ALGORITHMS FOR COMPUTING ISOGENIES BETWEEN ELLIPTIC CURVES

R. LERCIER AND F. MORAIN

Abstract. The efficient implementation of Schoof's algorithm for computing the cardinality of elliptic curves over finite fields requires the computation of isogenies between elliptic curves. We make a survey of algorithms used for accomplishing this task. When the characteristic of the field is large, Weierstrass's $\wp$ functions can be used. When the characteristic of the field is small, we now have three algorithms at our disposal, two due to Couveignes and one to the first author. We treat the same example using these three algorithms and make some comparisons between them.

1. Introduction

The motivation for this article is the so-called Schoof-Elkies-Atkin algorithm that computes the cardinality of an elliptic curve over any finite field. The improvements due to Elkies and Atkin require the ability to compute isogenies of prime degree ℓ between elliptic curves. The first method for doing this uses the Weierstrass's parametrization of elliptic curves and cannot work when the characteristic p of the field is smaller than ℓ. Couveignes developed a particular algorithm for the case $p \ll \ell$ in his thesis [7]. Following the implementation of Couveignes's algorithm for the case $p = 2$ (cf. [17, 16]), the first author worked out a new algorithm for this case [14]. Very recently, Couveignes [8], building on some of the ideas of [16] and [14], gave a new method using the properties of the p-torsion points.

One of the purposes of this paper is to compare these last three methods on a particular example. Before doing this, we need to recall some basic facts about elliptic curves, Schoof's algorithm and isogenies. We take the opportunity of this paper to present a new record for computing the number of points in characteristic 2, namely the cardinality of a curve defined over $\mathbb{F}_{2^{1301}}$.

2. Background on elliptic curves

The reference for what follows is [22]. Let $\mathbb{K}$ be a field and $E/\mathbb{K}$ be an elliptic curve of equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

and let as usual

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Since E is an elliptic curve, one has $\Delta \neq 0$ and the j-invariant of the curve is $j(E) = c_4^3/\Delta$. We will note O_E the neutral element of the group law on E. See the reference for the precise equations of the law.

Let m be any integer and let $\psi_m(X, Y)$ denote the m-th division polynomial, which satisfies the following formulas:

$$\psi_0 = 0, \psi_1 = 1, \psi_2 = 2Y + a_1X + a_3;$$

Date: Preliminary version, May 9, 1996.
The second author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.
The second author wants to thank the Newton Institute for its hospitality during the writing of this article.

$$\psi_3 = 3X^4 + b_2X^3 + 4b_4X^2 + 3b_6X + b_8;$$
$$\psi_4 = \psi_2\left(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\right);$$
$$\psi_2\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), m \geq 2;$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2.$$

We let $\psi'_m(X)$ denote $\psi_m(X,Y)$ reduced in $\mathbb{K}[X,Y]/(\mathcal{F}(X,\,Y,1))$. When m is even we let $f_m = \psi'_m/(2Y + a_1X + a_3)$ and if m is odd, then $f_m = \psi'_m$. If m is even, f_m has degree $(m^2-4)/2$ and leading coefficient $m/2$; if m is odd, f_m has degree $(m^2-1)/2$ and leading coefficient m.

Define $E[m] = \{P \in E(\overline{\mathbb{K}}), mP = O_E\}$. The principal property of $E[m]$ is the following.

Theorem 2.1. *Let $P = (X,Y) \in E(\overline{\mathbb{K}})$ such that $2P \neq O_E$. Then $P \in E[m]$ if and only if $f_m(X) = 0$.*

3. Counting points on elliptic curves over finite fields

We concentrate here on Schoof's algorithm, which runs in polynomial time. For other algorithms that are not polynomial time, but are useful in some cases, see for instance [6].

3.1. **Schoof's algorithm.** Let $\mathbb{K}$ a finite field of characteristic p and cardinality $q = p^n$. We begin with the following well known result.

Theorem 3.1. *Let ϕ denote the Frobenius of $E/\overline{\mathbb{K}}$, i.e., the map sending (X,Y) to (X^q, Y^q). The characteristic equation of ϕ is*

$$\pi^2 - c\pi + q = 0 \tag{1}$$

where c is an integer $|c| \leq 2\sqrt{q}$. Moreover $\#E(\mathbb{K}) = q + 1 - c$.

Schoof's algorithm for computing $\#E(\mathbb{K})$ consists in using equation (1) on the ℓ-torsion points of E, for sufficiently many primes ℓ. More precisely, for fixed ℓ, he looks for γ, $0 \leq \gamma < \ell$ such that

$$(X^{q^2}, Y^{q^2}) \oplus [q](X,Y) = [\gamma](X^q, Y^q)$$

in $E[\ell] \simeq \mathbb{K}[X,Y]/(E, f_\ell)$. Once γ is found, we have $c \equiv \gamma \bmod \ell$. If we do this for all primes ℓ such that $\prod_\ell \ell > 4\sqrt{q}$, then we can recover c using the Chinese Remainder Theorem.

It is clear that this algorithm has polynomial running time. However, the size of the polynomials is too large for computations, since f_ℓ has degree $O(\ell^2)$. The main improvement of Elkies to this algorithm is to replace f_ℓ, which is the denominator of an isogeny of degree ℓ^2, by a polynomial g_ℓ coming from an isogeny of degree ℓ.

3.2. **The role of isogenies.** Let $\ell \neq p$ be a prime number. Let F be any of the $\ell + 1$ cyclic subgroups of $E[\ell]$ and denote by E^* the elliptic curve E/F. There is an isogeny I of degree ℓ between E and E^* and we note I^* the dual isogeny:

$$\begin{tikzcd} E \arrow[rr, "{[\ell]}"] \arrow[dr, "I"'] & & E \\ & E^* \arrow[ur, "I^*"'] & \end{tikzcd}$$

The invariant of E^* satisfies

$$\Phi_\ell(j(E^*), j(E)) = 0$$

in $\mathbb{K}$, where $\Phi_\ell(X,Y)$ is the ℓ-th modular polynomial (see for instance [13]). In turn, if this equation has a rational root, then there is an F such E/F (as well as I) is defined over $\mathbb{K}$. The denominator of I will give us a factor of f_ℓ, since $[\ell] = I^* \circ I$.

Elkies remarked that if $t^2 - 4q$ is a square modulo ℓ, then the restriction of ϕ to $E[\ell]$ has two rational eigenspaces, which are rational cyclic subgroups of $E[\ell]$. In that case, we can build an isogeny as indicated above. This phenomenon happens probabilistically for half the prime numbers ℓ. This turns Schoof's algorithm in a probabilistic polynomial time algorithm. More important, this makes it efficient in practice.

We will explain how to build the pair (E^*, I) in the following sections.

4. Vélu's formulas

Given E and F, computing an isogeny I of kernel F can be done using Vélu's formulas [24]. After recalling these, we will rewrite them in a more useful form as Dewaghe did [9].

Suppose that ℓ is an odd integer and put $d = (\ell - 1)/2$. Then, we can write $F - \{0\} = R \cup (-R)$ with $R \cap -R = \emptyset$. For $Q \in R$, let

$$\left\{\begin{array}{lcl} g_Q^x &=& 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q, \\ g_Q^y &=& -2y_Q - a_1x_Q - a_3, \\ u_Q &=& 4x_Q^3 + b_2x_Q^2 + 2b_4x_Q + b_6, \\ t_Q &=& 6x_Q^2 + b_2x_Q + b_4. \end{array}\right.$$

Theorem 4.1 (Vélu). *An isogeny $I : E \to E^* = E/F$ sending (X, Y) to (X^*, Y^*) is given by*

$$X^* = X + \sum_{Q \in R} \left(\frac{t_Q}{X - x_Q} + \frac{u_Q}{(X - x_Q)^2} \right),$$

$$Y^* = Y - \sum_{Q \in R} u_Q \frac{2Y + a_1X + a_3}{(X - x_Q)^3} + t_Q \frac{a_1(X - x_Q) + Y - y_Q}{(X - x_Q)^2} + \frac{a_1u_Q - g_Q^x g_Q^y}{(X - x_Q)^2}.$$

Letting

$$t = \sum_Q t_Q, \quad w = \sum_Q (u_Q + x_Q t_Q),$$

the equation of E^* is

$$Y^{*2} + a_1^* X^* Y^* + a_3^* Y^* = X^{*3} + a_2^* X^{*2} + a_4^* X^* + a_6^*$$

with $a_1^* = a_1$, $a_2^* = a_2$, $a_3^* = a_3$ and

$$a_4^* = a_4 - 5t, \quad a_6^* = a_6 - b_2 t - 7w.$$

Our task is to rewrite these equations in term of the polynomial

$$H(X) = \prod_{Q \in R} (X - x_Q) = X^d - h_1X^{d-1} + h_2X^{d-2} - h_3X^{d-3} + \cdots + (-1)^d h_0.$$

First of all, we have to evaluate:

$$S_1 = \sum_Q x_Q, S_2 = \sum_Q x_Q^2, S_3 = \sum_Q x_Q^3,$$

$$\Sigma_1 = \sum_Q \frac{1}{X - x_Q}, \Sigma_2 = \sum_Q \frac{1}{(X - x_Q)^2}, \Sigma_3 = \sum_Q \frac{1}{(X - x_Q)^3}.$$

Lemma 4.1. *We have*

$$S_1 = h_1,\ S_2 = h_1^2 - 2h_2,\ S_3 = h_1^3 - 3h_1h_2 + 3h_3;$$

$$\Sigma_1 = \frac{H'}{H}, \Sigma_2 = -\left(\frac{H'}{H}\right)'.$$

When $\mathrm{char}(\mathbb{K}) \neq 2$,

$$\Sigma_3 = \frac{1}{2} \left(\frac{H'}{H}\right)''$$

and when $\mathrm{char}(\mathbb{K}) = 2$, *we must use*

$$\Sigma_3 = \frac{1}{H^3}\left(H^2\frac{H^{(3)}}{2} + HH'\frac{H''}{2} + H'^3\right)$$

where the derivatives of H *are taken over* $\mathbb{Q}$, *divided by* 2 *and then reduced modulo* 2.

(Note that the formula for Σ_3 boils down to extracting some precise coefficients of H.)

From this, it easily follows that

$$\begin{cases} t &= 6S_2 + b_2S_1 + b_4d, \\ w &= 10S_3 + 2b_2S_2 + 3b_4S_1 + b_6d \end{cases}$$

which give us the coefficients of E^*.

Decomposing the rational fractions and collecting the terms together, we can rewrite the X^* formula as

$$X^* = X + 2dX - 2h_1 - (6X^2 + b_2X + b_4)\Sigma_1 + (4X^3 + b_2X^2 + 2b_4X + b_6)\Sigma_2.$$

Let us turn our attention to the case of Y^*. It is convenient to put $f = X^3 + a_2X^2 + a_4X + a_6$ and $A = a_1X + a_3$. Differentiating X^* w.r.t. X, we can write

$$\begin{aligned} Y^* = Y\,\frac{\partial X^*}{\partial X} &+ \sum_Q \left(-a_3 - a_1x_Q + \frac{c_1}{X - x_Q} + \frac{c_2}{(X-x_Q)^2} + \frac{c_3}{(X-x_Q)^3}\right) \\ &= Y\,\frac{\partial X^*}{\partial X} - a_3d - a_1S_1 + c_1\Sigma_1 + c_2\Sigma_2 + c_3\Sigma_3 \end{aligned}$$

with

$$\begin{aligned} c_1 &= Af'' - A'f', \\ c_2 &= -\left(A'(A^2 - 2f) + 3Af'\right), \\ c_3 &= A(4f + A^2). \end{aligned}$$

Note that when $a_1 = a_3 = 0$, one has $A = 0$ and so Y^* is simply $Y\dfrac{\partial X^*}{\partial X}$.

An easy consequence of the above formulas is the following:

Proposition 4.1. *The isogeny* I *of degree* ℓ *sending* (X, Y) *to* (X^*, Y^*) *can be written as*

$$I(X,Y) = \left(\frac{G(X)}{H(X)^2}, \frac{J(X,Y)}{H(X)^3}\right),$$

where $G(X)$ *is of degree* ℓ *and* $H(X)$ *is of degree* $(\ell - 1)/2$.

5. Using Weierstrass's $\wp$ function

Assume for the moment that $\mathbb{K} = \mathbb{C}$. In this case, we can use the modular interpretation of elliptic curves. More precisely, we can use the Weierstrass's parametrization for $E : Y^2 = X^3 + AX + B$ viewing E as $\mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z})$ where $\tau = \omega_2/\omega_1$ has positive imaginary part. The Weierstrass function of E is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} w_k(E)z^{2k}$$

where $w_k(E) \in \mathbb{Z}[A, B, 1/(2k+4)!]$. We have also $j(E) = j(\tau) = 1/q + \sum_{n=1}^{\infty} c_nq^n$, $q = \exp(2i\pi\tau)$.

Remember that we are looking for one isogeny of degree ℓ. Let F consist of the point at infinity and the points of abscissa $\wp(r\omega_1/\ell)$, $1 \le r \le (\ell-1)/2$. The curve E^* is in fact $\mathbb{C}/(\omega_1/\ell, \omega_2)$. It can be shown that the coefficients of E^* can be deduced in a rational way from that of E (see [21] for instance). The functions $\wp$ and $\wp^*$ are related via

$$\wp^*(z) = I(\wp(z)).$$

At this point, we can find the isogeny I using Stark's method [23], i.e., developping the Weierstrass' function of E^* as a continued fraction in that of E. Since we know the degree of the fraction, this works well. Alternatively, we can turn Vélu's formulas into recurrence relations for the denominator of I, which is really what we are looking for.

We need about ℓ coefficients of $\wp$ and $\wp^*$ to be able to perform the computations. Therefore, the method works as well when $\mathrm{char}(\mathbb{K}) > 0$, provided $\mathrm{char}(\mathbb{K}) > 3$ and $\mathrm{char}(\mathbb{K}) \gg \ell$. Computing I takes $O(\ell^2)$ operations and uses $O(\ell)$ memory. We refer to [2, 10, 5, 3, 21, 19, 20] for more details. The method is very efficient in practice and the record is the computation of the cardinality of a curve modulo a prime of 500 decimal digits [19].

6. The small characteristic case

6.1. The problems to be solved. We assume from now on that $\mathbb{K}$ is a finite field of characteristic p and cardinality $q = p^n$. We suppose we are given E for which there exists a rational ℓ-isogeny and that $p \ll \ell$, so that will include $\mathrm{char}(\mathbb{K}) = 2, 3$ in particular. In this case, we have no valid modular representation, which means that we have no candidate for F. Still, we can find the invariant of E^* by solving $\Phi_\ell(X, j(E)) = 0$ in $\mathbb{K}$. Once we know $j(E^*)$, we need to find the isogeny class of E^* and the equation for I. The first task will be accomplished using the Hasse invariant and for the second, we will describe three algorithms in the subsequent sections. Note that we already know the form of I:

$$I(X) = \frac{G(X)}{H(X)^2}$$

where G and H are two polynomials of respective degree ℓ and $(\ell - 1)/2$.

For solving the first task, we introduce the formal group associated to an elliptic curve. This in turn will be used in Couveignes's first algorithm.

6.2. Formal group. The material below is taken from [22, Chap. IV].

Let E be our elliptic curve and let us make the change of variables $t = -X/Y$ and $s = -1/Y$. This transforms the equation of E as:

$$s = A(t, s) = t^3 + a_1 ts + a_2 t^2 s + a_3 s^2 + a_4 t s^2 + a_6 s^3.$$

This amounts to sending the point at infinity on the point $(0, 0)$. Substituting this equation into itself, we get s as a power series in t, that we will note $\mathcal{S}$, the first coefficients of which are:

$$\mathcal{S}(t) = \sum_{i=3}^{\infty} s_i t^i = t^3 + a_1\, t^4 + (a_1^2 + a_2) t^5 + O(t^6). \tag{2}$$

Using this relation, we see that a point in the formal group is completely characterized by its abscissa. Note also that, given any t on $\mathcal{E}$, we can compute $\mathcal{S}(t)$ by the same iterative process. From this, we get

$$Y = -\frac{1}{s} = -t^{-3} + a_1 t^{-2} + a_2 t^{-1} + a_3 + (a_1 a_3 + a_4) t + O(t^2),$$

and

$$X = \frac{t}{s} = -tY = t^{-2} - a_1 t^{-1} - a_2 - a_3 t - (a_1 a_3 + a_4) t^2 + O(t^3),$$

$$Z = \frac{1}{X} = t^2 + a_1 t^3 + (a_1^2 + a_2) t^4 + O(t^5).$$

Letting t be any formal series in $k[[\tau]]$, with strictly positive valuation, we can compute a series $s \in k[[\tau]]$ such that $s(\tau) = A(t(\tau), s(\tau))$. In this way, we get *formal points* $(t(\tau), s(\tau))$ on the formal curve $\mathcal{E}$ of equation $s - A(t, s) = 0$. Since this is again the equation of a cubic, we see that we can put a tangent-and-chord law on $\mathcal{E}$, thus building what is called the *formal group* associated to E.

Equations for this law are to be found in the reference given. The sum of t_1 and t_2 in this group will give us $t_3 = F_a(t_1, t_2)$. The first terms are:

(3) $\quad F_a(t_1,t_2) = t_1 + t_2 - a_1 t_1 t_2 - a_2(t_1^2 t_2 + t_1 t_2^2) - (2a_3 t_1^3 t_2 - (a_1 a_2 - 3a_3) t_1^2 t_2^2 + 2a_3 t_1 t_2^3) + \cdots$

Iterating this law, we get multiplication by m. A very important particular case is when $m = p$:

Theorem 6.1. *If E is not supersingular, then there exists a series $\Psi_{p,E}(t)$ such that*

$$[p](t) = \Psi_{p,E}(t)^p = c_p(E)t^p + O(t^p).$$

The number $c_p(E)$ is called the *Hasse invariant* of the curve and it has the very important property that

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{F}_p}(c_p(E)) \equiv \mathrm{Tr}(\phi) \bmod p$$

so that two isogenous curves have the same Hasse invariant, up to multiplication by the $(p-1)$-th power of an element of $\mathbb{F}_p$. Without loss of generality, we will build our curve E^* in such a way that this element is taken to be 1, so that the isogeny class of E^* will be found by imposing $c_p(E^*) = c_p(E)$.

7. The first algorithm of Couveignes

7.1. **Presentation of the algorithm.** What follows is part of Couveignes's thesis [7]. A complete version of it is given in [16], which also contains the first detailed implementation of it (see also [17]).

We look at the abscissa of the isogeny $I : E \to E^*$, where E^* has the same Hasse invariant as E (see the preceding section). It is equivalent to search for G and H of respective degree ℓ and $(\ell-1)/2$ such that

$$I : X \mapsto X^* = I(X) = \frac{G(X)}{H(X)^2}$$

or for $\hat{I}$ which sends $Z = 1/X$ to $Z^* = 1/X^*$, that is

$$\hat{I} : Z \mapsto Z^* = \hat{I}(Z) = Z\frac{\hat{H}^2(Z)}{\hat{G}(Z)}$$

with $\hat{G}(Z) = Z^\ell G(1/Z)$ and $\hat{H}(Z) = Z^{(\ell-1)/2} H(Z)$. It is well known that the coefficients of the expansion of a rational fraction $F(Z)$ with denominator of degree ℓ around $Z = 0$ satisfy a recurrence relation of depth ℓ. Reciprocally, given the 2ℓ first coefficients, one can recover $F(Z)$ exactly using for example the Berlekamp-Massey algorithm [18]. Couveignes's idea is just this: finding a series that looks like an isogeny and then check whether it comes from a fraction whose denominator has degree ℓ. In fact, we compute $2\ell+2$ terms of the isogeny, thus obtaining in general a fraction with denominator of degree *a priori* $\ell+1$. If this denominator turns out to have degree ℓ, then we are almost sure to have the right isogeny.

7.1.1. *Finding morphisms.* We will enumerate the putative isogenies the formal groups $\mathcal{E}$ and $\mathcal{E}^*$ associated to E and E^*:

$$\begin{array}{rrcl} \mathcal{E}: & t^3 + a_1 ts + a_2 t^2 s + a_3 s^2 + a_4 ts^2 + a_6 s^3 - s & = & 0, \\ \mathcal{E}^*: & t^3 + a_1^* ts + a_2^* t^2 s + a_3^* s^2 + a_4^* ts^2 + a_6^* s^3 - s & = & 0. \end{array}$$

We will write $\Psi(t)$ (resp. $\Psi^*(t)$) for $\Psi_{p,E}(t)$ (resp. $\Psi_{p,E^*}(t)$); we put also $c = c_p(E) = c_p(E^*)$ (see the discussion after Theorem 6.1). Our isogeny $\hat{I}$ is characterized by a series $\mathcal{I}$

$$Z^*(t) = \hat{I}(Z(t)) = \mathcal{I}(t) = \sum_{i=1}^{\infty} \alpha_i t^i$$

where $\alpha_i \in \mathbb{K}$.

The series $\mathcal{I}$ is an example of a morphism of formal groups. Generally speaking, such a morphism is given by $\mathcal{M}$ such that for all formal points $(t_1(\tau), s_1(\tau))$ and $(t_2(\tau), s_2(\tau))$ of $\mathcal{E}$:

$$\mathcal{M}((t_1(\tau), s_1(\tau)) \oplus (t_2(\tau), s_2(\tau))) = \mathcal{M}((t_1(\tau), s_1(\tau))) \oplus \mathcal{M}((t_2(\tau), s_2(\tau))).$$

Associated to $\mathcal{M}$, there is a series

$$\mathcal{U}(t) = \sum_{i \geq 1} u_i t^i,$$

such that a point $(t(\tau), s(\tau))$ of $\mathcal{E}$ is sent to the point $\mathcal{M}(t(\tau), s(\tau)) = (\mathcal{U}(t(\tau)), \mathcal{S}^*(\mathcal{U}(t(\tau))))$ of $\mathcal{E}^*$ ($\mathcal{S}^*$ is defined by (2)). *A fortiori*, the series $\mathcal{U}(t)$ satisfies

$$\mathcal{U}(t_1 \oplus t_2(\tau)) = \mathcal{U}(t_1(\tau)) \oplus \mathcal{U}(t_2(\tau)) \tag{4}$$

from which $\mathcal{U} \circ [n] = [n] \circ \mathcal{U}$ for any integer n. We know also that the set of morphisms from $\mathcal{E}$ to $\mathcal{E}^*$ is a $\mathbb{Z}_p$-module of rank 1 (see [11]).

The problem is now the following: among all morphims between $\mathcal{E}$ and $\mathcal{E}^*$, determine which is the one coming from $\mathcal{I}$, or equivalently, among all series satisfying (4), determine which is the one coming from $\hat{I}$.

Since $2\ell + 2$ terms of $\hat{I}(Z)$ are needed, and since $Z = 1/X = s/t = t^2 + O(t^3)$, this means that we need $\mathcal{L} = 4\ell + 2$ terms of the series $\mathcal{W}$ associated to $\mathcal{I}$. In other words, we need to consider a finite number of series in order to find the good one.

Since the set of morphisms has dimension 1, it is enough to find a generator, and any non-trivial morphism will do. We will compute the first $\mathcal{L}$ coefficients of our candidate

$$\mathcal{U}(t) = \sum_{i=1}^{\infty} u_i t^i$$

by induction. Starting from $u_1 = 1$, we find u_i by equating the coefficients of τ^i in

$$\mathcal{U}(\tau \oplus A\tau) = \mathcal{U}(\tau) \oplus \mathcal{U}(A\tau) \tag{5}$$

when i is not a power of p and the coefficients of τ^{ip} in

$$\mathcal{U}([p]\tau) = [p](\mathcal{U}(\tau))$$

otherwise. The first equation is linear in u_i and the second has in general p solutions.

7.1.2. *Enumerating all morphisms.* We now use the fact that the set of morphisms between $\mathcal{E}$ and $\mathcal{E}^*$ is a $\mathbb{Z}_p$-module of dimension 1. Let $\mathcal{U}$ be any non-trivial morphism found as in the preceding section. There exists a p-adic integer N such that $\mathcal{W} = [N] \circ \mathcal{U}$. Write

$$N = \sum_{i=0}^{\infty} n_i p^i.$$

Remembering that $p^r < \mathcal{L} < p^{r+1}$, we write

$$[N] \circ \mathcal{U} = \bigoplus_{i=0}^{r} \left([n_i] \circ ([p^i] \circ \mathcal{U})\right) \oplus \bigoplus_{i>r} \left([n_i] \circ ([p^i] \circ \mathcal{U})\right).$$

But the valuation of the series $[p^i](t)$ is p^i, which implies that, when $i > r$, the terms coming from $[p^i] \circ \mathcal{U}$ do not provide any contribution to the first $\mathcal{L}$ coefficients of $[N] \circ \mathcal{U}$. So, it is enough to check whether one of the series $[N] \circ \mathcal{U}$ comes from an isogeny for $N < p^{r+1}$. Moreover, n_0 cannot be 0.

7.1.3. *The algorithm in brief.* We summarize Couveignes's algorithm:
procedure ComputeIsogeny($\mathcal{E}$, ℓ, $\mathcal{E}^*$)

1. compute a generator $\mathcal{U}$ of the set of morphisms between $\mathcal{E}$ and $\mathcal{E}^*$;
2. **for** $N = 1$ to $p^{r+1}/2$ and N prime to p **do**
   (a) compute $(\mathcal{M}(t), \mathcal{S}^*(\mathcal{M}(t))) = [N] \circ (\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t)))$;
   (b) test whether $\mathcal{M}$ comes from isogeny; if yes, stop.

7.1.4. *Remarks on the implementation.* The computations required by the above algorithm deal with series computations over $\mathbb{K}$. The series involved have a lot of terms (if $\ell = 300$, then the number of terms is 1200). The algorithm can be made very fast if one uses a fast incremental for composition of series, as done in [16]. When this is done, we actually get:

Theorem 7.1. *Couveignes's algorithm has running time $O(\ell^3)$. The storage is $O(\ell^2)$.*

The record obtained with this implementation is for 2^{1009}, see [17].

7.2. **A numerical example.** We will compare all the algorithms on the following example. Let $\mathbb{K} = \mathbb{F}_{2^{11}} = \mathbb{F}_2[T]/(T^{11} + T^2 + 1)$,

$$E : Y^2 + XY = X^3 + a, E^* : Y^2 + XY = X^3 + b$$

with $a = T^4 + T^2 + T$, $b = T^{10} + T^9 + T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$ and we suppose that there is a rational isogeny of degree $\ell = 5$ between E and E^*. Note that for simplification, we will write any element of $\mathbb{K}$ as an overlined number. More precisely, if $x = x(T)$ is an element of $\mathbb{K}$, we will write x as $\overline{x(2)}$. For instance

$$a = T^4 + T^2 + T = \overline{22}.$$

We know that the isogeny I we are looking for can be written as

$$I(X) = \frac{G(X)}{H(X)^2}$$

where $G(X)$ has degree $\ell = 5$ and $H(X)$ has degree $(\ell - 1)/2 = 2$.

First of all, we choose $A = \overline{2}$. The algorithm consists in building a morphism between the two formal groups $s + t^3 + ts + as^3 = 0$ and $s + t^3 + ts + bs^3 = 0$. We look for a morphism $\mathcal{U}$ as a series in t. We will find the coefficients of $\mathcal{U}$ step by step. We initialize:

$$(\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t))) = (t + O(t^2), t^3 + O(t^4)).$$

We find u_2 by solving $\mathcal{U}([2]t) = [2]^*(\mathcal{U}(t))$, which leads to

$$\sqrt{u_2}^2 + \sqrt{u_2} = 0.$$

We take $u_2 = 0$.

For u_3, we solve $\mathcal{U}(t \oplus At) = \mathcal{U}(t) \oplus \mathcal{U}(At)$ which yields the unique value $u_3 = 0$. The case of u_4 ressembles that of u_2:

$$\sqrt{u_4}^2 + \sqrt{u_4} + \overline{1194} = 0.$$

and we take $u_4 = \overline{1820}$.

Eventually, we come up with

$$\begin{aligned}\mathcal{U}(t) = t &+ \overline{1820}t^4 + \overline{1820}t^5 + \overline{1641}t^7 + \overline{1280}t^8 + \overline{873}t^9 + \overline{783}t^{10} + \overline{1746}t^{11} + \overline{360}t^{12} + \overline{884}t^{13} + \overline{1082}t^{14} \\ &+ \overline{987}t^{15} + \overline{522}t^{16} + \overline{1556}t^{17} + \overline{1365}t^{18} + \overline{171}t^{19} + \overline{702}t^{20} + \overline{62}t^{21} + O(t^{22}),\end{aligned}$$

and

$$\begin{aligned}\mathcal{S}(\mathcal{U}(t)) = t^3 &+ t^4 + t^5 + \overline{1821}t^6 + \overline{1821}t^7 + \overline{1821}t^8 + \overline{1662}t^9 + \overline{541}t^{10} + \overline{872}t^{11} + \overline{678}t^{12} + \overline{260}t^{13} + \overline{193}t^{14} \\ &+ \overline{1407}t^{15} + \overline{868}t^{16} + \overline{1370}t^{17} + \overline{126}t^{18} + \overline{1244}t^{19} + \overline{1295}t^{20} + \overline{606}t^{21} + \overline{1473}t^{22} + \overline{791}t^{23} + O(t^{24}).\end{aligned}$$

The use of Berlekamp-Massey on $\mathcal{U}(t)$ does not give us the isogeny. We try in sequence $[i]\mathcal{U}(t)$ for increasing odd integers i. The one that works is

$$[11]\circ\mathcal{U}(t) = t+t^2+t^3+\overline{1820}t^4+\overline{1820}t^5+\overline{1820}t^6+\overline{373}t^7+\overline{1140}t^8+\overline{1140}t^9+\overline{260}t^{10}+\overline{1231}t^{11}+\overline{1205}t^{12}$$
$$+\overline{1291}t^{13}+\overline{305}t^{14}+\overline{175}t^{15}+\overline{480}t^{16}+\overline{113}t^{17}+\overline{1536}t^{18}+\overline{1205}t^{19}+\overline{274}t^{20}+\overline{1337}t^{21}+O(t^{22}),$$

for which Berlekamp-Massey gives:

$$I(X(t)) = \frac{X^5(t)+\overline{1641}X^3(t)+\overline{419}X(t)}{(X^2(t)+\overline{1821}X(t)+\overline{1958})^2}$$

and therefore

$$G(X) = X(X^4+\overline{1641}X^2+\overline{419}),$$
$$H(X) = X^2+\overline{1821}X+\overline{1958}.$$

8. Lercier's approach

The starting point of this is the following. Couveignes's (first) algorithm is rather intricate, both in theory and practice. Moreover, space requirement is huge, it is $O(\ell^2)$. Hence the desire to develop a more efficient approach.

In this section, we suppose $p = 2$ and $E : Y^2 + XY = X^3 + a$, $E^* : Y^2 + XY = X^3 + b$. The algorithm to be described has been developped in this particular case and it is not clear how to generalize it to other characteristics. Note that in particular, E and E^* are not supersingular curves.

8.1. **Presentation.** First of all, let us look at the example we have just computed. We see that the numerator of $I(X)$ is of the form $XL(X)^2$ for a polynomial $L(X)$. This is actually no accident and we can actually prove more.

Proposition 8.1. *Let $I(X) = G(X)/H(X)^2$ be our isogeny. Then $G = X(H^2 + H'(XH)')$.*

Proof: Using Vélu's formulas with $a_1 = 1$, $a_3 = a_2 = a_4 = 0$, we get

$$X^* = X - X\Sigma_1 + X^2\Sigma_2.$$

Note that in characteristic 2, for any polynomial $Q(X)$, $Q'(X)$ contains only even powers of X and $Q'' = 0$. Using this, we end up with the relation for G. □

Corollary 8.1. *With the above notations, one has $G(X) = XL(X)^2$ for some polynomial $L(X)$ of degree $d = (\ell-1)/2$.*

Proof: The polynomial H' contains even powers, as well as $(XH)'$, and therefore $H^2 + H'(XH)'$ also, and this means it is a square in characteristic 2. □

We can go further. To simplify notations, we put $\alpha = \sqrt[4]{a}$ and $\beta = \sqrt[4]{b}$.

Proposition 8.2. *The polynomials L and H satisfy*

$$L(X) = \lambda X^d H(\sqrt{a}/X)$$

where $\lambda = \sqrt{\beta/\alpha}\alpha^{-d}$.

Proof: The only point of order 2 on E (resp. E^*) is $P = (0, \sqrt{a})$ (resp. $P^* = (0, \sqrt{b})$). Note that for any point $M = (X, Y)$, the abscissa of $P \oplus M = (0, \sqrt{a}) \oplus (X, Y)$ is simply $\sqrt{a}/X$. Exploiting the fact that

$$I(P \oplus M) = P^* \oplus I(M),$$

we get

$$\frac{(\sqrt{a}/X)L(\sqrt{a}/X)^2}{H(\sqrt{a}X)^2} = \frac{\sqrt{b}}{XL(X)^2/H(X)^2}.$$

Taking square roots (remember that every element in $\mathbb{K}$ has a unique squareroot), we have

$$L(X)L(\sqrt{a}/X) = \frac{\beta}{\alpha} H(X)H(\sqrt{a}/X). \tag{6}$$

Since L and H have both degree d, $\tilde{L}(X) = X^d L(\sqrt{a}/X)$ and $\tilde{H}(X) = X^d H(\sqrt{a}/X)$ are polynomials. Using the fact that L and H are coprime, we deduce that $L(X) = \gamma \tilde{H}(X)$ for some γ in $\mathbb{K}$. Plugging this in (6) we get after simplification the value of γ and the result follows. □

Proposition 8.3. *Let $\hat{L}(X)$ (resp. $\hat{H}(X)$) denote the polynomial $\sqrt{L(X^2)}$ (resp. $\sqrt{H(X^2)}$). Then*
(i) $X^d \hat{H}(X + \sqrt{a}/X) = H(X)L(X)$;
(ii) $(X + \alpha)X^d \hat{L}(X + \sqrt{a}/X) = XL(X)^2 + \beta H(X)^2$.

Proof: We use the fact that for all point $M = (X, Y)$ on E, we have $I([2]M) = [2]I(M)$ or

$$\left(\frac{XL(X)^2}{H(X)^2}\right) \circ (X^2 + a/X^2) = (X^2 + b/X^2) \circ \left(\frac{XL(X)^2}{H(X)^2}\right).$$

Taking square roots twice, we get

$$(X + \alpha)\frac{X^d \hat{L}(X + \sqrt{a}/X)}{X^d \hat{H}(X + \sqrt{a}/X)} = \frac{XL(X)^2 + \beta H(X)^2}{L(X)H(X)}$$

and the result follows since both fractions are irreducible. □

We can now use these results to find the coefficients of $H(X)$ from those of $L(X)$. We write $L(X) = \sum_{i=0}^{d} p_i^2 X^i$, $H(X) = \sum_{i=0}^{d} q_i^2 X^i$. We can normalize $H(X)$ so that $q_d = 1$.

Corollary 8.2. *The coefficients p_i's and q_i's satisfy:*
(i) $p_d = q_d = 1$.
(ii) For all i, one has $q_i = \lambda \alpha^{-i} p_{d-i}$.

Proof:
(i) It is an an application of Proposition 8.1:
(ii) It follows from Proposition 8.2. □

We can go further:

Proposition 8.4. *One has*

$$p_{d-1} = \alpha + \beta, p_{d-2} = p_{d-1}^4 + \alpha p_{d-1} + d\alpha^2, p_0^4 = \alpha^{2d} + \alpha^{2d-1} p_{d-1}.$$

Proof: This is done using the second relation of Proposition 8.3 and identifying both side. □

The second relation of Proposition 8.3 yields a polynomial system which gives the p_i^4's as linear functions of the p_j's. However, solving this system is too time consuming. The idea is to use the first relation of Proposition 8.3. This gives an equation of degree 2 for p_i in terms of $p_1, p_2, \ldots, p_{i-1}$. Combining with a clever ordre of elimination of the variables, one can solve the system. Details are to be found in [14] where more elaborate strategies are given. The running time is heuristically $O(\ell^3)$ and space is $O(\ell^2)$.

Though of same complexity as Couveignes's first algorithm, the constants are much smaller in practice. For instance, the most elaborate version of Lercier's algorithm is almost 400 times faster for computing isogenies for $\mathbb{K} = \mathbb{F}_{2^{300}}$, resulting in a speed-up of 5 on the total running time for the complete SEA algorithm.

8.2. **A new record.** The record obtained (as of April 18, 1996) with our implementation is for $\mathbb{K} = \mathbb{F}_{2^{1301}}$. We represent $\mathbb{K}$ as $\mathbb{F}_2[T]/(T^{1301} + T^{11} + T^{10} + T + 1)$ and put

$$a = T^{16} + T^{14} + T^{13} + T^9 + T^8 + T^7 + T^6 + T^5 + T^4 + T^3$$

which is our zip code, 91128, written in binary. Then the curve $E : y^2 + xy = x^3 + a$ has $2^1 301 + 1 - c$ points where

$$\begin{aligned} c \;=\;& -125202046604585509943423813474143645809815976025515419374 \\ & 752510450916824670905165876650039250370012237528216030116547928372408 2 \\ & 5761437453092925430162137172566628268880767876046805121177132601520639. \end{aligned}$$

The computation was done on several DEC alpha's. The time needed on a single DEC alpha would have been 206 days among which, 7 days were spent computing isogenies. This is much smaller than what we had for $\mathbb{F}_{2^{1009}}$: 243 days for the whole computation, and 155 days for computing isogenies with Couveignes's algorithm [16]. Note that we had to use all ℓ's up to 673.

8.3. **The same example again.** We will find the isogeny I as

$$I(X) = \frac{G(X)}{H(X)^2} = \frac{XL^2(X)}{H(X)^2},$$

with $\deg(L(X)) = 2$ and $\deg(H(X)) = 2$.

For $\ell = 5$, it is enough to use Proposition 8.4. Put $d = (\ell - 1)/2 = 2$. With the above notations: $\alpha = \sqrt[4]{a} = \overline{571}$ and $\beta = \sqrt[4]{b} = \overline{859}$. Writing as above $L(X) = \sum_{i=0}^{d} p_i^2 X^i$ where the p_i's are the unknown coefficients of L, we get

$$\begin{aligned} p_2 &= \overline{1}, \\ p_1 &= \alpha + \beta = \overline{352}, \\ p_0 &= \sqrt[4]{\alpha^{2d} + \alpha^{2d-1} p_{d-1}} = \overline{1519}. \end{aligned}$$

We have found $L(X) = X^2 + \overline{1194}X + \overline{1746}$.

We now recover the coefficients of $H(X)$ using Corollary 8.2:

$$H(X) = X^2 + \overline{1821}X + \overline{1958}.$$

Very important remark: The ease with which we have computed the isogeny in this case is rather misleading. When ℓ grows, the equations giving the p_i's and the q_i's become more intricate, exhibiting non linear behaviour. The reader is urged to look at [14] for the details.

9. The second algorithm of Couveignes

This algorithm works in any characteristic p. Again, we suppose that E is not supersingular.

9.1. **Presentation.** We begin this presentation with a fundamental result.

Proposition 9.1. *Multiplication by p on E is given by*

$$[p](X, Y) = (F_p(X)^p, G_p(X, Y)^p) \tag{7}$$

where $F_p(X)$ and $G_p(X, Y)$ are two rational fractions.

Proof: Let us look at the following picture

$$\begin{tikzcd} E \arrow[rr, "{[p]}"] \arrow[dr, "\varpi"'] & & E \\ & E^p \arrow[ur, "\varpi^*"'] & \end{tikzcd}$$

Here, ϖ is the purely inseparable isogeny sending (X, Y) to (X^p, Y^p). By composition, we get $[p](X, Y) = \varpi^* \circ \varpi(X, Y) = \varpi^*(X^p, Y^p) = (\varpi^*(X, Y))^p$ and the claim follows. □

As a useful corollary, we note

Corollary 9.1. *There exists $\tilde{f}_{p^k}(X) \in \mathbb{K}[X]$ such that $f_{p^k}(X) = (\tilde{f}_{p^k}(X))^{p^k}$. The degree d_k of $\tilde{f}_{p^k}$ is $(p^k-1)/2$ if p is odd and $2^k - 1$ if $p = 2$.*

Remember also that the group $E[p^k]$ is cyclic, isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. To make things easier, we suppose that $E[p^k] \subset E(\mathbb{K})$, that is $\tilde{f}_{p^k}$ has all its roots over $\mathbb{K}$.

The new idea of Couveignes is simple. Let k be any integer. The isogeny I we are looking for sends $E[p^k]$ to $E^*[p^k]$. Suppose we know that P is sent to P^*. For all m, $1 \leq m < p^k$, we have $I(mP) = mP^*$. Let x_m (resp. x_m^*) denote the abscissa of mP (resp. mP^*). We can compute the polynomial $A(X)$ of degree $d_k - 1$ such that

$$A(x_m) = x_m^*$$

for all m, $1 \leq m \leq d_k$. This polynomial has the property that

$$I(X) = \frac{G(X)}{H(X)^2} \equiv A(X) \bmod \tilde{f}_{p^k}(X).$$

To recover H and G from this identity, we need that $d_k > 2\ell$. If this is the case, then one computes G via the euclidean algorithm:

$$\begin{array}{rcl} \tilde{f}_{p^k}(X) & = & q_1(X)A(X) + r_1(X), \deg(r_1) < \deg(A), \\ A(X) & = & q_2(X)r_1(X) + r_2(X), \deg(r_2) < \deg(r_1) \\ \cdots & = & \cdots \\ r_i(X) & = & q_{i+2}(X)r_{i+1}(X) + r_{i+2}(X), \deg(r_{i+2}) < \deg(r_{i+1}) \end{array}$$

for $i \geq 1$. Let us introduce

$$u_{-1} = 1, v_{-1} = 0, u_0 = 0, v_0 = 1$$

and

$$u_{i+2}(X) = u_i(X) - q_{i+2}(X)u_{i+1}(X),$$
$$v_{i+2}(X) = v_i(X) - q_{i+2}(X)v_{i+1}(X)$$

for all i. It is well known that

$$r_i(X) = \tilde{f}_{p^k}(X)u_i(X) + A(X)v_i(X)$$

for all i. When $\deg(v_i) = \ell - 1$, one has

$$A(X)v_i(X) \equiv r_i(X) \bmod \tilde{f}_{p^k}(X)$$

and if v_i is a square, we let H denote a square root and we are done.

Note that we can compute r_i very rapidly using the EMGCD algorithm of [1] or [12, 4].

In general of course, $E[p^k]$ is not rational and the interpolation part must be done with some care. We refer to [8] for the theory and to [15] for the implementation and examples. According to Couveignes, his algorithm should run in time $O(\ell^{2+\epsilon})$ and space $O(\ell)$.

Remarks.

1. In order for this method to work properly, P and P^* must be primitive points of p^k-division.
2. We need the factorization of $\tilde{f}_{p^k}(X)$, which can be considered as a one time job. However, we will need the factorization of $\tilde{f}^*_{p^k}$ for any curve E^*. The best and most efficient way of doing requires some care. See [8] for this.
3. We do not really need the full polynomial of p^k-division. Any factor of it of degree $> 2\ell$ will do.
4. Note that if P^* does not work, $-P^*$ will not work either.

9.2. **Again, the same example.** We look for the 5-isogeny between $E : Y^2 + XY = X^3 + \overline{22}$ and $E^* : Y^2 + XY = X^3 + \overline{1663}$. We take $k = 2 + \lceil \log_2 \ell \rceil = 5$. We select as primitive 2^k-division point $P = [\overline{355}, \overline{735}, \overline{1}]$ and give the values of x_m for all m, $1 \le m \le 16$:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x_m	$\overline{355}$	$\overline{498}$	$\overline{1954}$	$\overline{1182}$	$\overline{59}$	$\overline{1210}$	$\overline{1059}$	$\overline{571}$	$\overline{471}$	$\overline{1735}$	$\overline{1491}$	$\overline{2011}$	$\overline{1734}$	$\overline{1943}$	$\overline{1980}$	$\overline{0}$

After trial and error, we find that $P^* = [\overline{632}, \overline{974}, \overline{1}]$ is the image of P by I. First, we have

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x_m^*	$\overline{632}$	$\overline{759}$	$\overline{1151}$	$\overline{1769}$	$\overline{1898}$	$\overline{1949}$	$\overline{828}$	$\overline{859}$	$\overline{882}$	$\overline{1370}$	$\overline{1814}$	$\overline{695}$	$\overline{459}$	$\overline{94}$	$\overline{183}$	$\overline{0}$

Using Lagrange's formulas, we find that

$$A(X) = \overline{1488}X^{15} + \overline{1726}X^{14} + \overline{1429}X^{13} + \overline{326}X^{12} + \overline{1934}X^{11} + \overline{607}X^{10} + \overline{1661}X^9 + \overline{998}X^8 + \overline{760}X^7 + \overline{1460}X^6 + \overline{1070}X^5 + \overline{1580}X^4 + \overline{768}X^3 + \overline{1530}X^2 + \overline{1447}X.$$

and Euclid's algorithm gives us

$$v_2 = \overline{1207}X^4 + \overline{1934}X^2 + \overline{1396}$$

which is proportional to the square of

$$X^2 + \overline{1821}X + \overline{1958}.$$

10. Conclusion

We have described algorithms for computing isogenies between elliptic curves over fields of any characteristic. We give below some of their characteristics. The ideal running time for an algorithm computing isogenies of degree ℓ in the case $p \ll \ell$ should be comparable to that of the case $p \gg \ell$. This might be the case of Couveignes's second algorithm.

Case	Method	Time	Space
$p \gg \ell$	$\wp$	$O(\ell^2)$	$O(\ell)$
$p \ll \ell$	Couveignes 1	$O(\ell^3)$	$O(\ell^2)$
	Lercier	$O(\ell^3)$?	$O(\ell^2)$
	Couveignes 2	$O(\ell^{2+c})$?	$O(\ell)$?

The two most recent algorithms are being implemented and more work is needed to make them really efficient and the complexity of the last one is to be precised. No doubt that they will perform well in practice, as part of the computations needed in the SEA algorithm. They will probably replace Couveignes's first algorithm in this task.

References

[1] Alfred V. Aho, J. E. H., and D.Ullman, J. *The design and analysis of computer algorithms.* Reading. Addison–Wesley, 1974.

[2] Atkin, A. O. L. The number of points on an elliptic curve modulo a prime. Draft, 1988.

[3] Atkin, A. O. L. The number of points on an elliptic curve modulo a prime (ii). Draft, 1992.

[4] Brent, R. P., Gustavson, F. G., and Yun, D. Y. Y. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algorithms 1* (1980), 259–295.

[5] Charlap, L. S., Coley, R., and Robbins, D. P. Enumeration of rational points on elliptic curves over finite fields. Draft, 1991.

[6] Cohen, H. *A course in algorithmic algebraic number theory*, vol. 138 of *Graduate Texts in Mathematics.* Springer–Verlag, 1993.

[7] Couveignes, J.-M. *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, July 1994.

[8] Couveignes, J.-M. Computing l-isogenies with the p-torsion. To appear in the Proc. of ANTS-II, Jan. 1996.

[9] Dewaghe, L. Un corollaire aux formules de Vélu. Preprint, Dec. 1995.

[10] Elkies, N. D. Explicit isogenies. Draft, 1991.

[11] Fröhlich, A. *Formal groups*, vol. 74 of *Lecture Notes in Math.* Springer-Verlag, 1968.

[12] GUSTAVSON, F. G., AND YUN, D. Y. Fast algorithms for rational Hermite approximation and solution of Toeplitz systems. *IEEE Transactions on Circuits and Systems CAS-26*, 9 (Sept. 1979), 750–755.

[13] LANG, S. *Elliptic functions.* Addison-Wesley, 1973.

[14] LERCIER, R. Computing isogenies in characteristic 2. To appear in the Proc. of ANTS-II, available on `http://lix.polytechnique.fr/~lercier/`, Dec. 1995.

[15] LERCIER, R. Isogeny computations. Draft, Jan. 1996.

[16] LERCIER, R., AND MORAIN, F. Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm. Research Report LIX/RR/95/09, École Polytechnique–LIX, Sept. 1995. An improved version is being submitted.

[17] LERCIER, R., AND MORAIN, F. Counting the number of points on elliptic curves over finite fields: strategies and performances. In *Advances in Cryptology – EUROCRYPT '95* (1995), L. C. Guillou and J.-J. Quisquater, Eds., vol. 921 of *Lecture Notes in Comput. Sci.*, pp. 79–94. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[18] MASSEY, J. L. Shift-register and BCH decoding. *IEEE Trans. on Information Theory IT-15*, 1 (Jan. 1969), 122–127.

[19] MORAIN, F. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux 7* (1995), 255–282.

[20] MÜLLER, V. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei.* PhD thesis, Technischen Fakultät der Universität des Saarlandes, 1995.

[21] SCHOOF, R. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux 7* (1995), 219–254.

[22] SILVERMAN, J. H. *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics.* Springer, 1986.

[23] STARK, H. M. Class-numbers of complex quadratic fields. In *Modular functions of one variable I* (1973), W. Kuyk, Ed., vol. 320 of *Lecture Notes in Math.*, Springer Verlag, pp. 155–174. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.

[24] VÉLU, J. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math. 273* (July 1971), 238–241. Série A.

(R. Lercier) CELAR/SSIG, ROUTE DE LAILLÉ, F-35170 BRUZ, FRANCE
E-mail address, R. Lercier: `lercier@polytechnique.fr`

(F. Morain) LABORATOIRE D'INFORMATIQUE DE L'ÉCOLE POLYTECHNIQUE (LIX), F-91128 PALAISEAU CEDEX, FRANCE
E-mail address, F. Morain: `morain@polytechnique.fr`