neq \mathrm{Ker}\, V_i \subset E_i[2],$$

where $E_i,\ i = 1, ..., N$, are the lifted curves.

The preceding can be visualized in the following diagram:



To proceed, we need the following lemma:

Lemma 2.3. *Let $\overline{E}/\mathbb{F}_{2^d}$ and assume that we have a curve E in characteristic 0, which reduces to $\overline{E}$ mod 2, such that Fr_{2^d} can be lifted to $\Sigma \in \mathrm{End}(E)$. Then $\mathrm{Tr}(\Sigma) = \mathrm{Tr}(\mathrm{Fr}_{2^d})$.*

Proof. $\Sigma \circ \Sigma - [\mathrm{Tr}(\Sigma)] \circ \Sigma + [2^d] = [0]$ in $\mathrm{End}(E)$, and by reducing we obtain the following equality: $\mathrm{Fr} \circ \mathrm{Fr} - [\mathrm{Tr}(\Sigma)] \circ \mathrm{Fr} + [2^d] = [0]$ in $\mathrm{End}(\overline{E})$. Therefore we get $[\mathrm{Tr}(\Sigma)] = [\mathrm{Tr}(\mathrm{Fr})]$, since $\mathrm{Fr} \circ \mathrm{Fr} - [\mathrm{Tr}(\mathrm{Fr})] \circ \mathrm{Fr} + [2^d] = [0]$ in $\mathrm{End}(\overline{E})$ as well, and $\mathrm{End}(\overline{E})$ is an integral domain. Thereby, $\mathrm{Tr}(\Sigma) = \mathrm{Tr}(\mathrm{Fr})$. □

Using this, we conclude that it is enough to find $c = \prod_{i=1}^{N} c_{1,i} \mod 2^M$ for some suitable M, where

$$\tau_{i-1} \circ V_i = \sum_{n=1}^{\infty} c_{n,i} \tau_i^n.$$

The squares of the $c_{1,i}$'s turn out to be rational functions of the lifted j-invariants and the x-coordinate of the nontrivial point in $\ker V_i$, which we will also show to be a rational function of the lifted j-invariants. Furthermore, these functions are nice, in the sense that the 2-valuation of their numerators and denominators are bounded.

We will now turn to the technical details.

3. Lifting the j-invariants

The first algorithm shows how to double the precision of the solution of

$$\begin{cases} \Phi_2(w_0, w_1) = \Phi_2(w_1, w_2) = \cdots = \Phi_2(w_{N-1}, w_0) = 0, \\ \overline{w_i} = j(\overline{E}_i), \ i = 0, \ldots, N-1. \end{cases}$$

It is a slight modification of [Sat00, Proposition 3.3].

Algorithm 3.1.
Input: *$z_0, \ldots, z_{N-1} \in R$, $z_N = z_0$ satisfying:*
(1) $z_i^2 \equiv z_{i+1} \mod 2$
(2) $\overline{z_i} \notin \mathbb{F}_4$
(3) $\Phi_2(z_i, z_{i+1}) \equiv 0 \mod 2^m$

for all $0 \leq i < N$, and for some $m \in \mathbb{N}$.
Output: *$\zeta_0, \ldots, \zeta_{N-1}$, unique modulo 2^{2m}, satisfying:*
(i) $\zeta_i \equiv z_i \mod 2^m$
(ii) $\Phi_2(\zeta_i, \zeta_{i+1}) \equiv 0 \mod 2^{2m}$

for all $0 \leq i < N$.

Method: *Define* $\mathcal{F}: R^N \to R^N$ *by*

$$\mathcal{F}((x_0 \ \dots \ x_{N-1})^t) := (\Phi_2(x_0, x_1) \ \Phi_2(x_1, x_2) \ \dots \ \Phi_2(x_{N-1}, x_0))^t,$$

and let $(D\mathcal{F})(x)$ *be its Jacobian matrix:*

$$\begin{pmatrix} \frac{\partial \Phi_2}{\partial X}(x_0, x_1) & \frac{\partial \Phi_2}{\partial Y}(x_0, x_1) & 0 & \dots & 0 \\ 0 & \frac{\partial \Phi_2}{\partial X}(x_1, x_2) & \frac{\partial \Phi_2}{\partial Y}(x_1, x_2) & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \frac{\partial \Phi_2}{\partial Y}(x_{N-2}, x_{N-1}) \\ \frac{\partial \Phi_2}{\partial Y}(x_{N-1}, x_0) & 0 & 0 & \dots & \frac{\partial \Phi_2}{\partial X}(x_{N-1}, x_0) \end{pmatrix}.$$

Then $(D\mathcal{F})(z)$ *is invertible over* $M_N(R)$*, and we take*

$$(\zeta_0 \ \dots \ \zeta_{N-1})^t = z + 2^m\delta \quad \text{with } \delta := -2^{-m}(D\mathcal{F})(z)^{-1}\mathcal{F}(z).$$

Running time: *The* ζ_i*'s are found for all* $0 \le i < N$ *with* $O(N)$ *operations over* $R \mod 2^{2m}$.

Proof. The ζ_i's clearly satisfy (i), provided $\delta \in R^N$. We use the Kronecker relation,

$$\Phi_2(X, Y) \equiv (X^2 - Y)(X - Y^2) \mod 2,$$

together with conditions (1) and (2), to achieve

$$(1) \qquad \frac{\partial \Phi_2}{\partial X}(z_i, z_{i+1}) \equiv z_i^2 - z_{i+1} \equiv 0 \mod 2,$$

$$(2) \qquad \frac{\partial \Phi_2}{\partial Y}(z_i, z_{i+1}) \equiv z_i - z_{i+1}^2 \equiv z_i + z_i^4 \not\equiv 0 \mod 2.$$

These equations assure that $(D\mathcal{F})(z)$ is invertible, so δ is in R.

Now for $z = (z_0 \ \dots \ z_{N-1})^t$, we have

$$\mathcal{F}(z + 2^m\delta) \equiv \mathcal{F}(z) + (D\mathcal{F})(z)2^m\delta \mod 2^{2m},$$

which shows that the ζ_i's satisfy (ii) and are unique mod 2^{2m}.

For the computational complexity, see [Sat00, proposition 3.3]. □

The next algorithm shows that the E_i's exist and describes how we can find the $j(E_i)$'s modulo arbitrary powers of 2.

Algorithm 3.2.
Input: *An integer* M *and an elliptic curve* $\overline{E}$ *with* $j(\overline{E}) \notin \mathbb{F}_4$.
Output: *Numbers* $\widetilde{w}_i$ *satisfying* $\widetilde{w}_i \equiv j(E_i) \mod 2^M$*, where* $E = E_0, E_1, ..., E_{N-1}$ *are representatives for the unique classes of curves satisfying the condition that the reduction of* E_i *is* $\overline{E}_i$ *and that there exists a 2-isogeny from* E_i *to* E_{i+1} *for all* $0 \le i < N$.
Method: *Let* $w_{0,i} \in R$ *be a lift of* $j(\overline{E}_i) = j(\overline{E})^{2^i} \in \mathbb{F}_{2^N} \setminus \mathbb{F}_4$*. Then* $w_{0,0}, ..., w_{0,N-1}$ *satisfy the conditions of Algorithm 3.1, with* $m = 1$.

Let $n = \lceil \log_2 M \rceil$*. For* $1 \le m \le n$ *we define* $w_{m,0}, ..., w_{m,N-1}$ *to be the output of Algorithm 3.1, with input* $z_i = w_{m-1,i}$*. We then define* $\widetilde{w}_i := w_{n,i}$.
Running time: *The* $\widetilde{w}_i$*'s are obtained for all* $0 \le i < N$ *with* $O(N \log M)$ *operations over* $R \mod 2^M$.

Proof. Using induction on m, we see that

(1) $w_{m,i}^2 \equiv w_{m,i+1} \mod 2$,
(2) $\overline{w_{m,i}} = \overline{w_{0,i}} \notin \mathbb{F}_4$,

(3) $\Phi_2(w_{m,i}, w_{m,i+1}) \equiv 0 \mod 2^{2^m}$,
(4) $w_{m+1,i} \equiv w_{m,i} \mod 2^{2^m}$,

for all $1 \leq m \leq n$.

Since $\Phi_2(X, Y)$ is continuous with respect to the 2-adic norm, the set of values $(w_i = \lim_{m\to\infty} w_{m,i})_{i=0}^{N-1}$ (which exist for all i by (4)) is a solution to the system of equations

$$\begin{cases} \Phi_2(w_0, w_1) = \Phi_2(w_1, w_2) = \cdots = \Phi_2(w_{N-1}, w_0) = 0, \\ \overline{w_i} = j(\overline{E}_i),\ i = 0, \ldots, N-1. \end{cases}$$

By the uniqueness part of the output of Algorithm 3.1, the w_i's are unique, and by the discussion in the preliminaries, the corresponding elliptic curves have the desired properties.

It also follows from (4) that $w_{n,i} \equiv j(E_i) \mod 2^{2^n}$.

It is easy to see that this algorithm uses at most $O(Nn)$ operations over R mod 2^{2^n}. □

Remark. Since the limits of the sequences are in K, the lifted curves will all be defined over K.

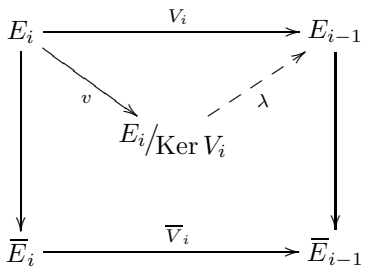
4. Finding the Squares of the $c_{1,i}$'s

The next step is to calculate the squares of the $c_{1,i}$'s, assuming that we are able to find the nontrivial point in $\operatorname{Ker} V_i$.

Proposition 4.1. *$c_{1,i}^2$ can be expressed as a rational function of $j(E_i)$ and the x-coordinate of the nontrivial point Q_i in $\operatorname{Ker} V_i$. Furthermore, the denominator has 2-valuation 0.*

Proof. As noted earlier, the rectangle in the following diagram is commutative.

(3)



We let $x(Q)$ (resp. $y(Q)$) denote the x- (resp. y-) coordinate of the point Q.

Let $v : E_i \to E_i/\operatorname{Ker} V_i$ be the isogeny constructed by Vélu [V71], which is explicitly given by

$$\begin{aligned} &v(X, Y) \\ &= \big(x(X, Y) + x((X, Y) + Q_i) - x(Q_i), y(X, Y) + y((X, Y) + Q_i) - y(Q_i)\big). \end{aligned}$$

Then $\operatorname{Ker} v = \operatorname{Ker} V_i$, which implies the existence of $\lambda \in \operatorname{Isog}(E_i/\operatorname{Ker} V_i, E_{i-1})$ making the triangle in the diagram commutative. Since $\deg(V_i) = \deg(v)\deg(\lambda)$, we see that $\deg(\lambda) = 1$, so λ is an isomorphism. We will now take a more careful look at λ.

According to [V71], a Weierstrass model of $E_i/\operatorname{Ker} V_i$ is given by

$$y^2 + xy = x^3 + A_i x + B_i,$$

where

$$A_i = -\frac{36}{j(E_i) - 1728} - 5t,$$
$$B_i = -\frac{1}{j(E_i) - 1728} - (1 + 7x(Q_i))t,$$

with

$$t := 3x(Q_i)^2 - \frac{36}{j(E_i) - 1728} - y(Q_i).$$

Since $2y(Q_i) + x(Q_i) = 0$, the formulas for A_i and B_i depend only on $j(E_i)$ and $x(Q_i)$.

Let λ be given by $\lambda(X, Y) = (u^2X + r, u^3Y + u^2sX + t)$. By letting $Z = \tau_i$ and looking at the Laurent series for X and Y,

$$X(Z) = Z^{-2} - b_1 Z^{-1} - b_2 \ldots,$$
$$Y(Z) = -Z^{-3} + b_1 Z^{-2} + \ldots,$$

we get

$$\hat{\lambda}(Z) = -\frac{u^2X(Z) + r}{u^3Y(Z) + u^2sX(Z) + t} = -\frac{u^2Z^{-2} - u^2b_1Z^{-1} - u^2b_2 + r - \ldots}{-u^3Z^{-3} + (u^3b_1 + u^2s)Z^{-2} + \ldots}$$
$$= -\frac{u^2Z - u^2b_1Z^2 - \ldots}{-u^3 + (u^3b_1 + u^2s)Z + \ldots} = -\frac{u^2(-u^3)}{(-u^3)^2}Z + O(Z^2) = \frac{1}{u}Z + O(Z^2).$$

Thus $c_{1,i} = \frac{1}{u}$, and all we need to do to find $c_{1,i}^2$ is to find u^2. Since λ is just a change of coordinates, we can find u^2 by solving the equations for a change of variables. This gives

$$u^2 = -\frac{48A_i - 1}{6 \cdot 12^2 B_i - 6 \cdot 12A_i + 1}.$$

Thus, we can calculate u^2 from A_i and B_i. Hence, ${c_{1,i}}^2$ is given by a rational function of $j(E_i)$ and $x(Q_i)$. Note that both the numerator and the denominator of u^2 have 2-valuation 0. □

Note that the formula for u^2 will always contain a factor 2^3 in front of $x(Q_i)$ and $y(Q_i)$, so we only need $\frac{x(Q_i)}{2}$ mod 2^{M-3} to get the square of the trace mod 2^M.

5. Finding $\operatorname{Ker} V_i$

Finally, we will show how to find the x-coordinate of the nontrivial point in $\operatorname{Ker} V_i$.

Lemma 5.1. *The x-coordinate of the the nontrivial point in $\operatorname{Ker} V_i$ is given by*

$$x = -2\frac{j(E_{i-1})^2 + 195120j(E_{i-1}) + 4095j(E_i) + 660960000}{8(j(E_{i-1})^2 - j(E_i)(512j(E_{i-1}) - 372735) + 563760j(E_{i-1}) + 8981280000)}.$$

The 2-valuation of the numerator and the denominator is 12.

Proof. Since $\operatorname{Ker} V_i \subset E_i[2]$, a nontrivial point $(x, y) \in \operatorname{Ker} V_i$ satisfies $2y + x = 0$. Squaring this gives $4y^2 + 4xy + x^2 = 0$, and using the equation for the curve, $y^2 + xy = x^3 - \frac{36}{j(E_i)-1728}x^2 - \frac{1}{j(E_i)-1728}$, we get the polynomial

$$4x^3 + x^2 - 4\frac{36}{j(E_i) - 1728}x - 4\frac{1}{j(E_i) - 1728} = 0.$$

Since λ in Diagram 3 is an isomorphism, the j-invariant of ${E_i}/{\operatorname{Ker} V_i}$ equals $j(E_{i-1})$; that is,

$$j(E_{i-1}) = \frac{(1 - 48A_i)^3}{(-(B_i - (A_i)^2) - 8(2A_i)^3 - 27(4B_i)^2 + 72A_iB_i)}.$$

This gives a sixth degree polynomial in $\frac{x}{2}$, with coefficients in $\mathbb{Z}[j(E_{i-1}), j(E_i)]$, which also has to be satisfied. Letting $z = \frac{x}{2}$, we get by carefully evaluating GCD's of the two resulting polynomials in z, and simplifying, that z must satisfy $az+b = 0$, where a and b are given by

$$\begin{aligned} a =& \ 8(j(E_{i-1})^2 - j(E_i)(512j(E_{i-1}) - 372735) + 563760j(E_{i-1}) + 8981280000) \\ b =& \ j(E_{i-1})^2 + 195120j(E_{i-1}) + 4095j(E_i) + 660960000. \end{aligned}$$

Since x has 2-valuation one, a and b must have the same 2-valuation. We investigate their values modulo 2^{13}:

$$\begin{aligned} a \equiv& \ 8(j(E_{i-1})^2 - j(E_i)(512j(E_{i-1}) - 4095) + 6704j(E_{i-1}) + 256) \mod 2^{13}; \\ b \equiv& \ j(E_{i-1})^2 + 6704j(E_{i-1}) + 4095j(E_i) + 4864 \mod 2^{13}. \end{aligned}$$

It is seen that $a \equiv 8b + 4096(j(E_i)j(E_{i-1}) + 1) \mod 2^{13}$, so $a \equiv 8b \mod 2^{12}$, and they both have to be zero mod 2^{12}. If they were both zero mod 2^{13}, then $0 \equiv j(E_i)j(E_{i-1}) + 1 \equiv j(E_{i-1})^3 + 1 \mod 2$; thus $\overline{j(E_{i-1})^4 - j(E_{i-1})} = 0$, which is not the case since $\overline{j(E_{i-1})} \notin \mathbb{F}_4$ by assumption. Therefore, $x = -2\,\frac{b}{a}$ gives the desired result. □

Note that this means that to get the value of $\frac{x}{2}$ modulo 2^M, we need the j-invariants mod 2^{M+12}.

6. Conclusion

Since the cost of a multiplication over $R \mod 2^N$ is $O(N^{2\log_2 3})$ when using the Karatsuba method [Knu98, p. 295], the computations of the lifted j-invariants modulo $2^{\frac{N+3}{2}+10}$ can be done in $O(N^{2\log_2 3+1}\log N)$ bit operations using Algorithm 3.2, and this can be reduced to $O(N^{2\log_2 3+1})$ by [Sat00, Remark 3.6]. With straightforward arithmetic it becomes $O(N^5)$.

Now we have given explicit formulas for finding $c^2 \mod 2^{\frac{N+3}{2}+1}$, and since $\operatorname{Tr}(\operatorname{Fr}_{2^N}) = c + \frac{q}{c}$ and $|\operatorname{Tr}(\operatorname{Fr}_{2^N})| \leq 2\sqrt{2^N}$, c modulo $2^{\frac{N+3}{2}}$ must be an integer. We can find it by inductive use of the following algorithm, starting with a solution mod 8 (which can easily be found).

Algorithm 6.1.
Input: *An integer n and elements $\alpha, \beta \in {\mathbb{Z}_2}^*$ such that $n \geq 3$ and $\beta^2 \equiv \alpha \bmod 2^n$.*
Output: *An element $\beta' \in {\mathbb{Z}_2}^*$, with $\beta^2 \equiv \alpha \mod 2^{2n-2}$ and $\beta' \equiv \beta \mod 2^{n-1}$.*
Method: *Take $\beta' = \beta - \frac{\frac{1}{2}(\beta^2-\alpha)}{\beta}$.*

Finally, we note that to satisfy the condition $\#\overline{E}(\mathbb{F}_{2^N}) \equiv 0 \mod 4$ we must have $\operatorname{Tr}(\operatorname{Fr}_{2^N}) \equiv 1 \mod 4$.

7. Example

In this section, we will give a small example to illustrate the method, and then we will discuss the performance of the algorithm for curves of cryptographic interest. Let $\overline{E}$ be the elliptic curve given by $y^2 + xy = x^3 + {}^1\!/\!_{(X^5+X+1)}$ defined over $\mathbb{F}_{2^7} = \mathbb{F}_2[X]/(X^7+X+1)$. Working modulo 2^{15}, which is needed to find the trace (this might seem ridiculously high, but note that the +10 has a big influence on these small numbers), we get the following lifted j-invariants:

$$\begin{aligned}
j(E_0) &= 7458X^6+15165X^5+28102X^4+13134X^3+2870X^2+16133X+30273,\\
j(E_1) &= 27342X^6+11862X^5+31943X^4+8739X^3+20969X^2+22810X+505,\\
j(E_2) &= 31767X^6+13154X^5+17419X^4+24778X^3+8797X^2+22389X+8979,\\
j(E_3) &= 1183X^6+25617X^5+18181X^4+8360X^3+5160X^2+32737X+10851,\\
j(E_4) &= 9147X^6+6081X^5+1001X^4+3855X^3+21694X^2+29887X+8315,\\
j(E_5) &= 3812X^6+7433X^5+28447X^4+7067X^3+1334X^2+4163X+31829,\\
j(E_6) &= 17595X^6+18992X^5+5979X^4+32371X^3+4712X^2+2953X+10875.
\end{aligned}$$

The halves of the x-coordinates modulo 2^3 are calculated to be:

$$\begin{aligned}
z_0 &= 6X^6+7X^5+4X^3+6X^2+1,\\
z_1 &= 6X^5+7X^4+7X^3+4X^2+4X+5,\\
z_2 &= X^6+4X^5+2X^4+6X^3+7X^2+X+7,\\
z_3 &= 5X^6+7X^5+5X^4+2X^3+5X^2+2X+7,\\
z_4 &= 7X^6+3X^5+6X^4+3X^3+X^2+7X+3,\\
z_5 &= X^5+5X^3+5X^2+2X+5,\\
z_6 &= 5X^6+4X^5+4X^4+5X^3+4X^2+7.
\end{aligned}$$

Now the square of the trace is computed to be $c^2 \equiv 9 \mod 64$, and the two square roots mod 32 are ± 3; thus $\mathrm{Tr}(\mathrm{Fr}_{2^7}) = -3$, since it should be 1 modulo 4, and the number of points on the curve is $2^7 + 1 + 3 = 132$, whereas the number of points on its twist is $2^7 + 1 - 3 = 126$.

For cryptographic applications the size of the prime dividing the group order should have approximately 50 digits. When searching for such a curve, one can choose j-invariants at random from a field of size approximately 2^{200}, and examine the two possible group orders for prime factors greater than, for example, 80% of the field size. This has been implemented with some optimizations, and run on a 32-bit 866 MHz (Pentium III) processor.

We evaluate the performance of our algorithm by finding 5 curves satisfying the above condition for different field sizes. The following table shows the average running time per j-invariant (i.e., the time for finding the trace, but not including the time for checking the prime factors of the two group orders), the average number of j-invariants that we tried before finding one giving a suitable curve, the maximal number of j-invariants tried, and the average number of curves we checked (e.g., if the twisted curve in the last try was the one we could use, the number of curves checked is twice the number of the j-invariants; otherwise it is twice this number minus 1). Between 3 and 5.2 MB of memory was used.

Field size	avg Time/s	avg #j-inv	max #j-inv	avg #curves
163	5.74	1.6	3	3.0
167	5.95	1.8	2	3.2
173	7.84	3.8	11	7.0
179	9.10	2.4	5	4.6
181	9.38	3.2	6	5.8
191	10.40	1.6	4	2.4
193	10.78	1.6	2	2.6
197	11.65	1.6	3	2.6
199	11.93	4.4	8	8.6
211	13.91	2.2	5	3.8
223	15.85	2.4	6	4.6
227	16.81	1.8	2	3.2
229	17.22	4.0	8	7.2

Only the average time for counting has been included in the table, since the ratio (max time)/(min time) is less than 1.03 in all the tested cases; thus fluctuations in the running times are very small. For the last column, note that a randomly chosen number has approximately 20% chance of having a prime divisor of bit size greater than 80% of its own size (see e.g., [Knu98, p.383]); thus we would expect to find a suitable curve in about 5 tries on average. So on average very few j-invariants have to be tested, and one would be unlucky not to get a good cryptographic curve in a minute.

Remarks

An independent and different generalization of Satoh's algorithm has been made and implemented by Mireille Fouquet, Pierrick Gaudry, Robert Harley and François Morain [GH00], with amazing results. They have used it to count the number of points on an elliptic curve over $\mathbb{F}_{2^{8009}}$ in 13 days, using a 750 MHz Alpha EV6 and 16.9 GB of memory. The old record was 65 days for a 1999-bit curve. In this case, their algorithm took 14 hours on a 500 MHz Alpha EV6. For more information see their homepage:

`http://www.lix.polytechnique.fr/Labo/Mireille.Fouquet/elliptic.html`

A demo-version in an unoptimized environment of the algorithm described in this paper can be found at:

`http://www.cryptomathic.com`

Acknowledgments

I would like to thank my advisor Peter Landrock for proposing the problem to me, as well as the CRYPTOMAThIC EC team for implementing the algorithm, Jørgen Tornehave for discussions on parts of the theory, René Schoof for suggesting that the canonical lift could be avoided, and Steven Galbraith for many helpful comments on previous versions of this paper. I am especially grateful to Takakazu Satoh, who found the algorithm upon which the current work is based, and who took the time to answer a great number of questions and to read previous versions of this paper. His help has been very valuable.

References

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1993. MR **94i:**11105

[Eng99] Andreas Enge, *Elliptic curves and their applications to cryptography*, Kluwer Academic Publishers, 1999.

[GH00] Mireille Fouquet, Pierrick Gaudry and Robert Harley, *An extension of Satoh's algorithm and its implementation*, J. Ramanujan Math. Soc. **15** (2000), no. 4, 281–318. CMP 2001:05

[Knu98] Donald E. Knuth, *Seminumerical algorithms*, 3 ed., The art of computer programming, vol. 2, Addison-Wesley, 1998. MR **83i:**68003 (2nd ed.)

[Kob87] Neal Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209. MR **88b:**94017

[Lan87] Serge Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics, Springer-Verlag, New York, 1987. MR **88c:**11028

[Mil86] Victor Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology—CRYPTO'85, Lecture Notes in Computer Science **218** (1986), 417–426. MR **88b:**68040

[Sat00] Takakazu Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), no. 4, 247–270. MR **2001j:**11049

[Sch85] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494. MR **86e:**11122

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1986. MR **87g:**11070

[V71] Jacques Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris **273** (1971), 238–241. MR **45:**3414

University of Aarhus, Department of Mathematics, Ny Munkegade, 8000 Aarhus C, Denmark

E-mail address: skjernaa@imf.au.dk