Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm

Reynald Lercier* & François Morain†‡

September 8, 1995

Abstract

The heart of the improvements of Elkies to Schoof's algorithm for computing the cardinality of elliptic curves over a finite field is the ability to compute isogenies between curves. Elkies' approach was well suited for the case where the characteristic of the field is large. Couveignes showed how to compute isogenies in small characteristic. The aim of this paper is to describe the first successful implementation of Couveignes's algorithm and to give numerous computational examples. In particular, we describe the use of fast algorithms for performing incremental operations on series. We will also insist on the particular case of the characteristic 2.

1 Introduction

Elliptic curves have been used successfully to factor integers [25, 34], and prove the primality of large integers [4, 18, 3]. Moreover they turned out to be an interesting alternative to the use of $\mathbb{Z}/N\mathbb{Z}$ in cryptographical schemes. The first schemes were presented in [33, 23] and followed by many more (see for instance [31] and the survey in [27]).

One of the main algorithmic problems to be solved is the efficient computation of the cardinality of elliptic curves over finite fields. It was not until recently that Schoof's polynomial time algorithm for solving this problem could be efficiently used, due to the work of Atkin [1, 2] and [15] (see also [41, 36] and the results of the implementation given in [36, 27, 38]). It gave satisfactory results in the large characteristic case, and only very recently was it possible to make it work as well in the small characteristic case, using Couveignes's thesis [10].

The aim of this paper is to explain how Couveignes's algorithm can be implemented in an efficient way.

The structure of this paper is as follows. Section 2 recalls basic facts on elliptic curves, division polynomials and formal groups. Section 3 gives additional results concerning elliptic curves over finite fields; in particular, we study the properties of the multiplication by p on elliptic curves in characteristic p, and insist on the role of the Hasse invariant; also, we give an algorithm for computing a factor of the p^k-division polynomial in characteristic p. Section 4 describes Schoof's algorithm in a synthetic way using the contributions of Atkin and Elkies. Elkies' method can be seen as computing isogenies between curves; using his ideas requires two tasks: given an elliptic curve E and an integer ℓ, find a curve E^* that is ℓ-isogenous over K and compute the isogeny.

*CELAR/SSIG, Route de Laillé, F-35170 Bruz

†LIX École Polytechnique, F-91128 Palaiseau CEDEX, FRANCE

‡On leave from the French Department of Defense, Délégation Générale pour l'Armement.

Elkies and Atkin have explained how to do this in the case of large characteristic. We explain how to solve the first task in small characteristic and section 5 will explain the decisive ideas of Couveignes for the computation of isogenies in small characteristic. Section 6 is concerned with fast algorithms for incremental computations on series. Section 7 details the algorithms we need to implement Couveignes's ideas. The complexity of Couveignes's approach is then derived. Then section 8 will be devoted to numerial examples and section 9 to the implementation in the special case of the characteristic 2.

Notations. Throughout the paper, we let $K = GF(q) = GF(p^n)$ be a finite field of characteristic p. The field K will be given as $GF(p)[T]/(f(T))$ for some irreducible polynomial $f(T)$ of degree n. An element of K can be written as a polynomial in T.

We will encounter many p-th roots in characteristic p and it will be convenient to write them as $\tilde{a} = \sqrt[p]{a}$ (note that every element a in $GF(p^n)$ has exactly one p-th root given by $a^{p^{n-1}}$). Moreover, if $A(X)$ is a series (or a polynomial) in $K[X]$:

$$A(X) = \sum_i a_i X^i$$

we will write

$$\tilde{A}(X) = \sum_i \tilde{a}_i X^i.$$

2 Elliptic curves and formal groups

We recall well known properties of elliptic curves. All these can be found in [42]. In this section, we let k be any field and denote by $\overline{k}$ its Galois closure.

2.1 Definition

We follow [42, Chap. III]. Let

$$\mathcal{F}(X, Y, Z) = Y^2 Z + a_1 XYZ + a_3 YZ^2 - (X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3)$$

where the a_i's are in k. Put

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1 a_3, b_6 = a_3^2 + 4a_6, b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, c_6 = b_2^3 + 36b_2 b_4 - 216b_6,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

If Δ is invertible in k, then $\mathcal{F}(X, Y, Z) = 0$ defines an elliptic curve E, that we will note $[a_1, a_3, a_2, a_4, a_6]$ for short. Then the j-invariant of the curve is $j(E) = c_4^3/\Delta$.

It is possible to define on the set of points $E(k)$ of E

$$E(k) = \{(X, Y) \in k^2, \mathcal{F}(X, Y, 1) = 0\} \cup \{O_E\}$$

an Abelian law using the so-called *tangent-and-chord* method, O_E being the neutral element $(0, 1, 0)$. We refer to the references given above for the precise equations of the law.

2.2 Division polynomials and torsion points

Let m be any integer. Then

$$m(X,Y) = \left(\frac{\phi_m(X,Y)}{\psi_m^2(X,Y)}, \frac{\omega_m(X,Y)}{\psi_m^3(X,Y)}\right)$$

where ϕ_m, ψ_m and ω_m are in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X, Y]$. The polynomial ψ_m, called the m-th division polynomial, is defined by the following formulas:

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

$$\psi_3 = 3X^4 + b_2X^3 + 4b_4X^2 + 3b_6X + b_8,$$

$$\psi_4 = (2Y + a_1X + a_3)\left(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\right);$$

$$\psi_2\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), m \geq 2;$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2.$$

The polynomials ω_m and ϕ_m satisfy:

$$\phi_m = X\psi_m^2 - \psi_{m-1}\psi_{m+1},$$

and if $p \neq 2$:

$$\omega_m = \frac{\psi_{2m}}{2\psi_m} - \frac{1}{2}\psi_m(a_1\phi_m + a_3\psi_m^2).$$

A particular role is played by the polynomial ψ_m. We let $\psi'_m(X)$ denote $\psi_m(X,Y)$ reduced in $k[X,Y]/(\mathcal{F}(X,Y,1))$. 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 $E[m] = \{P \in E(\overline{k}), mP = O_E\}$. The principal property of $E[m]$ is the following.

Theorem 2.1 *Let $P = (X,Y) \in E(\overline{k})$. Then $P \in E[m]$ if and only if $f_m(X) = 0$.*

2.3 The formal group associated to an elliptic curve

The material below is taken from [42, Chap. IV][1].

2.3.1 Definition

Let $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ be an elliptic curve. Let $t = -X/Y$ and $s = -1/Y$. We transform the equation of E to get:

$$s = A(t,s) = t^3 + a_1ts + a_2t^2s + a_3s^2 + a_4ts^2 + a_6s^3.$$

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. Letting t be any formal series in $k[[\tau]]$, 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. More details will be given in the following subsections.

[1] Be careful that there are some typos and missing equations in [21, Chap. 12].

2.3.2 Computing $\mathcal{S}(t)$

From the equation $s = A(t,s)$, it is easy to compute the first L coefficients of s as a formal series in t, by an iterative process in $O(L^2)$ operations. We can do better using standard techniques from combinatorics [9, 39]. In particular, $\mathcal{S}$ satisfies a second order linear differential equation with polynomial coefficients in t, from which we can easily deduce recurrence relations between the coefficients of $\mathcal{S}$. Hence, these coefficients can be computed in $O(L)$ operations modulo precomputations. See section 9.1 for the computations in characteristic 2.

The first coefficients of $\mathcal{S}$ are:

$$s = \mathcal{S}(t) = \sum_{i=3}^{\infty} s_i t^i = t^3 + a_1\, t^4 + (a_1^2 + a_2)t^5 + O(t^6). \tag{1}$$

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.

We deduce also that

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

and

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

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

2.3.3 Group law

Let us work out the addition law on $\mathcal{E}$, that we will note $\oplus$. The neutral element is $O_{\mathcal{E}} = (0,0)$ and the equation of $\mathcal{E}$ is $F(t,s) := A(t,s) - s = 0$. We start from two points $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$, different from $O_{\mathcal{E}}$, and we want to compute the sum $(t_3, s_3) = (t_1, s_1) \oplus (t_2, s_2)$. This is done as follows: we first draw the line passing through P_1 and P_2, which intersects $\mathcal{E}$ in a third point $P_i = (t_i, s_i)$. Then we draw the line passing through P_i and $(0,0)$, which intersects $\mathcal{E}$ in a third point $P_3 = (t_3, s_3)$.

More precisely, let $y = \lambda t + \nu$ be the line passing through the two points P_1 and P_2. If $(t_1, s_1) \neq (t_2, s_2)$ then

$$\lambda = \frac{s_2 - s_1}{t_2 - t_1} = t_1^2 + t_1 t_2 + t_2^2 + \cdots. \tag{2}$$

If the two points are equal, then

$$\lambda = -\frac{\dfrac{\partial F}{\partial t}}{\dfrac{\partial F}{\partial s}} = -\frac{a_1\, s_1 + 3\, t_1^2 + 2\, a_2\, t_1 s_1 + a_4\, s_1^2}{-1 + a_1\, t_1 + 2\, a_3\, s_1 + a_2\, t_1^2 + 2\, a_4\, t_1 s_1 + 3\, a_6\, s_1^2} = 3t_1^2 + 4a_1 t_1^3 + O(t_1^4). \tag{3}$$

In all cases, one has:

$$\nu = s_1 - \lambda t_1.$$

Let (t_i, s_i) be the third point of intersection of this line with $\mathcal{E}$. Then t_i satisfies

$$F(t_i, \lambda t_i + \nu) = 0$$

or

$$\left(a_4\,\lambda^2 + a_2\,\lambda + 1 + a_6\,\lambda^3\right) t^3 + \left(a_1\,\lambda + 2\,a_4\,\nu\,\lambda + a_2\,\nu + 3\,a_6\,\nu\,\lambda^2 + a_3\,\lambda^2\right) t^2 + \cdots = 0.$$

It follows that

$$t_1 + t_2 + t_i = -\frac{a_1\,\lambda + 2\,a_4\,\nu\,\lambda + a_2\,\nu + 3\,a_6\,\nu\,\lambda^2 + a_3\,\lambda^2}{a_4\,\lambda^2 + a_2\,\lambda + 1 + a_6\,\lambda^3}. \tag{4}$$

From this, we deduce $s_i = \lambda t_i + \nu$.

If $t_i = 0$, then P_2 is the opposite of P_1 and we are done, $P_3 = O_{\mathcal{E}}$. Otherwise, we have to compute the addition of (t_i, s_i) and the origin point $(0,0)$ to get (t_3, s_3). It is easy to see that the equation of the line we are interested in is $\lambda_i = s_i/t_i$ and $\nu_i = 0$. Using (4), one gets:

$$t_3 + 0 + t_i = -\frac{s_i\,\left(a_1\,t_i + a_3\,s_i\right) t_i}{a_4\,{s_i}^2 t_i + a_2\,s_i\,{t_i}^2 + {t_i}^3 + a_6\,{s_i}^3}.$$

Using the fact that $F(t_i, s_i) = 0$, the denominator simplifies as

$$s_i - a_1 t_i s_i - a_3 s_i^2$$

and finally we obtain

$$t_3 = \frac{t_i}{-1 + a_1\,t_i + a_3\,s_i}. \tag{5}$$

For s_3, one gets:

$$s_3 = \frac{s_i}{t_i}\,t_3.$$

We will write $t_3 = F_a(t_1, t_2)$. The first terms are:

$$F_a(t_1,t_2) = t_1 + t_2 - a_1 t_1 t_2 - a_2(t_1^2 t_2 + t_1 t_2^2) - (2a_3 t_1^3 t_2 - (a_1 a_2 - 3a_3) t_1^2 t_2^2 + 2a_3 t_1 t_2^3) + \cdots \tag{6}$$

It is now easy to compute the opposite of P, simply noting that this opposite is the third point of intersection of the line joining P and $O_{\mathcal{E}}$ with $\mathcal{E}$. Precisely, if $-P = (t', s')$, one has

$$t' = \frac{t}{-1 + a_1 t + a_3 s}. \tag{7}$$

When $t_1 = t_2$, we get

$$F_d(t_1) = [2]t_1 = 2\,t_1 - a_1\,t_1^2 - 2\,a_2\,t_1^3 + (a_1\,a_2 - 7\,a_3)\,t_1^4 + \cdots. \tag{8}$$

More generally, one can show the following [42, Corollary 4.4, pp. 120]:

Theorem 2.2 *For P prime, one has*

$$[P](t) = P f(t) + g(t^P)$$

where f and g are elements of $k[[t]]$.

3 Elliptic curves over finite fields

3.1 Summary of the theory

The most interesting object associated with an elliptic curve over a finite field $K = GF(q)$ is the Frobenius ϕ_E, which maps $E(\overline{K})$ onto itself and which sends a point $(X, Y, 1)$ to $(X^q, Y^q, 1)$. It is known that this endomorphism has characteristic equation:

$$\pi^2 - c\pi + q = 0 \tag{9}$$

with c in $\mathbb{Z}$ such that $c^2 - 4q < 0$. The *trace* of ϕ_E satisfies $\mathrm{Tr}(\phi_E) = c$ and the cardinality of $E(GF(q))$ is $\#E(K) = q + 1 - c$. In this way, we recover Hasse's theorem [42, Chap. V].

3.1.1 Supersingular curves

A curve E is said to be *supersingular* if and only if $c \equiv 0 \bmod p$. Many results are known for these curves. We refer to [42] and [21] for this. For instance, it is known that $j(E) \in GF(p^2)$ and it is a root of a fixed polynomial $S_p(X)$ that will be described below.

Let E be a supersingular curve of cardinality $\#E = q + 1 - c$. From [43, Theorem (4.1)], we deduce the following.

Proposition 3.1 *1. If the degree $[GF(q) : GF(p)]$ is odd, then one of the following holds:*

(a) $c = 0$;

(b) $c = \pm\sqrt{2q}$ and $p = 2$;

(c) $c = \pm\sqrt{3q}$ and $p = 3$.

2. If the degree $[GF(q) : GF(p)]$ is even, then one of the following holds:

(a) $c = 0$ and $p \not\equiv 1 \bmod 4$;

(b) $c = \pm 2\sqrt{q}$;

(c) $c = \pm\sqrt{q}$ and $p \not\equiv 1 \bmod 3$.

3.1.2 Torsion points

Let us now give a description of the torsion group $E[m]$ (see [42, Corollary 6.4, pp. 89]:

Theorem 3.1 *When m is prime to p, then $E[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ and when $m = p^e$, $E[m]$ is isomorphic to $\{O_E\}$ if E is supersingular and $(\mathbb{Z}/p^e\mathbb{Z})$ otherwise.*

3.2 Canonical curves

All the algorithms that we present in this paper work with a curve given by its five parameters. However, we can simplify greatly the exposition by considering "canonical curves" obtained by some change of variable. The parametrization given for $p = 2$ and $p = 3$ correspond to non supersingular curves.

When $p = 2$, we follow [32]. The most general equation of a non supersingular elliptic curve corresponds to $a_1 = 1$, $a_3 = a_4 = 0$. Moreover, $E : Y^2 + XY = X^3 + a_2X^2 + a_6$ and $E' : Y^2 + XY = X^3 + a_2'X^2 + a_6$ are K-isomorphic if and only if $\mathrm{Tr}(a_2) = \mathrm{Tr}(a_2')$; if $\mathrm{Tr}(a_2) \neq \mathrm{Tr}(a_2')$, E' is a twist of E, and thus $\#E + \#E' = 2(q+1)$. From what precedes, it is enough to consider curves of equation $Y^2 + XY = X^3 + a_6$ with $a_6 \in K^*$, whose invariant is $j(E) = 1/a_6$. We will note $E = [a_6]$.

When $p = 3$, we can take $a_1 = a_3 = a_4 = 0$. So the general case is

$$Y^2 = X^3 + a_2X^2 + a_6$$

with $j(E) = -a_2^3/a_6$ and we write $E = [a_2, a_6]$.

When $p > 3$, we can take $a_1 = a_3 = a_2 = 0$. One gets

$$Y^2 = X^3 + a_4X + a_6$$

with

$$j(E) = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}$$

and we will note $E = [a_4, a_6]$.

3.3 Multiplication by p

3.3.1 Multiplication by p on E

We begin with a precise characterization.

Proposition 3.2 *Multiplication by p on E is given by*

$$[p](X,Y) = (F_p(X)^p, G_p(X,Y)^p) \tag{10}$$

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

Proof: (We are indebted to J.-M. Couveignes for the following elegant proof.) Let E^p denote the curve of coefficients $[a_1^p, a_3^p, a_2^p, a_4^p, a_6^p]$. There is an isogeny I of degree p between E and E^p given by $(X,Y) \mapsto (X^p, Y^p)$. Let I^* denote the dual isogeny:

$$I^*(X,Y) = (F_p(X), G_p(X,Y))$$

with F_p and G_p two rational fractions. Using $I^* \circ I = [p]$, the result follows. $\Box$

We can precise things by looking at the division polynomials $f_{p^e}(X)$.

Corollary 3.1 *There exists $\tilde{f}_{p^e} \in K[X]$ such that $f_{p^e}(X) = (\tilde{f}_{p^e}(X))^{p^e}$.*

Proof: From (10), it follows that

$$[p^e](X,Y) = (F_{p^e}(X)^{p^e}, G_{p^e}(X,Y)^{p^e})$$

for all $e \geq 1$. In particular, this implies that ψ_{p^e} and *a fortiori* f_{p^e} are p^e-th powers. From this it follows that the degree of f_{p^e} is in fact at most $(p^{2e} - p^e)/2$. $\Box$

Corollary 3.2 *With the same conditions as above, $\tilde{f}_{p^e}(X)$ is divisible by $\tilde{f}_{p^{e-1}}(X)$, and thus we can find a primitive factor of $f_{p^e}(X)$ of degree at most $p^{e-1}(p-1)/2$.*

We can precise the properties of F_p and G_p as follows:

Proposition 3.3 *When $p = 2$ and $E = [a_6]$, one has*

$$F_2(X) = X + \frac{\tilde{a}_6}{X},\; G_2(X,Y) = \tilde{a}_6\left(1 + \frac{1}{X}\right) + \frac{a_6}{X^2} + Y\left(1 + \frac{\tilde{a}_6}{X^2}\right).$$

When $p = 3$ and $E = [a_2, a_6]$, one finds that

$$F_3(X) = \frac{X^3 + 2\,X\tilde{a}_2^3\tilde{a}_6 + \tilde{a}_6^3}{(\tilde{a}_2\,X + \tilde{a}_2\,\tilde{a}_6)^2},$$

$$G_3(X,Y) = Y\,\frac{X^3 + X\tilde{a}_2^3\tilde{a}_6 + \tilde{a}_6^3 - \tilde{a}_2^3\tilde{a}_6^2}{(\tilde{a}_2\,X + \tilde{a}_2\,\tilde{a}_6)^3}.$$

When $p > 3$ and $E = [a_4, a_6]$,

$$F_p(X) = \frac{A_p(X)}{\tilde{f}_p(X)^2}, G_p(X,Y) = Y\,\frac{C_p(X)}{\tilde{f}_p(X)^3}$$

where A_p is a polynomial of degree p and C_p a polynomial of degree $3(p-1)/2$.

Proof: In the case $p=2$, for the canonical curve $[a_6]$, we find:

$$[2](X,Y) = \left(X^2+\frac{a_6}{X^2}, \left(X+\frac{Y}{X}\right)\left(X^2+\frac{a_6}{X^2}\right)+\frac{a_6}{X^2}\right)$$
$$= \left(\left(X+\frac{\tilde{a}_6}{X}\right)^2, \left(Y+\frac{a_6}{X^2}+\tilde{a}_6\left(1+\frac{Y}{X^2}+\frac{1}{X}\right)\right)^2\right)$$

which yields the result.

The same reasonning can be made for $p=3$. As for the general case, note that the degree of the polynomials A_p and C_p can be deduced from the fact that they come fron an isogeny of degree p. □

Remark. It is possible to give an elementary proof that $f_p(X)$ is a p-th power, using Fricke's equation [16, vol II, pp. 191], that degenerates mod$p$ as:

$$(X^3+a_4X+a_6)\frac{\partial^2 F}{\partial X^2} - (-3/2X^2 - 1/2a_4)\frac{\partial F}{\partial X} = 0.$$

Then it is enough to prove that any polynomial solution of this must satisfy $\frac{\partial F}{\partial X} = 0$ or $F(X) = \tilde{F}(X^p)$ for some $\tilde{F}$.

Computing $f_{p^e}(X)$. From a practical point of view, one uses the algorithm given in [32] for $p=2$. For $p>3$, one can use the work of McKee [30] who derived recurrence relations for the coefficients of f_m from Fricke's differential equation. This enables us to compute only the non-zero coefficients of $\tilde{f}_{p^e}$, that is coefficients of index multiple of p^e.

When $p=3$ and $E=[a_2,a_6]$, we can generalize the work of McKee by using the fact that f_m, m odd, satisfies the differential equation

$$a_2(X^3+a_2X^2+a_6)\frac{\partial^2 F}{\partial X^2} - ((m^2-3/2)a_2X^2+(m^2-2)/2a_2^2X+3m^2/2a_6)\frac{\partial F}{\partial X}$$
$$+m^2/2(a_2^3+9a_6)\frac{\partial F}{\partial a_2} - m^2/2a_2^2a_6\frac{\partial F}{\partial a_6} + m^2(m^2-1)/4a_2XF = 0.\square$$

Example. Let $K = GF(5^3) = GF(5)[T]/(T^3+T+1)$ and $E: Y^2 = X^3+X+T$. We first find that

$$\tilde{f}_5(X) = 2X^2+(4T^2+2T+1)X+T.$$

Then

$$\tilde{f}_{5^2} = 4X^{12}+(3T^2+2T+2)X^{11}+(4T^2+2T)X^{10}+(T^2+2T)X^9+4T^2X^7+(3T^2+3)X^8$$
$$+(T^2+T+4)X^6+(T^2+3T+2)X^5+(T^2+4T+2)X^4+(2T^2+3T+1)X^3$$
$$+(T^2+4T+3)X^2+T^2+(3T^2+4T+4)X+3T$$

from which

$$g_{25}(X) = \tilde{f}_{5^2}/\tilde{f}_5 = 2X^{10}+4TX^9+(3T^2+T+3)X^8+(T^2+T+1)X^7+(2T^2+T+3)X^6+(2T+3)X^5$$
$$+(2T^2+3)X^4+(4T^2+3T+4)X^3+(3T^2+4T)X^2+(4T+1)X+T+3$$

is a primitive factor of $f_{25}(X)$.

Remark. When E is supersingular, then $f_{p^e}(X)$ is a constant (if $p^e < q$). For example, for $p = 3$ and $E = [0, 0, 0, a_4, a_6]$ for which $j(E) = 0$, one finds that

$$f_3(X) = -a_4^2, f_{3^2}(X) = a_4^{20}, f_{3^3}(X) = -a_4^{182}.$$

For a less trivial example, consider $p = 13$, for which $S_{13}(X) = X - 5$. A supersingular curve in characteristic 13 has equation $E = [4, 7]$. We find $f_{13}(X) = 12$ and $f_{13^2}(X) = 1$.

3.3.2 Multiplication by p on $\mathcal{E}$

We can precise the result of Theorem 2.2 as follows.

Theorem 3.2 *Multiplication by p on E can be expressed as a series in $t^{p^{h(E)}}$:*

$$[p]_E(t) = c_p(E)t^{p^{h(E)}} + O(t^{p^{2h(E)}})$$

where $h(E)$ is an integer – called the height *– which is equal to* 2 *if E is supersingular and* 1 *otherwise. The coefficient $c_p(E)$ of $t^{p^{h(E)}}$ is called the (relative)* Hasse invariant *of E.*

One of the important property of this invariant is the following [42, Chap. V, §4]:

Theorem 3.3 *The Hasse invariant satisfies:* $\mathrm{N}_{K/GF(p)}(c_p(E)) \equiv \mathrm{Tr}(\phi_E) \bmod p$.

3.3.3 Computing the Hasse invariant

In characteristic 2, one has $c_p(E) = a_1$; in characteristic 3, for $[a_2, a_6]$, it is a_2. When $p > 3$, for $E = [a_4, a_6]$, one can compute the Hasse invariant using the work of Deuring [13] or any other method (see [37] for a survey of these methods). For our purposes, this invariant appears naturally as the first coefficient of $[p]_E(t)$. The first few values of c_p are:

p	$c_p(a_4, a_6)$
5	$2a_4$
7	$3a_6$
11	$9a_4a_6$
13	$7a_4^3 + 2a_6^2$
17	$2a_4^4 + 15a_4a_6^2$

3.3.4 Computing $[p]_E(t)$

It will be useful to write

$$[p]_E(t) = \Phi_{p,E}(t)^p \tag{11}$$

where $\Phi_{p,E} \in K[[t]]$, so that $\Phi_{p,E} = \sqrt[p]{c_p(E)}t + O(t^2)$.

Of course, one can use the addition formulae and compute the series to any desired order. In this way, the computation of $c_p(E)$ is easy and does not require a formal formula.

There is an alternative way, that is of some interest. It consists in computing the multiplication by p on the original curve E and then make the change of variables $(X, Y) \mapsto (t, s)$.

The fractions F_p and G_p can be computed using the recurrence relations of section 2.2 in time $O(p^2 \log p)$. Then

$$[p]_E(t) = -\left(\frac{F_p(t/s)}{G_p(t/s, -1/s)}\right)^p.$$

We see that this is equal to $\mathcal{R}_{p,E}(t,s)^p$ with

$$\mathcal{R}_{p,E}(t,s) = (-1)^p \frac{F_p(t/s)}{G_p(t/s,-1/s)}. \tag{12}$$

We can recover $\Phi_{p,E}$ by computing the expansion of $\mathcal{R}_{p,E}(t,s(t))$. For instance, when $p=2$, one finds

$$\mathcal{R}_{2,E}(t,s) = \frac{\left(t^2+\tilde{a}_6 s^2\right)t}{t^3+\left(1+\tilde{a}_6 s\right)t^2+\left(\tilde{a}_6 s^2+s\right)t+\tilde{a}_6 s^2+s}. \tag{13}$$

We will see the interest of such computations in section 7.2.2.

4 Counting the number of points

4.1 Schoof's algorithm

Schoof's algorithm [40] uses the properties of the Frobenius. More precisely, let ℓ be a prime number. Equation (9) is still valid when ϕ_E is restricted to the group $E[\ell]$, and equivalently

$$\pi^2 - c\pi + q \equiv 0 \bmod \ell. \tag{14}$$

We can find $c_\ell \equiv c \bmod \ell$ by finding which value of γ, $0 \leq \gamma < \ell$, satisfies

$$(X^{q^2}, Y^{q^2}) + q(X,Y) = \gamma(X^q, Y^q)$$

in $K[X,Y]/(\mathcal{F}(X,Y,1), f_\ell(X))$. If we know $c \bmod \ell$ for enough ℓ's such that

$$\prod \ell > 4\sqrt{q}$$

then we can determine c using the Chinese remaindering theorem.

4.2 An overview of the improvements of Atkin and Elkies

Though Schoof's algorithm has polynomial running time, its implementation was rather inefficient, due to the size of the polynomials involved. However, Atkin first and then Elkies devised theoretical and practical improvements. We suppose from now on that we want to compute $c_\ell \equiv c \bmod \ell$, ℓ a prime number different from p (see below for the particular case $\ell = p$).

Firstly, Atkin [1] explained how to use the properties of the modular polynomial $\Phi_\ell(X,Y)$ modulo p to get a list of possible values of t_ℓ. The polynomial $\Phi_\ell(X,Y)$ is symmetric in X and Y and has degree $\ell+1$. The polynomial $\Phi(X) = \Phi_\ell(X, j(E))$ describes the cyclic subgroups of $E[\ell]$. It can have basically two splittings in K: $(11r\ldots r)$ with $\ell-1 = rs$ or $(r\ldots r)$ with $\ell+1 = rs$ (there are two particular cases described in the paper which are rare and we omit the relevant details for the sake of simplicity). In the first case, ℓ is said to be an *Elkies prime* and an *Atkin prime* in the second. In both cases, r is the order of α/β where α and β are the roots of

$$\pi^2 - c\pi + q \equiv 0 \bmod \ell$$

and lie in $GF(\ell)$ if ℓ is an Elkies prime (and thus c^2-4q must be a square modulo ℓ) and in $GF(\ell^2)$ otherwise (implying that c^2-4q is not a square modulo ℓ). Once r is known, there are $\varphi(r)$ possible values of c_ℓ and in many cases, this value is much less than ℓ. It remains to combine these values in a clever way, using a *match and sort* technique described in [1]. (The referred work contains also many ideas concerning the alternative use of other modular equations, that turn out to be essential in practice, but that we do not want to describe here (for this see also [36]).

Elkies [15] remarked that when $c^2 - 4q$ is a square modulo ℓ, then $f_\ell(X)$ has a factor $g_\ell(X)$ of degree $(\ell-1)/2$. Moreover, ϕ_E has an eigenspace V associated with g_ℓ, that is a cyclic group of E. This in turn is equivalent to saying that E and $E^* = E/V$ are two elliptic curves connected by an isogeny I of degree ℓ. The kernel of this isogeny yields the factor $g_\ell(X)$.

Once we have g_ℓ, we now look for some k, $1 \le k < \ell$ such that

$$(X^q, Y^q) = k(X, Y)$$

in $K[X,Y]/(\mathcal{F}(X,Y,1), g_\ell(X))$; then we recover $c_\ell = (k^2+q)/k \bmod \ell$. This change was crucial, because it was then possible to use polynomials of degree $(\ell-1)/2$ rather than of degree $(\ell^2-1)/2$. Elkies gave an algorithm to compute g_ℓ using further properties of modular equations. Another approach was given in [8].

Atkin [2] gave his own solution to the problem of computing $g_\ell(X)$ using more modular equations and modular forms. Though rather tricky to implement, his approach is very fast in practice.

Recently, Couveignes and Morain showed how to use powers of small Elkies primes [12].

All these ideas are also described in [41] and were implemented [2, 24, 36, 35]. The results are striking, the record being that of the computation of the cardinality of a curve modulo a prime p of 500 digits (see [27]).

The only remaining problem was that these ideas could not work when $p = 2$ (and more generally $p < \ell$). As a matter of fact, the theory of Atkin and Elkies remains valid, but one could no longer use the ordinary parameterization of elliptic curves via Weierstrass' $\wp$-functions to get a suitable way of computing g_ℓ. Couveignes solved this problem in his thesis [10], using formal groups as a powerful tool.

4.3 Remark on supersingular curves

Suppose one wants to check whether E is supersingular or not. First of all, it is easy to check for some random points P if $(q+1-c)P = O_E$ for one of the c's above. If not, we can proceed to compute the number of points as described in section 4. If this condition is met, then we can prove that E is supersingular as described in [41]. We just have to verify that all modular equations $\Phi_\ell(X, j(E))$ have factors of degree 1 and 2 only for enough ℓ's such that $\prod \ell > 4\sqrt{q}$.

4.4 Finding the isogenous curve in small characteristic

We suppose from now on that E is not supersingular.

The problem we face is the following. We know that E is ℓ-isogenous to a curve E^* whose invariant j^* is known. As a matter of fact, we select one of the roots F^* of $\Phi_\ell(X, j(E))$ in K and then j^* is a root of $\Phi_\ell(F^*, Y)$ (see the references already given for more precisions). It can happen that this polynomial has several roots. One must try all of them to get the right one (see the remark at the end of section 7.1.2). The invariant j^* does not characterize completely E^*, as is well known. The problem is to find the equation of this curve E^*.

In the case of large characteristic, Elkies and Atkin gave very powerful algorithms to compute the equation of E^*. In the small characteristic case, we now show how to do this using the Hasse invariant.

Since E and E^* are isogenous, one has by Theorem 3.3

$$\mathrm{N}_{K/GF(p)}(c_p(E)) \equiv \mathrm{N}_{K/GF(p)}(c_p(E^*)) \bmod p$$

or

$$\mathrm{N}_{K/GF(p)}(c_p(E^*)/c_p(E)) \equiv 1 \bmod p,$$

that is

$$c_p(E^*) = \epsilon^{p-1} c_p(E) \tag{15}$$

where ϵ is any element of $GF(p)^*$.

We now give some details for the different characteristics. When $p = 2$, one has $c_p(E) = a_1 = 1$. In the case where we consider $E = [a_6]$, we deduce that the curve E^* we are looking for is simply $[1/j^*]$.

When $p = 3$, we look for $E^* = [a_2^*, a_6^*]$ such that $j(E^*) = j^*$. The curve E^* is given by $[\lambda\gamma, \lambda^3]$, where γ is the unique cubic root of $-j^*$ and λ is such that $c_p(\lambda\gamma, \lambda^3) = \epsilon^2 c_p(E)$ or $\lambda = \epsilon^2 a_2/\gamma$.

For the remaining case where $p > 3$, we look for $E^* = [3k^*\lambda^2, 2k^*\lambda^3]$ where $k^* = j^*/(1728 - j^*)$ and λ satisfies $c_p(3k^*\lambda^2, 2k^*\lambda^3) = c_p(E)$. It follows from Theorem 3.3 that

$$c_p(3k^*\lambda^2, 2k^*\lambda^3) = \lambda^{(p-1)/2} c_p(3k^*, 2k^*)$$

and thus we have to solve

$$\lambda^{(p-1)/2} = \epsilon^{p-1} \frac{c_p(E)}{c_p(3k^*, 2k^*)} \tag{16}$$

in K. Finding the solution of this equation can be done in $O(p^2 \log p)$ operations, which is very costly when p is large.

4.5 The case $\ell = p$

The case $\ell = p$ can be treated easily. First of all, using Theorem 3.3, one knows $c \bmod p$. Then, from Corollary 3.2, we know that f_{p^e} has a factor g_{p^e} of degree $p^{e-1}(p-1)/2$. Moreover, as long as $p^e < q$, then equation (14) is simply

$$\phi_E^2 - c\phi_E \equiv 0 \bmod p^e$$

which shows that ϕ_E has two distinct eigenvalues (since E is not supersingular), one of which is c and is associated to g_{p^e}.

5 Couveignes's algorithm: the theory

5.1 An overview

Let E and E^* be two elliptic curves defined over K by

$$\begin{array}{rrcl} E: & Y^2 + a_1XY + a_3Y & = & X^3 + a_2X^2 + a_4X + a_6, \\ E^*: & Y^2 + a_1^*XY + a_3^*Y & = & X^3 + a_2^*X^2 + a_4^*X + a_6^*, \end{array}$$

such that there exists an isogeny I of degree ℓ between them given by

$$\begin{array}{rrcl} I: & E & \longrightarrow & E^* \\ & (X,Y) & \longmapsto & \left(\dfrac{g(X)}{h^2(X)}, \dfrac{r(X) + Yt(X)}{h^3(X)}\right), \end{array}$$

where $g(X)$, $h(X)$, $r(X)$ and $t(X)$ are polynomials of degree ℓ, $(\ell-1)/2$, $3(\ell+1)/2$ and $3(\ell-1)/2$. The aim of Couveignes's algorithm [10] is the computation of $g(X)$ and $h(X)$.

We look at the abscissa of I only. It is equivalent to search for g and h 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 $\hat{h}(Z) = Z^{(\ell-1)/2}h(Z)$. We note that $\hat{g}$ has degree ℓ. 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 (see section 7.3.2 for more details). Reciprocally, given the 2ℓ first coefficients, one can recover $F(Z)$ exactly. 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. See section 7.3 for more details.

Enumerating the putative isogenies is possible using the formal groups associated to E and E^* as described below.

5.2 Morphisms of formal groups

As shown in section 2.3, associated to E and E^*, there are two formal groups $\mathcal{E}$ and $\mathcal{E}^*$,

$$\begin{array}{rrcl} \mathcal{E}: & t^3 + a_1ts + a_2t^2s + a_3s^2 + a_4ts^2 + a_6s^3 - s & = & 0, \\ \mathcal{E}^*: & t^3 + a_1^*ts + a_2^*t^2s + a_3^*s^2 + a_4^*ts^2 + a_6^*s^3 - s & = & 0. \end{array}$$

A *morphism* of formal groups 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 a morphism $\mathcal{M}$ between $\mathcal{E}$ and $\mathcal{E}^*$, 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 (1)). *A fortiori*, the series $\mathcal{U}(t)$ satisfies

$$\mathcal{U}(t_1 \oplus t_2(\tau)) = \mathcal{U}(t_1(\tau)) \oplus \mathcal{U}(t_2(\tau)) \tag{17}$$

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 [17]).

Coming back to our problem, $\hat{I}$ gives rise to a morphism $\mathcal{I}$ between $\mathcal{E}$ and $\mathcal{E}^*$, and to a series $\mathcal{W}$. 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 (17), 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. We will compute the precise number of such series in the following section.

5.3 Finding conditions satisfied by morphisms

Let us now look at the properties satisfied by morphisms between $\mathcal{E}$ and $\mathcal{E}^*$, or more precisely by the associated series. We will compute the first $\mathcal{L}$ coefficients of

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

by induction. Let us assume that $u_1, \ldots, u_{i-1}$ are known. An ingenious exploitation of equation (17) will allow us to calculate u_i.

Let us specialize $t_1(\tau) = \tau$ and $t_2(\tau) = A\tau$ where A is in K. Equation (17) becomes

$$\mathcal{U}(\tau \oplus A\tau) = \mathcal{U}(\tau) \oplus \mathcal{U}(A\tau). \tag{18}$$

Let us extract the coefficient of τ^i in (18). We know from (6) that

$$\tau \oplus A\tau = (1 + A)\tau + O(\tau^2)$$

so that

$$\mathcal{U}(\tau \oplus A\tau) = \sum_{k=1}^{\infty} u_k((1 + A)\tau + O(\tau^2))^k$$

and u_i appears alone in the coefficient of τ^i as $(1 + A)^i u_i$ among terms depending only on u_1, u_2, ..., u_{i-1}. On the other hand,

$$\mathcal{U}(\tau) \oplus \mathcal{U}(A\tau) = \mathcal{U}(\tau) + \mathcal{U}(A\tau) + P(\mathcal{U}(\tau), \mathcal{U}(A\tau))$$

where $P(\mathcal{U}(\tau), \mathcal{U}(A\tau))$ contains monomials of total degree greater than 1 in $\mathcal{U}(\tau)$ and $\mathcal{U}(A\tau)$. This means that u_i appears in the coefficient of τ^i as $(1 + A^i)u_i$ among terms depending only on u_1, u_2, ..., u_{i-1}. From this, we deduce that

$$u_i\left((1 + A)^i - 1 - A^i\right) + e_i(A, u_1 \ldots, u_{i-1}) = 0, \tag{19}$$

with e_i a multivariate polynomial. If $(1 + A)^i \neq 1 + A^i$, then this relation gives us u_i. We see that this condition on A cannot be met when i is a power of p, but for other values of i, we can find A such that it is realized, at least if $i < q$.

Suppose now that $i = p^e$. We will write $\Phi(t)$ (resp. $\Phi^*(t)$) for $\Phi_{p,E}(t)$ (resp. $\Phi_{p,E^*}(t)$); in the same vein, we put $c = c_p(E)$ and $c^* = c_p(E^*)$. We take advantage of the fact that

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

obtained from equation (17). Let us write $\tilde{\mathcal{U}}(t) = \sum_{k=1}^{\infty} \tilde{u}_k t^k$. Using (11) we deduce that

$$\tilde{\mathcal{U}}(\tau) \circ \Phi(\tau) = \Phi^*(\tau) \circ \mathcal{U}(\tau). \tag{20}$$

Here, the equality of the coefficients of X^i on the left and right hand side leads to a non trivial equation of degree p in $\tilde{u}_i$:

$$c^{p^{e-1}} \tilde{u}_i - \sqrt[p]{c^*} u_i = f_i(\tilde{u}_1, \ldots, \tilde{u}_{i-1}), \tag{21}$$

with f_i a multivariate polynomial. We put

$$\eta = \frac{c^{(p^e-1)/(p-1)}}{\epsilon}$$

and we rewrite (21) as

$$\left(\frac{u_i}{\eta}\right) - \left(\frac{u_i}{\eta}\right)^p = f_i'. \tag{22}$$

We will see in section 7.1.2 how to solve this equation. Obviously, it has at most p solutions.

Let us look at the case $i = 1 = p^0$. The corresponding equation is simply

$$c u_1^p = u_1 c^*.$$

Using (15), one gets

$$u_1^{p-1} = \epsilon^{p-1}.$$

We remark that taking $\epsilon = 1$ simplifies the problem, since then u_1 is in the prime field and not in the whole field.

5.4 Enumerating all morphisms

We can summarize the results of the preceding section as follows. Once u_{p^e} is fixed, all coefficients u_j for $p^e < j < p^{e+1}$ are uniquely determined. In this way, we can count the number of different truncated morphisms up to order $\mathcal{L}$. Let $p^r < \mathcal{L} < p^{r+1}$. Then there are at most p^{r+1} distinct series. For each e, $1 \le e \le r$, there are at most p values for u_{p^e}; if $e = 0$ this number is at most $p - 1$ since $u_1 = 0$ is not valid. Therefore, there are $p^r(p-1)$ morphisms $\mathcal{U}$. We need to enumerate them in order to find the one that comes from an isogeny.

5.4.1 First approach

It consists in testing all possible values of u_{p^e} for each e, using a backtracking procedure, that is straightforward from the explanations given above.

5.4.2 Second approach

We can take advantage of the fact that the set of morphisms between $\mathcal{E}$ and $\mathcal{E}^*$ is a $\mathbb{Z}_p$-module of dimension 1. So, 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.

We can reduce the number of tentative morphisms, using the following result.

Proposition 5.1 *Let k be an integer ≥ 1 and N an integer satisfying $0 \le N < p^k$. Then one has*

$$[p^k - N]_E(t) = -[N]_E(t) + O(t^{p^k}). \tag{23}$$

Proof: The result follows easily from (2.2) since

$$[p^k - N]_E(t) \oplus [N]_E(t) = [p^k]_E(t) = c_p(E)^{p^{k-1}} t^{p^k} + O(t^{2p^k}).\square$$

We deduce from this result that

$$[p^{r+1} - N] \circ \mathcal{U} = [-N] \circ \mathcal{U} + O(t^{p^{r+1}}).$$

Furthermore, the morphisms $\mathcal{W}$ and $-\mathcal{W}$ yield the same isogeny $\hat{I}$. So, at least one morphism $[N] \circ \mathcal{U}$ for $N < p^{r+1}/2$ and N prime to p is equal to $\mathcal{W}$ or $-\mathcal{W}$ and is associated to $\hat{I}$. That is to say, we have to compute at most $p^r(p-1)/2$ morphisms $\mathcal{M}$. This amounts to considering in the first alternative only one half of the potential u_1, in fact $u_1 = 1, \ldots, (p-1)/2$ if p is odd and only $u_1 = 1$ when $p = 2$.

As a final point in this section, we note the important result:

Proposition 5.2 *When $p = 2$,*

$$\mathcal{U}(t) \oplus \mathcal{U}\left(\frac{t}{1+t}\right) = 0;$$

and when p is odd, $\mathcal{U}$ is odd.

Proof: this follows from the fact that the opposite of t is given by equation (7). $\square$

6 Series computations

The implementation of Couveignes's algorithm requires the use of fast algorithms for series computations. As will be described in section 7, the algorithms we need are concerned with incremental computations: we will find the coefficients of a particular series, one at a time, using other series, some of which are also known coefficient by coefficient.

After describing the incremental algorithms for the four basic operations, we will apply these ideas to some additional algorithms needed in the formal group. Then, we will give an incremental version of the Brent and Kung algorithm for composition of series.

In these sections, we note for any series $\mathcal{A}(\tau) = \sum_{i \geq v}^{\infty} a_i \tau^i$ of valuation v in $K[[\tau]]$, $\mathcal{A}(\tau)_k$ the finite sum $\sum_{i=v}^{k} a_i \tau^i$. The i-th coefficient of a series $\mathcal{A}$ will always denote a_i.

After that, we describe the computations performed on series. In the remaining of the paper, our unit of cost will be the time needed to perform a multiplication in K, a unit being thus $O(n^2 (\log p)^2)$ bit complexity. We make the general assumption that multiplying two series with m terms uses $O(m^\mu)$ units; of course, we assume $1 < \mu \leq 2$.

6.1 Some basic facts about series

First, we give some easy results about addition, multiplication and division of two series $(\mathcal{A}(t), \mathcal{B}(t))$ in $K[[t]]^2$. Let $\mathcal{C}(t) \in K[[t]]$ be the result of these operations. We note

$$\mathcal{A}(t) = \sum_{i=0}^{\infty} a_i t^i, \ \mathcal{B}(t) = \sum_{i=0}^{\infty} b_i t^i \text{ and } \mathcal{C}(t) = \sum_{i=0}^{\infty} c_i t^i.$$

The proofs of Propositions 6.1, 6.2 and 6.3 can be found for instance in [22, chap. 4.7].

Proposition 6.1 *Let $\mathcal{C}(t) = \mathcal{A}(t) \pm \mathcal{B}(t)$. Then, we obtain, for any positive integer L, c_L from a_L and b_L by*

$$c_L = a_L \pm b_L$$

with one addition/subtraction in K.

Proposition 6.2 *Let $\mathcal{C}(t) = \mathcal{A}(t)\mathcal{B}(t)$, we obtain, for any positive integer L, c_L from $(a_0, \ldots, a_L)$ and $(b_0, \ldots, b_L)$ by*

$$c_L = \sum_{i=0}^{L} a_i b_{L-i}.$$

with $L+1$ multiplications in K.

Proposition 6.3 *Let $\mathcal{C}(t) = \mathcal{A}(t)/\mathcal{B}(t)$ when $b_0 \neq 0$, we obtain, for any positive integer L, c_L from a_L, $(b_0, \ldots, b_L)$ and $(c_0, \ldots, c_{L-1})$ by*

$$c_L = \left(a_L - \sum_{i=0}^{L-1} c_i b_{L-i} \right) / b_0.$$

with L multiplications and one division in K.

6.2 Computations in the formal group

Let $(\mathcal{V}(t), \mathcal{S}(\mathcal{V}(t)))$ be a formal point of $\mathcal{E}$. We note

$$\mathcal{V}(t) = \sum_{i=1}^{\infty} v_i t^i \text{ and } \mathcal{S}(\mathcal{V}(t)) = \sum_{i=3}^{\infty} \varpi_i t^i.$$

As noticed in section 2.3.2, computing the coefficients $s_1, \ldots, s_L$ of $\mathcal{S}(t)$ from t can be done in $O(L^2)$ multiplications. Proposition 6.4 gives more details about this.

Proposition 6.4 *We can obtain ϖ_L from $(\varpi_3, \ldots, \varpi_{L-1})$ and $(v_1, \ldots, v_{L-2})$ with $O(L)$ multiplications in K.*

Proof: As $(\mathcal{V}(t), \mathcal{S}(\mathcal{V}(t)))$ is an element of the formal group defined by $\mathcal{E}$,

$$\mathcal{V}^3 + a_1\mathcal{V}\mathcal{S}(\mathcal{V}) + a_2\mathcal{V}^2\mathcal{S}(\mathcal{V}) + a_3\mathcal{S}(\mathcal{V})^2 + a_4\mathcal{V}\mathcal{S}(\mathcal{W})^2 + a_6\mathcal{S}(\mathcal{V})^3 = \mathcal{S}(\mathcal{V}). \tag{24}$$

As shown in proposition 6.1, 6.2 and since the valuation of $\mathcal{V}(t)$ is 1 and the valuation of $\mathcal{S}(\mathcal{V}(t))$ is 3, the L^{th} coefficient of $\mathcal{V}^3$ depends on $(v_1, \ldots, v_{L-2})$, the L^{th} coefficient of $\mathcal{V}\mathcal{S}(\mathcal{V})$ depends on $(v_1, \ldots, v_{L-3})$ and $(\varpi_3, \ldots, \varpi_{L-1})$, the L^{th} coefficient of $\mathcal{V}^2\mathcal{S}(\mathcal{V})$ depends on $(v_1, \ldots, v_{L-4})$ and $(\varpi_3, \ldots, \varpi_{L-2})$, the L^{th} coefficient of $\mathcal{S}^2(\mathcal{V})$ depends on $(\varpi_3, \ldots, \varpi_{L-3})$, the L^{th} coefficient of $\mathcal{V}\mathcal{S}^2(\mathcal{V})$ depends on $(v_1, \ldots, v_{L-6})$ and $(\varpi_3, \ldots, \varpi_{L-4})$ and the L^{th} coefficient of $\mathcal{S}(\mathcal{V})^3$ depends on $(\varpi_3, \ldots, \varpi_{L-6})$.

Therefore, from equation (24), we deduce that ϖ_L is a multivariate polynomial in $(v_1, \ldots, v_{L-2})$ and $(\varpi_3, \ldots, \varpi_{L-1})$.

Furthermore, since we saw that getting the L^{th} coefficient of a product of series can be done with $O(L)$ multiplications, the L^{th} coefficient of $\mathcal{S}(\mathcal{V})$ can be computed with $O(L)$ multiplications too. □

Proposition 6.5 *Let* $\mathcal{A}(t) = \sum_i a_i t^i$ *and* $\mathcal{A}'(t) = \sum_i a'_i t^i$ *be two formal series and put* $\mathcal{S}(t) = \mathcal{S}(\mathcal{A}(t)) = \sum_{i=3}^{\infty} \varpi_i t^i$ *(resp.* $\mathcal{S}'(t) = \mathcal{S}(\mathcal{A}'(t)) = \sum_{i=3}^{\infty} \varpi'_i t^i$*). We can obtain* $(\mathcal{A}(t) \oplus \mathcal{A}'(t))_L$ *from the truncated formal points* $(\mathcal{A}(t)_L, \mathcal{S}_{L+1}(t))$ *and* $(\mathcal{A}'(t)_L, \mathcal{S}'_{L+1}(t))$ *with* $O(L^2)$ *multiplications in* K*.*

Proof: Let us apply now the formulae of section 2.3.3 to compute $(\mathcal{A}(t) \oplus \mathcal{A}'(t))_L$. We deduce again from the valuation of the series that the L^{th} coefficient of the series

$$\lambda(t) = \frac{\mathcal{S}(t) - \mathcal{S}'(t)}{\mathcal{A}(t) - \mathcal{A}'(t)},$$

depends on $(a_1, \ldots, a_{L-1})$ and $(\varpi_3, \ldots, \varpi_{L+1})$ (resp. a'_i and ϖ'_i with the same indices). Furthermore, the valuation of $\lambda(t)$ is two. Then, the L^{th} coefficient of the series

$$\nu(t) = \mathcal{S}(t) - \lambda(t)\mathcal{A}(t)$$

depends on $(a_1, \ldots, a_{L-2})$ and $(\varpi_3, \ldots, \varpi_L)$. The valuation of $\nu(t)$ is three. It follows that the L^{th} coefficient of the series

$$t_i(t) = -\mathcal{A}(t) - \mathcal{A}'(t) - \frac{a_1\,\lambda(t) + 2\,a_4\,\nu(t)\,\lambda(t) + a_2\,\nu(t) + 3\,a_6\,\nu(t)\,\lambda(t)^2 + a_3\,\lambda(t)^2}{1 + a_4\,\lambda(t)^2 + a_2\,\lambda(t) + a_6\,\lambda(t)^3}$$

depends on $(a_1, \ldots, a_L)$ and $(\varpi_3, \ldots, \varpi_{L+1})$ (ditto with a'_i and ϖ'_i). The valuation of $t_i(t)$ is two. Then, the L^{th} coefficient of the series

$$s_i(t) = \lambda(t) t_i(t) + \nu(t),$$

depends on $a_1, \ldots, a_{L-2}$ and $\varpi_3, \ldots, \varpi_L$ (same for the a'_i and ϖ'_i). The valuation of $s_i(t)$ is three. Therefore, from

$$\mathcal{A}(t) \oplus \mathcal{A}'(t) = \frac{t_i(t)}{-1 + a_1\,t_i(t) + a_3\,s_i(t)}$$

we deduce that the L^{th} coefficient of the series depends on $(a_1, \ldots, a_L)$ and $(\varpi_3, \ldots, \varpi_{L+1})$ (same on the a'_i and ϖ'_i).

Furthermore, since we saw that getting the first L coefficients of a product or division of series can be done with $O(L^2)$ multiplications, L coefficients of this series can be computed with $O(L^2)$ multiplications too. □

This last result can be proved in the same way from the formulae of section 3.3.1.

Proposition 6.6 *We can obtain the first* L *terms of the series* $\mathcal{R}(t, \mathcal{S}(t)) \circ \mathcal{V}(t)$ *from the truncated formal point* $(\mathcal{V}(t)_L,\ \mathcal{S}(\mathcal{V}(t))_{L+1})$ *with* $O(L^2)$ *multiplications in* K*.*

6.3 An incremental algorithm for composition of series

Let $f = \sum_{i=1}^{\infty} a_i t^i$ and $g = \sum_{i=0}^{\infty} b_i t^i$ be two formal series in $K[[t]]$. We want to compute the series

$$h = g \circ f = \sum_{i=0}^{\infty} c_i t^i$$

incrementally. More precisely, we assume f is known up to order L and that we need to compute the coefficients $h_0, h_1, \ldots, h_L$ one at a time, or equivalently, given all series at order i, find h_i. We do this by an incremental version of the algorithm of Brent and Kung [6].

Let B be an integer $\leq L$ that we will determine later on. Let i be an integer less than L and assume we know all coefficients of g (resp. h) of index $< i$. We are looking for c_i. To compute $g_i \circ f$, we write

$$g_i(t) = \sum_{k=0}^{i} b_k t^k = \sum_{0 \leq j \leq i/B} G_j(t) t^{Bj}$$

where $G_j(t)$ is a polynomial of degree at most $B-1$ in t. Then

$$g_i \circ f = \sum_{0 \leq j \leq i/B} G_j(f) f^{Bj}.$$

We precompute $f_j = f^j$ for $0 \leq j \leq B$ and $F_j = f_B^j$ for $0 \leq j \leq L/B$, up to order L. Now, put $i = JB + I$ with $0 \leq I < B$. One gets

$$g_i \circ f = \sum_{0 \leq j < J} G_j(f_1) F_j + \left(\sum_{k=0}^{I-1} b_{JB+k} f_k \right) F_J + b_i f_I F_J = \Sigma_{1,i} + \Sigma_{2,i} F_J + b_i f_I F_J.$$

(We use the convention that if $I = 0$, $\Sigma_{2,i} = 0$.) It is easy to see that all terms of $\Sigma_{1,i}$ and $\Sigma_{2,i}$ up to order L (not i) depend only on the first coefficients b_1, ..., b_{i-1}. Now, it is easy to get the i-th term of $\Sigma_{2,i} F_J$ in $O(i)$ steps, as well as that of $f_I F_J$, which enables us to find the desired coefficient c_i.

Once this is done, we have to update the series. Note that we do not need the terms of indices $\leq i$. We see that if $I < B-1$, then $\Sigma_{1,i+1} = \Sigma_{1,i}$ and

$$\Sigma_{2,i+1} = \Sigma_{2,i} + b_i f_I.$$

In this case, updating the series costs $O(L-i)$. If $I = B-1$, then

$$\Sigma_{1,i+1} = \Sigma_{1,i} + (\Sigma_{2,i} + c_i f_I) F_J$$

and $\Sigma_{2,i+1} = 0$. Since we only need the terms of degree $> i$, this costs $O((L-i)^\mu)$.

Precomputing the f_j's costs

$$\sum_{j=2}^{B} (L-j)^\mu,$$

that of the F_j's is

$$\sum_{j=2}^{L/B} (L-jB)^\mu$$

and leads to a storage of $O(B + L/B)$ series with L terms. The cost of the computations of all $\Sigma_{1,i}$ and $\Sigma_{2,i}$ is also

$$\sum_{j=2}^{L/B} (L-jB)^\mu.$$

So we need minimize:

$$\sum_{j=2}^{B} (L-j)^\mu + 2 \sum_{j=2}^{L/B} (L-jB)^\mu.$$

We approximate this quantity with the corresponding integrals and so we have to minimize:

$$C(B) = (L-2)^{\mu+1} - (L-B)^{\mu+1} + 2(L-2B)^{\mu+1}/B.$$

We differentiate this w.r.t. B and replace B by $L\beta$. We develop the derivative as a function of β and find:

$$C'(B) = L^{\mu+1}\left(-2 + ((\mu+1)L + 4\mu^2 + 4\mu)\beta^2 + O(\beta^3)\right).$$

This leads to the choice of

$$\beta = \left(\sqrt{\frac{\mu+1}{2}}L\right)^{-1}$$

or

$$B = \sqrt{\frac{2}{\mu+1}}L^{1/2}.$$

Hence the overall cost of this phase is approximately $2BL^{\mu+1/2}$ with a storage in $O(L^{1/2})$.

Remark. The role of the constant $\sqrt{\frac{2}{\mu+1}}$ is not very important, since it is always in the interval $[0.816, 1]$.

7 Efficient implementation of Couveignes's algorithm

In this section, we give the algorithms needed to implement Couveignes's ideas, and deduce from this the complexity of the method. First we describe the precomputations that depend on p alone: we compute the multiplication by p and show how to compute the solution of the equation $X - X^p = \alpha$ in K. Then we recall some basic facts on the algorithms that can be used to recover a fraction from its series expansion. We end this section with the two strategies for finding the morphisms and analyze the complexities.

7.1 Precomputations for p alone

7.1.1 Multiplication by p

The first thing we need is to compute the multiplication by p and the fraction $\mathcal{R}(t,s)$, as indicated in section 3.3.4. These computations do not depend on ℓ. The cost is $O(p^2 \log p)$ elementary operations.

7.1.2 Solving $X - X^p = \alpha$

We use the following result from [29]:

Proposition 7.1 *The equation*

$$\beta - \beta^p = \alpha \tag{25}$$

has a solution in K if and only if $\mathrm{Tr}_{K/GF(2)}(\alpha) = 0$. Moreover, if θ has trace 1, then a solution of this equation is:

$$\beta = \alpha\theta^p + (\alpha + \alpha^p)\theta^{p^2} + \cdots + (\alpha + \alpha^p + \cdots + \alpha^{p^{n-2}})\theta^{p^{n-1}}. \tag{26}$$

Remark that if (25) has a solution β, then $\beta + k$ is a solution for all k in the prime field $GF(p)$. It is also easy to see that the map $\alpha \mapsto \beta$ is linear. Having computed the matrix of this application, all equations (22) can be solved by applying this matrix to the coefficients of this equation.

Note also the very important fact that the computation of this matrix depends only on p and n and not on ℓ. This means that it can be performed only once before any isogeny computation. The cost of setting up this matrix can thus be neglected. Note that we need to store $O(n^2)$ elements in $GF(p)$ and that the time needed to apply the matrix is $O(1)$ (multiplications in K).

Remark. In the process of SEA, we find the isogenous curve by its j-invariant, which is a root of a polynomial. It can happen that there are several roots to this polynomial, only one of which being the invariant we are looking for. The preceding process can very frequently detect false curves, because one of the equations (21) does not have any solution.

7.2 Finding one morphism

The heart of the algorithm is the computation of morphisms $\mathcal{M}$ (or more precisely the associated series $\mathcal{U}$) with equation (18) and equation (20).

Now, we distinguish two steps: a precomputation step and then the actual computation.

7.2.1 Precomputation phase

Series which are independent of $\mathcal{U}$ are completely computed while only a few terms of the other series can be initialized. We also perform some precomputations for use in the composition of series as described in the next sections. We assume we want $\mathcal{L}$ terms of $\mathcal{U}$.

Precisely, we precompute:

1. $\mathcal{S}(\tau)_{\mathcal{L}+1}$ from $(\tau)_{\mathcal{L}}$ with proposition 6.4;
2. A such that $(1+A)^i \neq 1 + A^i$ for all $i \leq \mathcal{L}$ (this implies in particular that $q > \mathcal{L}$).
3. $\mathcal{S}(A\tau)_{\mathcal{L}+1}$ from $\mathcal{S}(\tau)_{\mathcal{L}+1}$.
4. The series
$$((\tau \oplus A\tau(\tau))_{\mathcal{L}}, \mathcal{S}^*(\tau \oplus A\tau(\tau))_{\mathcal{L}+1}) = ((\tau)_{\mathcal{L}}, \mathcal{S}(\tau)_{\mathcal{L}+1}) \oplus ((A\tau)_{\mathcal{L}}, \mathcal{S}(A\tau)_{\mathcal{L}+1})$$
from the addition law of section 2.3.3.
5. The truncated series $\Phi(\tau)_{p^r} = \mathcal{R}(\tau, \mathcal{S}(\tau))_{p^r+1}$ and its powers up to the order needed for the fast substitution algorithm. (The choice of these will be explained later).
6. All the intermediate series to compute $\mathcal{R}^*(\mathcal{U}(\tau),\ \mathcal{S}^*(\mathcal{U}(\tau)))$ as far as possible as in proposition 6.6. For instance, in characteristic 2,
$$\mathcal{R}_2^*(t,s) = \frac{t^3 + \tilde{a}_6^* s^2 t}{t^2 + \tilde{a}_6^* s^2 + \tilde{a}_6^* t^2 s + s + ts + t^3 + \tilde{a}_6^* t s^2}$$
and we initialize all the monomials of this fraction once substituted $(\mathcal{U}(\tau), \mathcal{S}^*(\mathcal{U}(\tau)))$ for (t,s); $\mathcal{U}(\tau)_1 = \tau$, $\mathcal{S}^*(\mathcal{U}(\tau))_3 = \tau^3$, $\mathcal{U}(\tau)\mathcal{S}^*(\mathcal{U}(\tau))_4 = \tau^4$, $\mathcal{U}^2(\tau)_2 = \tau^2$, $\mathcal{S}^*(\mathcal{U}(\tau))_6^2 = \tau^6$, ...
7. As in step 6, all the intermediate series to compute $\mathcal{U}(\tau) \oplus \mathcal{U}(A\tau)$ as in the proof of proposition 6.5; $\mathcal{U}(A\tau)_1 = A\tau$, $\mathcal{S}^*(\mathcal{U}(\tau))_3 = A^3\tau^3$, $\lambda(\tau)_2 = (A^2 + A + 1)\tau^2$, $\nu(\tau)_3 = (A^2 + A)\tau^3$, ...

Complexity. Step 1 costs $O(\mathcal{L}^2)$ multiplications in K; step 2 costs at least $O(\mathcal{L})$ multiplications; step 3 needs $O(\mathcal{L})$ multiplications; step 4, $O(\mathcal{L}^\mu)$ multiplications in K; step 5, $O(p\mathcal{L}^\mu)$ multiplications to get $\Phi(\tau) = \mathcal{R}(\tau)_{p^r}$, and step 6, step 7 can be performed in $O(1)$ multiplications.

So, the complexity of this phase is at most $O(\mathcal{L}^\mu)$ with a storage in $O(p\mathcal{L})$ (since the fraction $\mathcal{R}$ has $O(p)$ terms).

7.2.2 Finding the morphism

At the beginning of the i^{th} iteration, $\mathcal{U}(\tau)_{i-1}$ is known and as far as the intermediate series are concerned, $\mathcal{S}(\mathcal{U}(\tau))_{i+1}$, $\mathcal{U}(A\tau)_{i-1}$, $\mathcal{S}(\mathcal{U}(\tau))_{i+1}$, $\lambda(\tau)_i$, $\nu(\tau)_{i+1}\dots$ are known by proposition 6.4. Then, formal computations enable us to compute u_i whose knowledge allows us to update the intermediate series in order to be ready for the $(i+1)^{\text{th}}$ iteration. We study both cases $i \neq p^e$ and $i = p^e$ separately.

The case $i \neq p^e$. We find u_i using

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

The left hand side will give us an equation of the form $(1+A)^i u_i + d$ and the right hand side of the form $(1+A^i)u_i + b$. We will then solve $u_i = (d-b)/(1+A^i-(1+A)^i)$ and get u_i.

Step 1-a: we need to compute the i^{th} coefficient of $\mathcal{U}(\tau \oplus A\tau)$. We do this using the algorithm described in section 6.3. We get an equation of the type $(1+A)^i u_i + d$.

Step 1-b: we have to calculate the i^{th} coefficient of $\mathcal{U}(\tau) \oplus \mathcal{U}(A\tau)$ as a function of u_i. To perform that, we follow step by step the computations done in the proof of proposition 6.5. Since each intermediate series needed in this proof is known up to i, one can obtain as a function of u_i, the $(i+2)^{\text{th}}$ coefficient of $\mathcal{S}(\mathcal{U}(\tau))$, the i^{th} coefficient of $\mathcal{U}(A\tau)$, the $(i+2)^{\text{th}}$ coefficient of $\mathcal{S}(\mathcal{U}(\tau))$, the $(i+1)^{\text{th}}$ coefficient of $\lambda(\tau)$ and so on. Finally the coefficient we are looking for is equal to $(1+A^i)u_i + b$.

The complexity of this phase is $O(i)$.

The case $i = p^e$. We find u_i with equation (20) that we rewrite as

$$\tilde{\mathcal{U}}(\Phi(\tau)) = \mathcal{R}^*(\mathcal{U}(\tau), \mathcal{S}^*(\mathcal{U}(\tau))).$$

This enables us to use the same techniques as the one described just above, namely applying $\tilde{\mathcal{U}}$ to a known series using precomputations and computing a rational fraction in two series.

Step 2-a: we compute as a function of u_i the i^{th} coefficient of $\tilde{\mathcal{U}}(\tau) \circ \Phi(\tau)$. This is done as in step 1-a. This coefficient is equal to $a\tilde{u}_i + d$.

Step 2-b: we compute formally the i^{th} coefficient of $\mathcal{R}^*(\mathcal{U}(\tau), \mathcal{S}^*(\mathcal{U}(\tau)))$. To perform that, we proceed as in step 1-b. We have to compute as a function of u_i the $(i+2)^{\text{th}}$ coefficient of $\mathcal{S}^*(\mathcal{U}(\tau))$, the $(i+2)^{\text{th}}$ coefficient of $\mathcal{S}^*(\mathcal{U}(\tau))$, ... This coefficient is equal to $u_i + b$.

Finally $u_i^p - a^p u_i + b^p - d^p = 0$ and we choose one of the roots for u_i.

We update the intermediate series, that is to say we obtain from $\mathcal{U}(\tau)_i$ the intermediate truncated series $\mathcal{S}(\mathcal{U}(\tau))_{i+2}$, $\mathcal{U}(A\tau)_i$, $\mathcal{S}(\mathcal{U}(\tau))_{i+2}$, $\lambda(\tau)_{i+1}$, $\nu(\tau)_{i+2}\dots$ as shown in the proofs of proposition 6.5 or 6.6.

Complexity. We see that the computation of one morphism is dominated by the composition of series. Hence, the overall cost of this is $O(\mathcal{L}^{\mu+1/2}) = O(\ell^{\mu+1/2})$.

7.3 Isogeny testing

Suppose we are given a morphism $\mathcal{M}(t)$ between $\mathcal{E}$ and $\mathcal{E}^*$. Put

$$Z^*(t) = \frac{\mathcal{S}^*(\mathcal{M}(t))}{\mathcal{M}(t)}$$

and we want to find a series $\hat{M}$ such that

$$Z^*(t) = \hat{M}(Z(t)).$$

Once we have done this, we need to compute a fraction whose expansion coindices with that of $\hat{M}$.

7.3.1 From $\mathcal{M}$ to $\hat{M}$

We know the expansion of $Z(t) = t^2 + a_1 t^3 + (a_1^2 + a_2)t^4 + O(t^5)$ and we suppose that $Z^*(t) = m_2 t^2 + \cdots + m_{4\ell+1} t^{4\ell+1} + O(t^{4\ell+2})$. We are looking for the coefficients of $\hat{M}(u) = \hat{m}_1 u + \hat{m}_3 u^3 + \cdots + \hat{m}_{2\ell+1} u^{2\ell+1} + O(u^{2\ell+2})$. We will find these coefficients one at a time. Since we will have to perform many isogeny tests, it is worth precomputing all odd powers of $Z(t)$, namely $Z_i(t) = Z(t)^i$ for $1 \leq i \leq 4\ell+1$, i odd.

The procedure is the following:

procedure RecoverSeriesInZ

1. $\hat{m}_1 := m_2$; $W := W - \hat{m}_1 Z_1$;
2. **for** $i = 1$ **to** ℓ **do**

   {at this point, $W = wt^{2i+1} + O(t^{2i+2})$}

   (a) $\hat{m}_{2i+1} := w$;

   (b) $W := W - \hat{m}_{2i+1} Z_{2i+1}$;

The precomputation phase requires $O(\ell^{\mu+1})$ operations and is done only once. The computation phase takes $O(\ell^2)$.

7.3.2 Recovering the fraction

Assume $F(z) = f_0 + f_1 z + \cdots + f_m z^m$ and $G(z) = g_0 + g_1 z + \cdots + g_m z^m$ are two polynomials in z. Then

$$\frac{F(z)}{G(z)} = A(z) = \sum_{k=0}^{\infty} a_k z^k$$

where the a_k's satisfy the recurrence relations:

$$\sum_{i=0}^{k} g_i a_{k-i} = f_k, 0 \leq k \leq m,$$

and for $k > m$:

$$\sum_{i=0}^{m} g_i a_{k-i} = 0.$$

Conversely, given a series $A(z)$, known up to order $2m$, we can compute its (m, m) Padé approximant defined as a rational fraction $U(z)/V(z)$ with $\deg(U) \leq m$, $\deg(V) \leq m$ and

$$A(z)V(z) - U(z) = O(z^{2m+1}).$$

The (m, m) approximant can be computed using Berlekamp's algorithm [28] in $O(m^2)$ operations or using algorithm EMGCD of [5] in $O(m(\log m)^2)$ operations. Note that from a practical point of view, Berlekamp's algorithm is faster.

7.3.3 The final algorithm and its complexity

The isogeny test can be summarized as follows:

procedure IsogenyTest(ℓ, $\mathcal{M}(t)$, $\mathcal{S}^*(\mathcal{M}(t))$)

1. compute $Z^*(t) = \mathcal{S}^*(\mathcal{M}(t))/\mathcal{M}(t)$;
2. compute $\hat{M}(Z) = \hat{m}_1 Z + \hat{m}_3 Z^3 + \cdots + \hat{m}_{2\ell+1} Z^{2\ell+1} + O(Z^{2\ell+2})$ using algorithm RecoverSeriesInZ;
3. recover the fraction $F(Z)/G(Z)$ which is a $(\ell+1, \ell+1)$ Padé approximant of $\hat{M}(Z)$; at this point, F and G have degree $\leq \ell + 1$ *a priori*;
4. if $\deg(F) = \deg(G)$ and F is Z times the square of a polynomial, then $\hat{M}$ might be the isogeny we are looking for; in this case, we compute the factor $g_\ell(X)$ of the ℓ-th division polynomial and check whether $\ell(X, Y) = O_E$ on the curve $GF(q)[X, Y]/(\mathcal{F}(X, Y), g_\ell(X))$.

The first step takes $O(\ell^\mu)$ operations, the second $O(\ell^2)$ which dominates the third step. Therefore, we see that the cost of the isogeny test (minus the final check) is $O(\ell^2)$.

Note also that in the "multiplication" strategy, one already has $\mathcal{S}^*(\mathcal{M}(t))$ at one's disposal.

7.4 Enumerating all the morphisms

7.4.1 Backtracking

It is easy to see that the cost of this approach is $O(\mathcal{L})$ times the cost of finding one morphism plus that of an isogeny test. The total cost is thus $O(\ell^{\max(\mu+3/2,3)})$.

7.4.2 Multiplication by a p-adic integer

In fact, we do not really multiply by a p-adic integer, but merely perform additions in the formal group, until we find the isogeny. The algorithm is as follows:

procedure ComputeIsogeny(ℓ, $\mathcal{E}$, $\mathcal{E}^*$)

1. compute a generator $\mathcal{U}$ of the set of morphisms between $\mathcal{E}$ and $\mathcal{E}^*$ using the algorithms of section 7.2;
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) use IsogenyTest to test whether $\mathcal{M}$ comes from isogeny; if yes, stop.

Note that we compute $(\mathcal{M}(t), \mathcal{S}^*(\mathcal{M}(t)))$ using a formal addition between the preceding computed value and $(\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t)))$ or $[2](\mathcal{U}(t), \mathcal{S}(\mathcal{U}(t)))$.

The cost of the second approach is the cost of finding one morphism, $O(\mathcal{L}^{\mu+1/2})$ multiplications, plus $O(\mathcal{L})$ times the cost of an addition in the formal group – $O(\mathcal{L}^{\mu})$ multiplications – plus $O(\mathcal{L})$ times the cost of the isogeny test of cost $O(\mathcal{L}^2)$. So, the complexity of this second approach is $O(\ell^{\max(\mu+1,3)})$.

Asymptotically, if $\mu \leq 3/2$, both methods have the same complexity $O(\ell^3)$. If $\mu > 3/2$, the second one is better and the complexity is $O(\ell^3)$.

However, from a practical point of view, the second approach is always better, since, apart from the isogeny test, we replace a substitution of series whose complexity is $O(\mathcal{L}^{\mu+1/2})$ by a formal addition whose complexity is only $O(\mathcal{L}^{\mu})$ (remember that $1 \leq \mu \leq 2$).

We illustrate this conclusion by the giving the numerical comparison of the two methods in Figure 1, for the case $K = GF(2^{10})$, for 50 curves.

7.5 Overall complexity

Proposition 7.2 *After preprocesing, the cost of Couveignes's algorithm is* $O(\max(p^2 \log p, \ell^3))$.

Proof: The first term comes from the computation of the isogenous curve by equation (16). The second from the computations described above. □

Remark. It should be remarked here that the dependance on p is not really relevant, for if $p > \ell$, then the Elkies-Atkin approach works and thus Couveignes's algorithm is not used. So the complexity is really $O(\ell^3)$.

8 Examples

According to the parametrization of elliptic curves of section 3.2, there are three cases: $p = 2$, $p = 3$ and $p > 3$, a representant of which will be $p = 5$. The aim of this section is to give three examples of use of SEA for these three cases, starting from the more generic one, $p = 5$, to the less $p = 3$ and $p = 2$.

8.1 Examples in characteristic 5

Let $K = GF(5^3) = GF(5)[T]/(T^3 + T + 1)$ and $E : Y^2 = X^3 + X + T$. Since $2 \times 3 \times 5^2 = 150 > 4\sqrt{q} \approx 44.72$, we will have to look for $c \bmod \ell$ at least for $\ell \in \{2, 3, 5\}$.

We begin with $\ell = 2$ and find that $X^3 + X + T$ has no roots and therefore $q + 1 - c$ is odd, or $c \equiv 1 \bmod 2$.

For $\ell = 3$, we take

$$\Phi_3(F, J) = F^4 + 36F^3 + 270F^2 - (J - 756)F + 729$$

and $\Phi_3(F, j(E))$ factors as

$$(F + 4T^2 + 4T + 1)(F + 4T + 3)(F^2 + (T^2 + 2T + 2)F + 3T^2 + T + 1)$$

in K. We choose $F = T+2$, which yields $j^* = 3T^2+T$. We now look for the equation of E^*. We will look for λ such that the equation of E^* is $[(T^2+T+2)\lambda^2, (4T^2+4T+3)\lambda^3]$. Computing the developments of [5] and $[5]^*$, we find that

$$[5] = 2t^5 + O(t^7)$$

$$[5]^* = (2T^2+2T+4)\lambda^2 t^5 + O(t^7).$$

Equating the coefficients of t^5, we find that

$$\lambda^2 = 3T+2.$$

We take $\lambda = 2T^2+2T$ and thus $E^* = [1, 3T^2+3T]$.

In this case, we have $5 < 4\times 3 < 5^2$ and we must compute $\mathcal{U}$ up to order 12. We first select $A = T$ and we set $\mathcal{U}_1 = t$. We find u_3 by equating $\mathcal{U}(F_a(t, At))$ and $F_a^*(\mathcal{U}(t), \mathcal{U}(At))$, which yields

$$(3T^2+3T)u_3 = 0$$

or $u_3 = 0$. Then, it is the turn of u_5 for which we have to equate $\mathcal{U}\circ[5]$ and $[5]^*\circ\mathcal{U}$ or

$$T+1+2u_5+3u_5^5+4T^2 = 0.$$

The solutions of this equation are $T^2, T^2+1, T^2+2, T^2+3, T^2+4$. We choose $u_5 = T^2$ and go on. We keep on like this and finally find

$$\mathcal{U} = t + T^2t^5 + (3T^2+2T)t^7 + 3T^2t^9 + (3T^2+4T+4)t^{11} + (T^2+T)t^{13} + O(t^{14}).$$

Now, we have to look for N, $1 \le N \le \lfloor p^{r+1}/2 \rfloor = 12$, $N \not\equiv 0 \bmod p$, such that $[N]\circ\mathcal{U}$ is the series associated with I. We first find that

$$Z = \frac{\mathcal{S}(t)}{t} = t^2 + t^6 + Tt^8 + 2t^{10} + O(t^{14}).$$

We begin with $N = 1$:

$$\mathcal{U}\circ[1] = t + T^2t^5 + (3T^2+2T)t^7 + 3T^2t^9 + (3T^2+4T+4)t^{11} + (T^2+T)t^{13} + O(t^{14})$$

and

$$Z^*(\mathcal{U}\circ[1]) = t^2 + (2T^2+1)t^6 + (4T^2+2T)t^8 + (T^2+4T+2)t^{10} + (4T^2+2T)t^{12} + O(t^{14})$$

which can be written as

$$Z + 2T^2Z^3 + (4T^2+T)Z^4 + 4TZ^5 + (3T^2+4T+1)Z^6 + O(Z^7).$$

Now, we use the Berlekamp-Massey algorithm to recover the fraction, which in this particular case gives:

$$\frac{(2T^2+5T+5)Z^3 + (8T^2+6T+2)Z^2 + (5T^2+5T+1)Z}{(3T^2+3T+2)Z^4 + (3T^2+7T+7)Z^3 + 5T^2 + (3T^2+T+2)Z + 5T + 6}.$$

This fraction has not the degree we are expecting, so it does not correspond to the isogeny we are looking for. We test the other values of N, and we finally find that, when $N = 12$, we obtain

$$Z^*(\mathcal{U}\circ[12]) = 4t^2 + (2+3T^2)t^6 + (4T^2+T)t^8 + (2T^2+T)t^{10} + (T^2+T+1)t^{12} + O(t^{14})$$

$$= 4Z + (3T^2+3)Z^3 + (4T^2+2T)Z^4 + (3T^2+T+3)Z^5 + 3TZ^6 + O(Z^7)$$

which comes from the fraction:

$$\frac{(3T^2+1)Z^3 + (2T^2+4T)Z^2 + Z}{(4T^2+T+3)Z^3 + (T^2+4)Z^2 + (2T^2+4T)Z + 1}$$

the numerator of which is

$$Z(3T^2+1)(Z+4T+2)^2$$

so the factor we are looking for is the reciprocal of $Z + 4\,T + 2$, that is $g_3(X) = X + T^2 + 2T$. It is now easy to check that it is really a factor, by computing $[3](X,Y)$ on $K[X,Y]/(\mathcal{F}(X,Y,1), g_3(X))$. We are now able to find that the eigenvalue is 2, and thus $c \equiv 0 \bmod 3$.

Let us turn our attention to the case $\ell = 5$. First, using Theorem 3.3, one has

$$c \equiv \mathrm{N}_{K/GF(5)}(2) \equiv 2 \times 2^5 \times 2^{5^2} \equiv 3 \bmod 5.$$

We deduce from this that the eigenvalue associated to g_5 is 3.

We already computed g_5 and g_{25} in Section 3.1. We use

$$g_{25}(X) = \tilde{f}_{5^2}/\tilde{f}_5 = 2X^{10} + 4X^9T + (3T^2+T+3)X^8 + (T^2+T+1)X^7 + (2T^2+T+3)X^6 + (2T+3)X^5$$
$$+(2T^2+3)X^4 + (4T^2+3T+4)X^3 + (3T^2+4T)X^2 + (4T+1)X + T + 3.$$

We easily compute that the eigenvalue is 3, and therefore $c \equiv 3 \bmod 5^2$.

Finally, one finds that $c \equiv 3 \bmod 150$, which yields $c = 3$ and $\#E = q + 1 - c = 123$.

8.2 Example in characteristic 3

Let us consider $K = GF(3^4) = GF(3)[T]/(T^4 + 2T + 2)$ and $E : Y^2 = X^3 + X^2 + T.$ and $\ell = 5$. We find that the isogenous curve is $E^* = [1, 2T^3 + 2T]$. We compute along the same ways that:

$$\mathcal{U}(t) = t + Tt^3 + 2t^5T + 2T^2t^7 + (2T^3+T^2+T)t^9 + (2T^3+2T)t^{11} + (2T^3+T^2+2T+2)t^{13} + (T^2+2T+2)t^{15}$$
$$+(T^2+2T+2)t^{17} + (2+T^3+T^2+2T)t^{19} + (2T^3+T^2+T+1)t^{21} + O(t^{23}).$$

We find that for $N = 2$, one gets a fraction of suitable degree, the numerator of which is

$$\left(T^3+T+2\right)\left(Z^2 + \left(2\,T^3+T^2+T+2\right)Z + 2\,T^2+1\right)^2$$

which yields $g_5(X) = X^2 + (T+2)X + 2T^3 + 2T + 1$.

9 Implementation in characteristic 2

We give an example of our implementation of Couveignes's idea for $q = p^n = 2^n$. Let $E : Y^2 + XY = X^3 + a_6$ be an elliptic curve.

9.1 Simplifying formulas

After the classical change of variables $t=-x/y,\ s=-1/y$ to set $O_E=(0,0)$, the equation of $\mathcal{E}$ becomes

$$s=t^3+ts+a_6s^3. \tag{27}$$

We obtain, in the special case $t(\tau)=\tau$, the series $\mathcal{S}(\tau)=\sum_{i=1}^{\infty}\mathcal{S}_i\tau^i$ of the formal point $(\tau,\mathcal{S}(\tau))$ as

$$\mathcal{S}_{2i+1}=\begin{cases}1 & \text{if } i=1,2,3,5,\\ 1+a_6 & \text{if } i=4,\\ \mathcal{S}_{2i}+a_6\left(\mathcal{S}_{2i-5}+\mathcal{S}_{i-1}^2+\sum_{j=4}^{i-2}\mathcal{S}_j^2\mathcal{S}_{2i-2j+1}\right) & \text{otherwise;}\end{cases} \tag{28}$$

and

$$\mathcal{S}_{2i}=\begin{cases}1 & \text{if } i=1,2,3,4,5,\\ \mathcal{S}_{2i-1}+a_6\left(\mathcal{S}_{2i-6}+\sum_{j=4}^{i-2}\mathcal{S}_j^2\mathcal{S}_{2i-2j}\right) & \text{otherwise.}\end{cases} \tag{29}$$

Using standard tools [39], we also find that $\mathcal{S}(t)$ satisfies the diffential equation:

$$\left(-54\,t^5-4\,t^3+14\,t^2-18\,t+8\right)y+\left(-48\,t+54\,t^2-28\,t^3+6\,t^4+54\,t^6+16\right)y'$$
$$+\left(-27\,t^8+28\,t^2-36\,t^3+20\,t^4-4\,t^5+54\,t^7-8\,t\right)y''=0$$

over $\mathbb{Z}[a_6]$, from which we find that the s_i's satisfy the recurrence relation

$$\left(-27\,n^2+27\,n\right)s_n+\left(108\,n+54\,n^2\right)s_{n+1}+\left(-10-14\,n-4\,n^2\right)s_{n+3}+\left(142+112\,n+20\,n^2\right)s_{n+4}$$
$$+\left(-468-270\,n-36\,n^2\right)s_{n+5}+\left(560+260\,n+28\,n^2\right)s_{n+6}+\left(-88\,n-224-8\,n^2\right)s_{n+7}=0$$

together with the initial values:

$$s_0=s_1=s_2=0, s_3=s_4=s_5=s_6=1.$$

Using these formulas, we can compute the s_n over $\mathbb{Z}[a_6]$ and then reduce them modulo 2.

We can rewrite the formulae of section 2.3.3 in order to decrease their computational cost. If $t_1\neq t_2$, $(t_1\oplus t_2(\tau),\mathcal{S}(t_1\oplus t_2(\tau)))=(t_1(\tau),s_1(\tau))\oplus(t_2(\tau),s_2(\tau))$ is computed as:

$$\begin{cases}\lambda(\tau)=\dfrac{s_1(\tau)+s_2(\tau)}{t_1(\tau)+t_2(\tau)},\ \nu(\tau)=s_1(\tau)+\lambda(\tau)t_1(\tau),\\[2ex] t_1\oplus t_2(\tau)=\dfrac{t_1(\tau)+t_2(\tau)+\lambda(\tau)+a_6\lambda^2(\tau)(s_1(\tau)+s_2(\tau)+\nu(\tau))}{1+t_1(\tau)+t_2(\tau)+\lambda(\tau)+a_6\lambda^2(\tau)\left(s_1(\tau)+s_2(\tau)+\nu(\tau)+\lambda(\tau)\right)},\\[2ex] \mathcal{S}(t_1(\tau)\oplus t_2(\tau))=\nu(\tau)+(\lambda(\tau)+\nu(\tau))(t_1\oplus t_2(\tau)).\end{cases}$$

For computing $([2]t(\tau),\mathcal{S}([2]t(\tau)))=[2](t(\tau),s(\tau))$, we use (13):

$$\begin{cases}\delta(\tau)=t^3(\tau)+(1+\tilde{a}_6s(\tau))\,t^2(\tau)+\left(\tilde{a}_6s^2(\tau)+s(\tau)\right)t(\tau)+\tilde{a}_6s^2(\tau)+s(\tau),\\ \kappa(t)=\dfrac{\left(t^2(\tau)+\tilde{a}_6s^2(\tau)\right)t(\tau)}{\delta(\tau)},\\ [2]t(\tau)=\kappa^2(\tau),\\ \mathcal{S}([2]t(\tau))=\left(\dfrac{\delta(\tau)}{s(\tau)t(\tau)^2}\right)^2.\end{cases} \tag{30}$$

This computation costs 5 multiplications of series and 2 divisions.

9.2 Example

Let $K = GF(2^8) = GF(2)[T]/(T^8+T^4+T^3+T+1)$. Every element of K can be written as a polynomial in T. In order to pack the different results, we will write such a polynomial $a(T)=\sum_{i=0}^{n-1} a_i T^i$ as $\overline{a(2)}$. For instance, the polynomial T^2+T will be abbreviated as $\overline{6}$.

Let us compute an isogeny of degree $\ell = 5$ between $E = [\overline{7}]$ and $E^* = [\overline{8}]$. We first find that $A = \overline{2}$ is valid. Then equation (18) becomes

$$0 \;=\; \left(\overline{6}\,u_2+\overline{6}\,u_3\right)t^3+\left(\overline{4}\,{u_2}^2+\overline{4}\,u_2\right)t^4+O(t^5)$$

and equation (20) becomes

$$0 \;=\; \left(\sqrt{u_2}^2+\sqrt{u_2}\right)t^2+\left(\sqrt{u_3}^2+\sqrt{u_3}\right)t^3+\left(\sqrt{u_4}^2+\sqrt{u_4}+\sqrt{\overline{15}}\right)t^4+O(t^5).$$

Consequently,

$$\begin{array}{rcll}
\sqrt{u_2}^2+\sqrt{u_2}=0 & \Longrightarrow & u_2\in\{\overline{0},\overline{1}\}, & \text{we choose } u_2=0,\\
\overline{6}\,u_2+\overline{6}\,u_3=0 & \Longrightarrow & u_3\in\{\overline{0}\}, & \text{we have } u_3=0,\\
\sqrt{u_4}^2+\sqrt{u_4}+\sqrt{\overline{15}}=0 & \Longrightarrow & u_4\in\{\overline{56},\overline{57}\}, & \text{we choose } u_4=\overline{56},
\end{array}$$

and once all computations are done, we find

$$\begin{array}{rcl}
\mathcal{U}(t) & = & t+\overline{56}t^4+\overline{56}t^5+\overline{15}t^7+\overline{16}t^8+\overline{31}t^9+\overline{219}t^{10}+\\
& & \overline{124}t^{11}+\overline{5}t^{12}+\overline{44}t^{13}+\overline{91}t^{14}+\overline{47}t^{15}+\overline{210}t^{16}+\\
& & \overline{201}t^{17}+\overline{231}t^{18}+\overline{198}t^{19}+\overline{188}t^{20}+\overline{118}t^{21}+O(t^{22}).
\end{array}$$

Let us use first the backtrack method, the morphism $\mathcal{M}_1$ obtained from $\mathcal{M}$ by setting $u_{16}=\overline{211}$ is

$$\begin{array}{rcl}
\mathcal{U}_1(t) & = & t+\overline{56}t^4+\overline{56}t^5+\overline{15}t^7+\overline{16}t^8+\overline{31}t^9+\overline{219}t^{10}+\overline{124}t^{11}+\\
& & \overline{5}t^{12}+\overline{44}t^{13}+\overline{91}t^{14}+\overline{47}t^{15}+\overline{211}t^{16}+\overline{200}t^{17}+\overline{231}t^{18}+\\
& & \overline{198}t^{19}+\overline{132}t^{20}+\overline{78}t^{21}+O(t^{22}).
\end{array}$$

Then the morphism $\mathcal{M}_2$ obtained from $\mathcal{M}_1$ by setting $u_8=\overline{17}$ is

$$\begin{array}{rcl}
\mathcal{U}_2(t) & = & t+\overline{56}t^4+\overline{56}t^5+\overline{15}t^7+\overline{17}t^8+\overline{30}t^9+\overline{219}t^{10}+\overline{124}t^{11}+\\
& & \overline{61}t^{12}+\overline{20}t^{13}+\overline{83}t^{14}+\overline{32}t^{15}+\overline{202}t^{16}+\overline{214}t^{17}+\overline{52}t^{18}+\\
& & \overline{186}t^{19}+\overline{18}t^{20}+\overline{82}t^{21}+O(t^{22}).
\end{array}$$

Afterwards the morphism $\mathcal{M}_3$ obtained from $\mathcal{M}_2$ by setting $u_{16}=\overline{203}$ is

$$\begin{array}{rcl}
\mathcal{U}_3(t) & = & t+\overline{56}t^4+\overline{56}t^5+\overline{15}t^7+\overline{17}t^8+\overline{30}t^9+\overline{219}t^{10}+\overline{124}t^{11}+\\
& & \overline{61}t^{12}+\overline{20}t^{13}+\overline{83}t^{14}+\overline{32}t^{15}+\overline{203}t^{16}+\overline{215}t^{17}+\overline{52}t^{18}+\\
& & \overline{186}t^{19}+\overline{42}t^{20}+\overline{106}t^{21}+O(t^{22}).
\end{array}$$

Continuing in the same vein, we try

$$\begin{array}{rcl}
\mathcal{U}_4(t) & = & t+\overline{57}t^4+\overline{57}t^5+\overline{15}t^7+\overline{40}t^8+\overline{39}t^9+\overline{211}t^{10}+\overline{115}t^{11}+\\
& & \overline{29}t^{12}+\overline{59}t^{13}+\overline{136}t^{14}+\overline{91}t^{15}+\overline{132}t^{16}+\overline{21}t^{17}+\overline{196}t^{18}+\\
& & \overline{2}t^{19}+\overline{188}t^{20}+\overline{109}t^{21}+O(t^{22}),\\
\mathcal{U}_5(t) & = & t+\overline{57}t^4+\overline{57}t^5+\overline{15}t^7+\overline{40}t^8+\overline{39}t^9+\overline{211}t^{10}+\overline{115}t^{11}+\\
& & \overline{29}t^{12}+\overline{59}t^{13}+\overline{136}t^{14}+\overline{91}t^{15}+\overline{133}t^{16}+\overline{20}t^{17}+\overline{196}t^{18}+\\
& & \overline{2}t^{19}+\overline{133}t^{20}+\overline{84}t^{21}+O(t^{22}),
\end{array}$$

and finally we find that

$$\begin{aligned}\mathcal{U}_6(t) &= t+\overline{57}t^4+\overline{57}t^5+\overline{15}t^7+\overline{41}t^8+\overline{38}t^9+\overline{211}t^{10}+\overline{115}t^{11}+\\ &\quad \overline{36}t^{12}+\overline{2}t^{13}+\overline{128}t^{14}+\overline{84}t^{15}+\overline{164}t^{16}+\overline{50}t^{17}+\overline{31}t^{18}+\\ &\quad \overline{113}t^{19}+\overline{2}t^{20}+\overline{94}t^{21}+O(t^{22})\end{aligned}$$

is the isogeny.

In the multiplication method, additions in the formal group give

$$\begin{aligned}[2](\mathcal{U}(t)) &= t^2+\overline{63}t^8+\overline{63}t^{10}+\overline{29}t^{14}+\overline{184}t^{16}+\overline{165}t^{18}+\overline{227}t^{20}+O(t^{22})\\ [3](\mathcal{U}(t)) &= t+t^2+t^3+\overline{56}t^4+\overline{56}t^5+\overline{56}t^6+\overline{55}t^7+\overline{39}t^8+\overline{39}t^9+\\ &\quad \overline{244}t^{10}+\overline{84}t^{11}+\overline{154}t^{12}+\overline{28}t^{13}+\overline{79}t^{14}+\overline{52}t^{15}+\overline{247}t^{16}+\\ &\quad \overline{51}t^{17}+\overline{44}t^{18}+\overline{66}t^{19}+\overline{102}t^{20}+\overline{84}t^{21}+O(t^{22})\end{aligned}$$

We obtain finally with the Berlekamp-Massey algorithm from $[3](\mathcal{U}(t))$ or from $\mathcal{U}_6(t)$,

$$\mathcal{I}(X(t))=\frac{X^5(t)+\overline{15}X^3(t)+\overline{140}X(t)}{(X^2(t)+\overline{57}X(t)+\overline{74})^2}.$$

Let us notice here that $U_6(t)$ is the opposite of $[3](\mathcal{U}(t))$, that is to say that $[3](\mathcal{U}(t))=U_6(t/(1+t))$.

9.3 Implementation and results

9.3.1 General remarks

We note that almost all the ideas (and tricks) of Atkin are valid for all characteristics. The first implementation of part of the above ideas is described in [32], which contains many interesting details. Moreover, recent algorithmic improvements developped in the case of p large are still valid, notably the work of Couveignes and Morain [12, 11], which is very powerful in the small characteristic case, since computing a factor of f_{ℓ^n} requires computing an isogeny of degree ℓ and not ℓ^n; the work of Müller [38] with the improvement of Dewaghe [14].

9.3.2 Basic arithmetic

Our implementation is based on the library `GFQ` written by F. Chabaud [7] (on top of `BigNum` – cf. [20]), and improved by the authors. It represents $GF(2^n)$ as the residue class ring $GF(2)[T]/(T^n+f(T))$ where $f(T)$ is a polynomial of degree smaller than n such that $T^n+f(T)$ is irreducible over $GF(2)$. In practice – in the range $1\le n\le 700$ – we were always able to find a suitable f of degree less than 15. More details can be found in [27], including a description of the polynomial arithmetic used. In particular, Karatsuba's algorithm is used for polynomial multiplication, as well as for series multiplications.

9.3.3 Benchmarks

In [19], the authors give running times for curves defined over $GF(2^{65})$, $GF(2^{89})$ and $GF(2^{105})$. We used these fields as benchmarks for our implementation. We took the 50 curves defined as $y^2+xy=x^3+a_6$ where $a_6\in GF(2)[T]$ and $2\le\overline{a_6(2)}\le 51$ (none of such coefficient a_6 belongs to a smaller extension of $GF(2^{65})$, $GF(2^{89})$ and $GF(2^{105})$).

We give: ℓ_{max}, the maximal prime used; the number of U primes (a U prime ℓ is one for which we have one value for $c \bmod \ell$), the number of L primes (the other primes); M, the number of combinations; the cumulated time for X^q, X^{q^r}, Schoof's algorithm; computing g_ℓ and k when ℓ is Elkies; the time for the match and sort program; the total time. For each category, we give the minimal, maximal and average values.

As explained in [27], we can tune our program using parameters describing several strategies. There are four bounds $\mathcal{S}$, $\mathcal{E}$, $\mathcal{A}$, and $\mathcal{C}$ which describe the use of Schoof's original algorithm, computing isogenies for Elkies primes, finding the splitting of Atkin primes, and using powers of small primes. We refer to the article cited for more details. Playing with the different parameters finally yields the best results for our three fields in Table 1. In each case, one has $\mathcal{A} = \infty$.

	$GF(2^{65})$ $\mathcal{E}=2, \mathcal{C}=2, \mathcal{S}=0$			$GF(2^{89})$ $\mathcal{E}=3, \mathcal{C}=4, \mathcal{S}=0$			$GF(2^{105})$ $\mathcal{E}=3, \mathcal{C}=4, \mathcal{S}=24$		
	min	max	avg	min	max	avg	min	max	avg
$\ell_{\max}$	29	29	29	37	41	39	43	43	43
$\#U$	1	4	2	1	6	3	4	6	5
$\#L$	6	9	7	6	12	9	8	10	9
M	10^3	$3.7\,10^5$	$5.8\,10^4$	$7.7\,10^2$	$2.8\,10^7$	$2.4\,10^6$	$1.5\,10^5$	$7.1\,10^8$	$6.6\,10^7$
X^q	3.8	4.0	3.9	10.2	14.9	12.5	22.4	24.8	23.3
X^{q^r}	1.3	3.2	2.2	3.8	12.0	8.1	11.5	18.3	14.7
Schoof	0.0	0.0	0.0	0.0	0.0	0.0	0.0	30.0	12.9
g	0.0	1.1	0.4	0.0	2.5	1.0	0.0	2.4	1.0
k	0.1	0.2	0.1	0.3	0.6	0.5	0.3	0.8	0.6
M − S	0.1	1.7	1.1	0.2	5.9	2.5	0.5	18.8	5.7
Total	6.1	8.8	7.7	17.9	32.2	24.6	43.0	73.9	58.1

Table 1: Best parameters for $GF(2^n)$

For the case $K = GF(2^{300})$, we have made precise statistics on every part of the algorithm. The results are given in the tables and graphs given at the end of the article. In Table 2, one finds for each Elkies prime power ℓ^d the number of values of J^* to try, `Num` refers to the computation of the numerator of the isogeny for ℓ^d, `Prec` to the precomputations, $\oplus$ designates the time of a formal addition, `BM` the time for the Berlekamp-Massey algorithm and N is the 2-adic integer such that $[N] \circ \mathcal{U}$ comes from an isogeny (we take all coefficients $u_{2^i} = P_i(T)$ of $\mathcal{U}$ such that $P_i(0) = 0$).

9.3.4 Records

In [32, 31], the authors gave timings for larger fields $GF(2^{155})$ and $GF(2^{195})$. For these fields and for larger fields (the last one being the current record, as of June 1995), our implementation gave the following timings, for the curve:

$$E_X : y^2 + xy = x^3 + T^{16} + T^{14} + T^{13} + T^9 + T^8 + T^7 + T^6 + T^5 + T^4 + T^3$$

(the coefficient was chosen as the binary expression of 91128 – our zip code – converted to a polynomial if $GF(2^n)$). Table 2 gives for some values of n a polynomial $f(T)$ such that $T^n + f(T)$ is a defining polynomial of $GF(2^n)$ and the value of c such that $\#\mathcal{E}_X(GF(2^n)) = 2^n + 1 - c$.

Table 3 corresponds to the first version of our implementation, which used the backtrack approach. The cases $n = 300$ and $n = 400$ were done with a poor implementation of the treatment of Atkin primes; moreover no power of small primes were used. For the cases $n = 500$ and 601, fast splitting techniques à la Atkin were used, as well as powers of small primes and Karatsuba's algorithm for series (and polynomial) multiplication. But for all of these, we did not use equations (30), but rather the corresponding series.

n	$f(T)$	c
155	$T^7+T^5+T^4+1$	80860670297104421704641
196	T^3+1	16895903179083099567397034739З
300	T^5+1	$-1057128182990122062466877450474871210809126З$
400	$T^5+T^3+T^2+1$	83131171959337393875969292317817192062621127877417\ 9820465793
500	$T^8+T^6+T^5+T^2+T+1$	$-$10225253794172200535372156483716747043308861809 12\ 8461542342453382593652697 5
601	$T^7+T^4+T^3+T^2+T+1$	3777574276317218065463769817992276297989717292080 0\ 67701458146624068364548898667013349009665
701	$T^9+T^8+T^7+T^4+T^2+1$	$-$63599550342089483190003112163094789173215798033 29\ 4651795982701854210500439646514818766445288922635 8\ 9295359
1009	$T^{11}+T^4+T^2+1$	5500790584993461414462440950171237941919763462052 4\ 5345676322604836553775970582138769762823202296503 4\ 095450594133404979993418055065277722637699785638630 5

Table 2: Values of c such that $\#E_X = q+1-c$.

Table 4 refers to the implementation that uses all features described in the present article. The comparison for the case $GF(2^{300})$ is striking.

All these records have been done using a network of DecAlpha workstations, using an obvious distributed implementation of the algorithm.

A comparison with the prime field case is given in [27]. It seems that the program for $GF(2^n)$ is slower than the program for large prime characteristic around $n = 150$.

10 Conclusion

There are basically two approaches for computing isogenies between elliptic curves over a finite field. The Atkin-Elkies method works well when the characteristic is large and Couveignes's method for the small characteristic. It remains to find the break-even point between the two methods. This and many more will be done elsewhere.

In the particular case of the characteristic 2, a new method is being developped by the first author [26], that could be faster than Couveignes's.

Acknowledgments. First of all, the authors want to express their gratitude to J.-M. Couveignes, without whom this work could not have been possible. Many thanks to J.-M. Steyaert for his careful reading and for pointing out to us the use of GFUN and the theory lying behind.

References

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

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

	$GF(2^{300})$	$GF(2^{400})$	$GF(2^{500})$	$GF(2^{601})$
ℓ_{max}	109	173	179	241
$\#U$	20	26	27	29
$\#L$	9	13	11	23
M	$1.2\,10^{10}$	$2.5\,10^{9}$	$1.3\,10^{7}$	$2.1\,10^{10}$
X^q	15886	92643	29137	109708
X^{q^r}	47562	94965	6106	52885
Schoof	12194	186607	65799	240091
g	672994	1119077	518697	3139250
k	40655	774895	492213	1392113
M − S	7183	27088	3609	1728
Total	796474	2511000	1112093	4935776

Table 3: Records for the first implementation

	$GF(2^{155})$	$GF(2^{196})$	$GF(2^{300})$	$GF(2^{701})$	$GF(2^{1009})$
$\ell_{\max}$	59	73	109	337	577
$\#U$	6	11	18	40	57
$\#L$	11	10	11	28	46
M	$2\,10^{7}$	10^{8}	$3\,10^{8}$	$1.2 10^{10}$	$3.9\,10^{9}$
X^q	121	440	3221	505004	2613536
X^{q^r}	42	127	356	282637	498462
Schoof	0	69	0	1172674	413936
g	24	580	22974	4842770	13457961
k	19	141	3613	1094254	4000569
M − S	10	23	56	2098	3688
Total	217	1381	30221	7897343	21018853

Table 4: Records for the second implementation

[3] Atkin, A. O. L., and Morain, F. Elliptic curves and primality proving. *Math. Comp. 61*, 203 (July 1993), 29–68.

[4] Bosma, W. Primality testing using elliptic curves. Tech. Rep. 85-12, Math. Instituut, Universiteit van Amsterdam, 1985.

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

[6] Brent, R. P., and Kung, H. T. Fast algorithms for manipulating formal power series. *J. ACM 25* (1978), 581–595.

[7] Chabaud, F. Sécurité des crypto-systèmes de McEliece. Mémoire de DEA, École polytechnique, 1993.

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

[9] Comtet, L. Calcul pratique des coefficients de Taylor d'une fonction algébrique. *Enseignement Math. 10* (1964), 267–270.

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

[11] Couveignes, J.-M., Dewaghe, L., and Morain, F. Isogeny cycles and Schoof's algorithm. Draft, Mar. 1995.

[12] Couveignes, J.-M., and Morain, F. Schoof's algorithm and isogeny cycles. In *ANTS-I* (1994), L. Adleman and M.-D. Huang, Eds., vol. 877 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 43–58. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[13] Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg 14* (1941), 197–272.

[14] Dewaghe, L. Remarques sur l'algorithme SEA. In preparation, Dec. 1994.

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

[16] Fricke, R. *Die elliptischen Funktionen und ihre Anwendungen.* Teubner, Leipzig, 1992.

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

[18] Goldwasser, S., and Kilian, J. Almost all primes can be quickly certified. In *Proc. 18th STOC* (1986), ACM, pp. 316–329. May 28–30, Berkeley.

[19] Harper, G., Menezes, A., and Vanstone, S. Public-key cryptosystems with very small key length. In *Advances in Cryptoloy – EUROCRYPT '92* (1993), R. A. Rueppel, Ed., vol. 658 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 163–173. Workshop on the Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992, Proceedings.

[20] Hervé, J.-C., Serpette, B., and Vuillemin, J. BigNum: A portable and efficient package for arbitrary-precision arithmetic. Tech. Rep. 2, Digital Paris Research Laboratory, May 1989.

[21] Husemöller, D. *Elliptic curves*, vol. 111 of *Graduate Texts in Mathematics*. Springer, 1987.

[22] Knuth, D. E. *The Art of Computer Programming: Seminumerical Algorithms*, 2nd ed. Addison-Wesley, 1981.

[23] Koblitz, N. Elliptic curve cryptosystems. *Math. Comp. 48*, 177 (Jan. 1987), 203–209.

[24] Lehmann, F., Maurer, M., Müller, V., and Shoup, V. Counting the number of points on elliptic curves over finite fields of characteristic greater than three. In *ANTS-I* (1994), L. Adleman and M.-D. Huang, Eds., vol. 877 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 60–70. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[25] Lenstra, Jr., H. W. Factoring integers with elliptic curves. *Annals of Math. 126* (1987), 649–673.

[26] Lercier, R. Computing isogenies in characteristic 2. Draft, Apr. 1995.

[27] 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., no. 921 in Lecture Notes in Comput. Sci., pp. 79–94. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

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

[29] McEliece, R. *Finite fields for computer scientists and engineers.* Kluwer international series in engineering and computer science. Kluwer Academic Publishers, 1988.

[30] McKee, J. Computing division polynomials. *Math. Comp. 63*, 208 (Oct. 1994), 767–771.

[31] Menezes, A. J. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1993.

[32] Menezes, A. J., Vanstone, S. A., and Zuccherato, R. J. Counting points on elliptic curves over F_{2^m}. *Math. Comp. 60*, 201 (Jan. 1993), 407–420.

[33] Miller, V. Use of elliptic curves in cryptography. In *Advances in Cryptology* (1987), A. M. Odlyzko, Ed., vol. 263 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 417–426. Proceedings Crypto '86, Santa Barbara (USA), August11–15, 1986.

[34] Montgomery, P. L. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp. 48*, 177 (Jan. 1987), 243–264.

[35] Morain, F. Implantation de l'algorithme de Schoof-Elkies-Atkin. Preprint, January, 1994.

[36] Morain, F. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. To appear in the Actes des Journées Arithmétiques 1993, Feb. 1995.

[37] Morain, F. On Hasse invariants and supersingular polynomials. Draft, June 1995.

[38] Müller, V. Looking for the eigenvalue in Schoof's algorithm. In preparation, Oct. 1994.

[39] Salvy, B., and Zimmermann, P. Gfun: a maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software 20*, 2 (1994), 163–177.

[40] Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp. 44* (1985), 483–494.

[41] Schoof, R. Counting points on elliptic curves over finite fields. To appear in Proc. Journées Arithmétiques 93, Jan. 1995.

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

[43] Waterhouse, E. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. 2* (1969), 521–560.

ℓ	d	T	X^q	Atkin	Elkies	Tot
2	1	E	-	-	-	0.0
	2	E	-	-	-	0.0
	3	E	-	-	0.4	0.4
	4	E	-	-	1.3	1.3
	5	E	-	-	5.1	5.1
	6	E	-	-	18.4	18.4
	7	E	-	-	72.6	72.6
	8	E	-	-	170.4	170.4
3	1	1	0.1	-	0.5	0.6
	2	-	-	-	-	0.0
5	1	1	0.3	-	1.8	2.1
	2	-	-	-	-	0.0
7	1	1	0.2	-	3.1	3.3
	2	-	-	-	-	0.0
11	1	E	3.8	-	8.3	12.1
	2	E	-	-	220.1	220.1
13	1	A	3.4	0.0	-	3.4
17	1	A	8.2	0.9	-	9.1
19	1	E	9.6	-	63.2	72.8
23	1	A	14.2	2.1	-	16.3
29	1	A	26.3	4.3	-	30.6
31	1	E	26.9	-	150.2	177.1
37	1	E	36.5	-	479.8	516.3
41	1	E	51.5	-	388.1	439.6
43	1	A	50.7	16.1	-	66.8
47	1	E	60.7	-	566.3	627.0
53	1	A	57.6	12.3	-	69.9
59	1	E	61.2	-	737.2	798.4
61	1	E	65.9	-	212.5	278.4
67	1	1	87.4	-	1069.8	1157.2
71	1	A	92.6	31.1	-	123.7
73	1	A	105.0	0.0	-	105.0
79	1	E	120.2	-	1849.8	1970.0
83	1	A	128.7	37.8	-	166.5
89	1	A	138.8	48.5	-	187.3
97	1	E	159.7	-	1642.6	1802.3
101	1	E	159.1	-	3100.1	3259.2
103	1	E	167.0	-	1045.6	1212.6
107	1	E	174.2	-	4733.4	4907.6
109	1	A	174.7	62.5	-	237.2
Tot			1984.5	215.6	16540.6	18740.7

Table 5: Data for $GF(2^{300})$.

ℓ	d	Y^q	kM	k	o
2	3	0.4	0.0	1	-
	4	1.3	0.0	1	-
	5	5.0	0.0	1	-
	6	18.4	0.0	1	-
	7	72.6	0.0	1	-
	8	149.7	20.7	129	-
3	1	0.1	0.0	2	1
5	1	0.5	0.0	1	1
7	1	0.9	0.0	6	1
11	1	2.3	0.0	3	5
11	2	136.9	72.4	80	-
19	1	7.0	0.2	16	9
31	1	17.6	1.1	4	5
37	1	25.1	7.7	24	18
41	1	30.4	13.5	17	20
47	1	39.9	1.2	44	23
59	1	63.4	34.2	39	29
61	1	72.5	27.2	46	15
67	1	80.7	60.0	27	11
79	1	118.0	38.3	13	39
97	1	176.7	56.9	13	48
101	1	184.5	218.9	42	50
103	1	118.8	71.8	81	17
107	1	123.9	174.1	48	53
Tot		1446.6	798.2	-	-

Table 6: Data for $GF(2^{300})$ (cont'd).

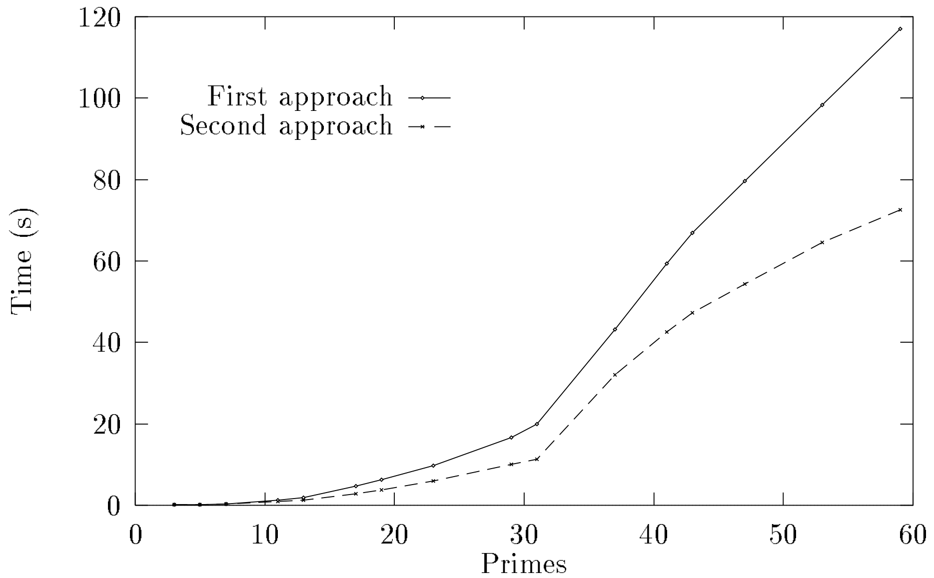
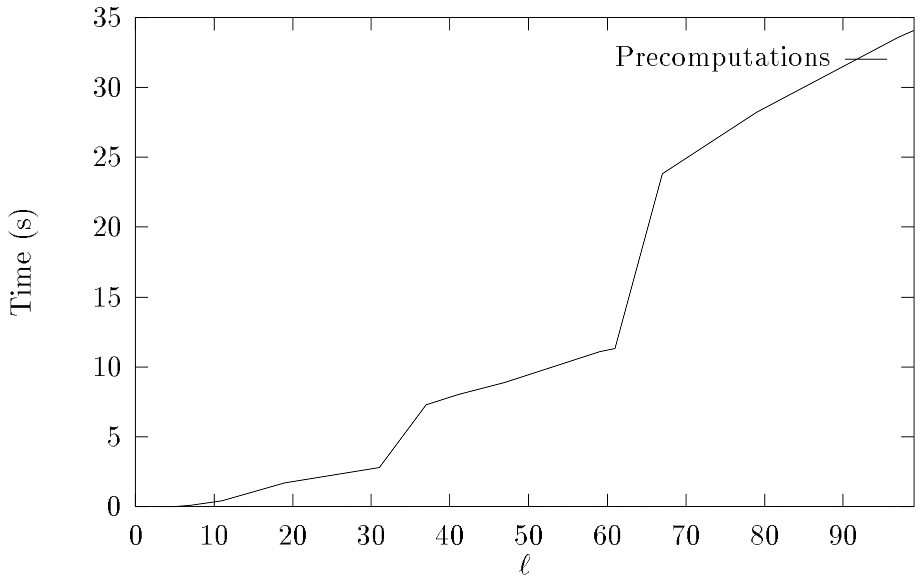
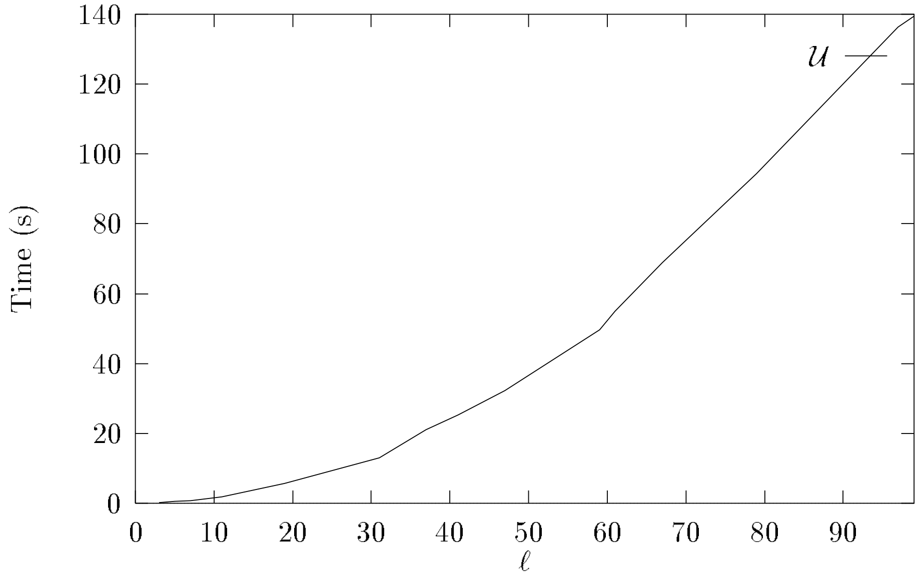


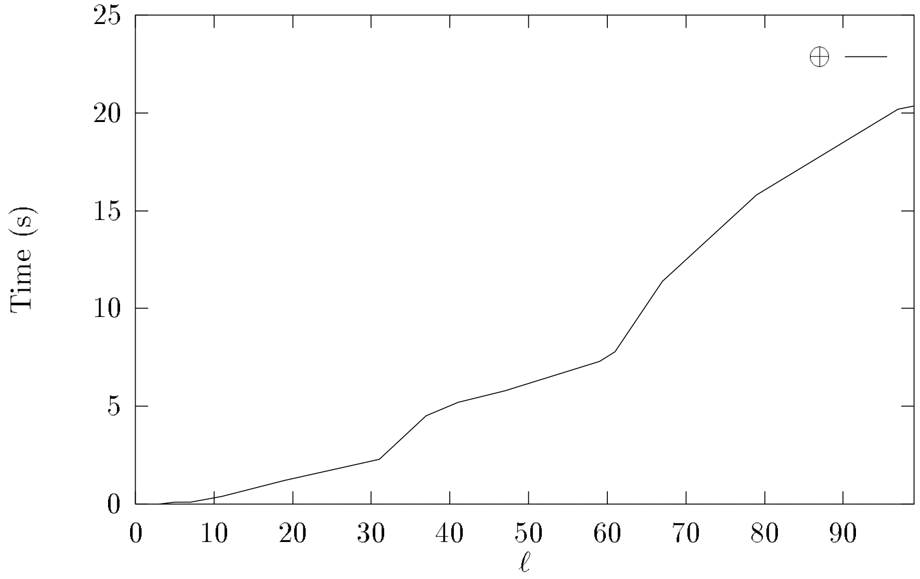
Figure 1: Average practical timings for both approaches (50 curves).

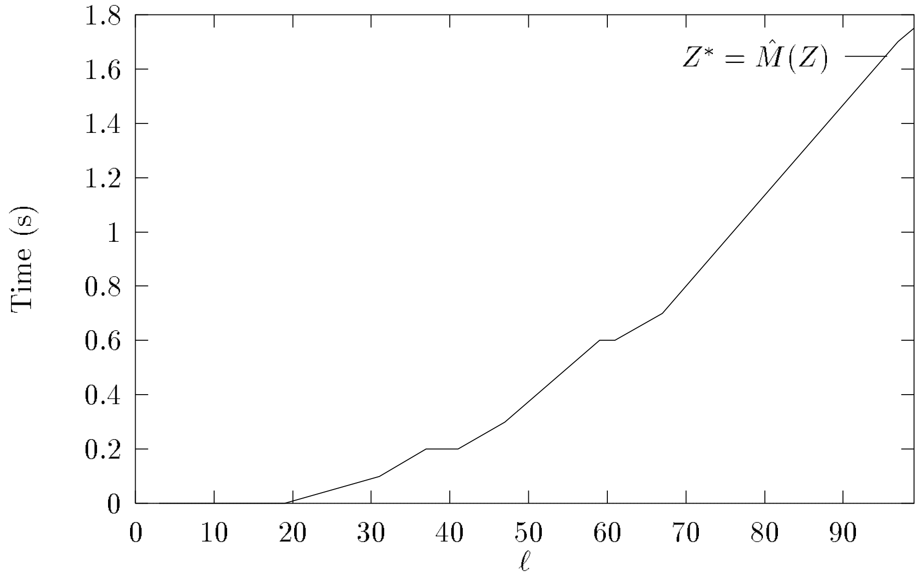
ℓ	d	J^*	$\#J^*$	Num	Prec	$\mathcal{U}$	$Z(t)^i$	$\oplus$	$Z^* = \hat{M}(Z)$	BM	N
2	3	-	-	-	-	-	-	-	-	-	-
	4	-	-	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	-	-
	6	-	-	-	-	-	-	-	-	-	-
	7	-	-	-	-	-	-	-	-	-	-
	8	-	-	-	-	-	-	-	-	-	-
3	1	0.0	1	-	0.0	0.2	0.0	0.0	0.0	0.0	3
5	1	0.0	1	-	0.0	0.5	0.0	0.1	0.0	0.0	7
7	1	0.0	1	-	0.1	0.8	0.0	0.1	0.0	0.0	7
11	1	0.8	2	-	0.4	1.9	0.1	0.4	0.0	0.0	7
	2	0.8	2	0.2	0.5	2.1	0.1	0.4	0.0	0.0	7
19	1	0.4	3	-	5.2	5.6	0.6	1.2	0.0	0.1	47
31	1	0.0	1	-	2.8	13.1	2.3	2.3	0.1	0.2	63
37	1	0.7	3	-	7.3	21.0	3.7	4.5	0.2	0.3	127
41	1	0.0	1	-	8.0	25.2	5.0	5.2	0.2	0.4	81
47	1	0.0	1	-	8.9	32.3	7.5	5.8	0.3	0.5	111
59	1	0.0	1	-	11.1	49.6	13.6	7.3	0.6	0.7	103
61	1	0.3	1	-	11.3	55.0	14.7	7.8	0.6	0.8	3
67	1	1.2	3	-	47.6	68.9	18.5	11.4	0.7	0.8	93
79	1	0.7	3	-	28.2	94.4	29.8	15.8	1.1	1.2	133
97	1	1.8	1	-	33.6	136.3	52.6	20.2	1.7	1.7	79
101	1	0.2	1	-	34.6	142.5	58.6	20.5	1.8	1.8	161
103	1	0.8	1	-	35.1	147.4	62.0	20.7	1.8	1.9	37
107	1	2.3	5	-	144.4	159.1	68.3	21.6	2.0	2.0	251
Tot		10.0	-	0.2	379.1	955.9	68.3	-	-	-	-

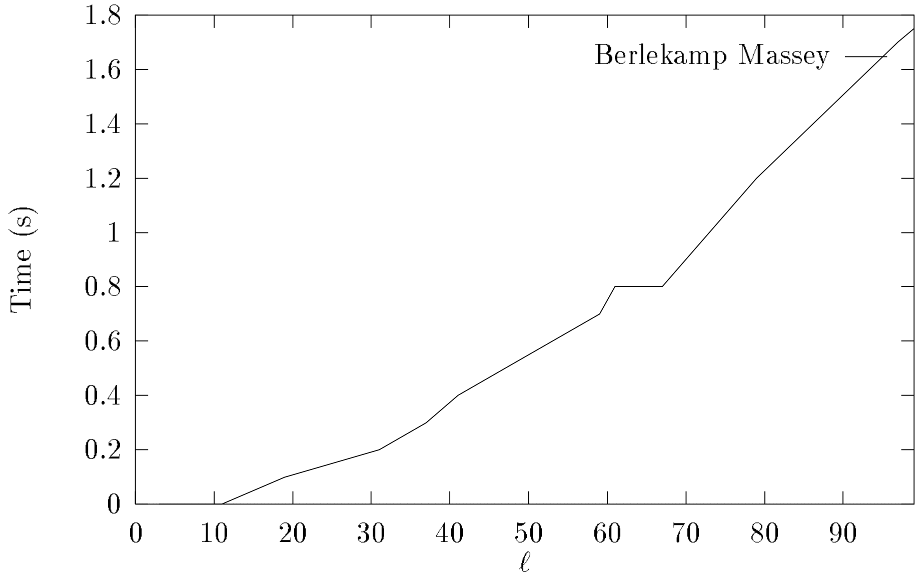
Figure 2: Data for $GF(2^{300})$ (cont'd).




Time (s)
140
120
100
80
60
40
20
0
0 10 20 30 40 50 60 70 80 90
ℓ
$\mathcal{U}$


Time (s)
25
20
15
10
5
0
0 10 20 30 40 50 60 70 80 90
ℓ
$\oplus$


$Z^* = \hat{M}(Z)$
Time (s)
ℓ
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
0
10
20
30
40
50
60
70
80
90


Berlekamp Massey
Time (s)
ℓ
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
0
10
20
30
40
50
60
70
80
90