ÉCOLE POLYTECHNIQUE

Isogeny cycles and the Schoof-Elkies-Atkin algorithm

J.-M. Couveignes
L. Dewaghe
F. Morain

LIX/RR/96/03

August 30, 1996

LABORATOIRE D'INFORMATIQUE
Unité CNRS n°1439
École polytechnique 91128 Palaiseau Cedex FRANCE

ISOGENY CYCLES AND THE SCHOOF-ELKIES-ATKIN ALGORITHM

J.-M. COUVEIGNES, L. DEWAGHE, AND F. MORAIN

ABSTRACT. The heart of Schoof's algorithm for computing the cardinality m of an elliptic curve over a finite field is the computation of m modulo small primes ℓ. Elkies and Atkin have designed practical improvements to the basic algorithm, that make use of "good" primes ℓ. We show how to use powers of good primes in an efficient way. This is done by computing isogenies between curves over the ground field. We investigate the properties of the "isogeny cycles" that appear.

1. INTRODUCTION

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ where $q = p^r$, p prime. The curve is given by some equation $\mathcal{E}(X, Y) = 0$ in Weierstrass form

$$\mathcal{E}(X, Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$$

so that a generic point on the curve is given by (X, Y) mod $\mathcal{E}$. Let m be the number of points of E. It is well known that $m = q + 1 - t$, with t an integer satisfying $|t| \leq 2\sqrt{q}$. If q is small the problem of computing the cardinality of E is easy: one can simply enumerate all the points on E. When q is moderately large, say $q \approx 10^{30}$ (see for example [5] for q prime), one can use Shanks's baby-steps giant-steps method. When q is larger, say q up to 10^{500}, one must use Schoof's algorithm, or more precisely the improvements of Atkin, Elkies and more recently Couveignes to the basic scheme.

From a historical point of view, the emphasis was first put on finite fields of large prime characteristic. We note that Atkin gave some improvements to Schoof's algorithm as early as 1986 [1], coming up with the use of modular equations in 1988 [2]. In 1989, Elkies [13], described the use of good primes, some details of which were given in [6]. Then, in 1992, Atkin [3] gave the major improvements to Elkies' scheme and made it very practical, his record (March 1994) being computing the cardinality of $E_I : Y^2 = X^3 + 105X + 78153$ modulo $10^{275} + 693$. Other implementations include that of Müller [22] and of the third author [20], the record being the computation of the cardinality of $E_X : Y^2 = X^3 + 4589X + 91128$ modulo $10^{499} + 153$ (see [18, 20]). Recently, Schoof has written an account of the relevant theory in [24]. Some algorithmic details are given in [20] (see also [22]).

Elkies' ideas for the computation of isogenies between elliptic curves, although quite efficient when the characteristic is large do not apply as soon as we need to compute isogenies of degree greater than the characteristic. This will happen each time the field we consider is not primitive. A first solution to this problem was given by the first author replacing part of the modular formulae by considerations on formal groups and their isomorphisms [7, 8]. Lercier and the third author have implemented this algorithm for the case of $q = 2^r$, r up to 1009 [18, 17]. The theoretical aspects of the implementation for any p small are given in [17]. Note also that Lercier [16] has given a different algorithm for the special case $p = 2$. More recently, the first author [9] has given a new algorithm for all p.

Date: April 12, 1996.

The first author is a member of Option Recherche du Corps des Ingénieurs de l'Armement.

The third author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

This article is an improved and corrected version of [10].

Schoof's algorithm computes t mod ℓ for sufficiently many small primes ℓ, performing arithmetic modulo polynomials of degree $O(\ell^2)$. The basic algorithm can be extended to the case of prime powers ℓ^n as well. In Elkies' improvements, a prime ℓ can be either good or bad. When ℓ is good, one can compute t mod ℓ more rapidly than in Schoof's basic approach, performing arithmetic modulo polynomials of degree $O(\ell)$. Moreover, one can in this case compute t mod ℓ^n pretty much as in Schoof's case. However, one can do better in this case, and the purpose of this paper is to explain how this can be done.

Though the methods to be described do not improve on the complexity of the whole algorithm, they speed up the computations in practice and they are at the heart of the recent records.

We need to review first Schoof's algorithm, then we give a rough explanation of the improvements of Elkies and Atkin. After that, we explain the role of isogenies and deduce from that three algorithms that enable one to compute t mod ℓ^n. We note that our method has some common points with that of [19], but in a different context.

2. A rough description of the Schoof-Atkin-Elkies ideas

2.1. **The basic scheme.** We refer to [23]. Let E be a non-supersingular elliptic curve defined over $\mathbb{F}_q$. We recall that if π denotes the Frobenius action on the curve, then the ring of endomorphisms of the curve contains $\mathbb{Z}[\pi]$ and π satisfies the following degree 2 equation

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

where t is related to the cardinality of the curve by $\#E(\mathbb{F}_q) = q + 1 - t$ and satisfies $|t| \leq 2\sqrt{q}$.

Let ℓ be some prime number. Then π induces an automorphism of the ℓ-torsion space $E[\ell]$ which extends to Tate's module $T_\ell(E)$. Of course, equality (1) holds if we consider π as an element of $GL(E[\ell])$ or $GL(T_\ell(E))$. This remark leads to Schoof's idea: compute t modulo ℓ by looking at the action of π on the ℓ-torsion.

To achieve this goal, one first needs to compute the ℓ-torsion polynomial of E, $f_\ell^E(X)$, using the well known recurrence formulae (see for instance [17] for formulas valid in any characteristic). Then, a nonzero ℓ-torsion point on E is given by

$$(X, Y) \bmod (\mathcal{E}(X, Y), f_\ell^E(X)),$$

so that, for any residue λ mod ℓ, one can test whether the trace of π is λ by checking the following identity, written in homogeneous coordinates:

$$(X^{q^2}, Y^{q^2}, 1) \ominus [\lambda](X^q, Y^q, 1) \oplus [q](X, Y, 1) = (0, 1, 0) \bmod (\mathcal{E}, f_\ell^E).$$

For some λ the above equality will hold thus giving t mod ℓ. If one does the same computation for enough primes ℓ_i (i.e., such that $\prod_i \ell_i > 4\sqrt{q}$), then one knows the cardinality of E.

This leads to a polynomial time algorithm. From a practical point of view, the problem is the size of the torsion polynomials. Indeed, $f_\ell^E(X)$ is of degree $O(\ell^2)$. In practice one cannot hope to compute t mod ℓ in this way for $\ell > 31$, say.

2.2. **Elkies' ideas.** The whole theoretical background for this section can be found in [15], particularly chapters 12 and 13. In order to simplify the exposition, we assume ℓ is an odd prime (the case $\ell = 2$ will be treated in section 6).

The center of Elkies' ideas [13] is that if $\mathrm{disc}(\pi) = t^2 - 4q$ is a nonzero square modulo ℓ (the zero case works as well but in a slightly different way, see section 6) then π has two rational distinct eigenvalues τ_1 and τ_2 in $\mathbb{F}_\ell$ and even in $\mathbb{Z}_\ell$. Then, Tate's module decomposes as a sum of the two corresponding rational eigenspaces

$$T_\ell(E) = T_1^E \oplus T_2^E$$

and the ℓ-torsion as well. Such a prime ℓ is called good, and bad in the other case. (Note that a bad case has nothing to do with the pathological cases that will be introduced in section 6.)

We know that there exist $\ell+1$ isogenies of degree ℓ

$$E \stackrel{I_u}{\to} E_u \ , \ 1 \leq u \leq \ell+1$$

and we are looking for some explicit knowledge about these isogenies, such as their field of definition or their kernel for example. The kernel of those isogenies are the one dimensional eigenspaces of the ℓ-torsion. Furthermore, their definition field is the definition field of their kernel. Indeed, E_u is just defined to be the quotient of E by the corresponding linear subspace. So, the existence of two rational eigenvalues for the Frobenius implies the existence of two isogenies defined over the base field, each isogeny being of degree ℓ. We thus have two isogenous curves E_i, for $i=1,\ 2$, given by some equations $\mathcal{E}_i(X,Y)=0$ together with two isogenies $I_1 : E \to E_1$ and $I_2 : E \to E_2$, with kernel $T_1^E \cap E[\ell]$ and $T_2^E \cap E[\ell]$. For $P=(X,Y) \bmod \mathcal{E}$ a point on E, on each curve E_i, $i=1,2$, one has

$$I_i(P) = \left(\frac{k_i(X)}{h_i^2(X)}, \frac{g_i(X,Y)}{h_i^3(X)} \right) \bmod \mathcal{E}_i$$

where h_i is a polynomial of degree $(\ell-1)/2$. Therefore, the ℓ-torsion polynomial will have two (not necessarily irreducible) factors h_1 and h_2 of degree $(\ell-1)/2$, each corresponding to an eigenvalue.

All along the paper, we represent the ℓ-torsion on some elliptic curve as a parallelogram with sides the "rational directions". The picture for $\ell=5$ is given in Figure 1.

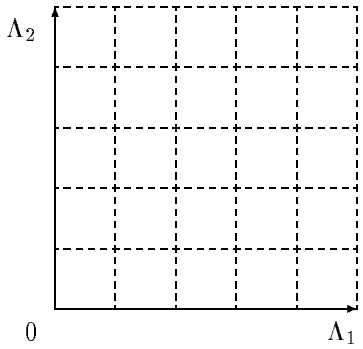


FIGURE 1. The 5-torsion structure

A nonzero point in $T_1^E \cap E[\ell]$ is given by $(X,Y) \bmod (\mathcal{E}(X,Y), h_1(X))$, which is much nicer than the above, because of the degree of h_1. In view of those considerations, one would like to replace, in Schoof's algorithm, the torsion polynomial by some rational factor h_i when it exists. Or, more conceptually, the $[\ell]$-isogeny by some isogeny of degree ℓ.

We now need to compute the I_i's, and firstly the h_i's. Brute force factorization of f_ℓ^E would be even more difficult than the whole Schoof's method since we would need to compute

$$X^{(q^d-1)/2} \bmod f_\ell^E$$

for some integer d. We will explain next how to do compute I_i efficiently.

2.3. **Computing isogenies over $\mathbb{C}$.** It is easier to consider this particular case first. Details are given in [3, 13, 6, 20, 22].

Suppose that we are dealing with a complex curve $E=\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, of invariant $j(\tau)$ with $\Im(\tau)>0$. The curve E admits an equation of the form $Y^2=X^3+AX+B$. Let $\Phi_\ell(X,Y)$ be the modular equation of index ℓ, that is the algebraic relation between $j(x)$ and $j(\ell x)$ (with $x=\exp(2i\pi\tau)$):

$$\Phi_\ell(X,Y) = \sum_{r=1}^{\ell+1} C_r(Y) X^r$$

where the C_r's have integer coefficients and $C_{\ell+1}(Y) = 1$. Then one knows that E and E' are ℓ-isogenous if and only if $\Phi_\ell(j(E'), j(E)) = 0$. In other words, the j-invariant of the curves E' that ℓ-isogenous to E are the roots of $\Phi_\ell(X, j(E)) = 0$.

Let $\wp(z)$ denote the Weierstrass function of E:

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

where the c_k are in $\mathbb{Q}(A, B)$: $c_1 = -A/5, c_2 = -B/7$, and for $k \geq 3$:

$$c_k = \frac{3}{(k-2)(2k+3)} \sum_{h=1}^{k-2} c_h c_{k-1-h}.$$

For ℓ odd, the ℓ-th division polynomial is then simply

$$f_\ell^E(X) = \ell \prod_{\substack{0 \leq r \leq (\ell-1)/2 \\ 0 \leq s < \ell \\ r>0 \text{ or } 1 \leq s \leq (\ell-1)/2}} (X - \wp((r + s\tau)/\ell))$$

and is in fact in $\mathbb{Q}(A, B)[X]$. This polynomial has a factor

$$h_1(X) = \prod_{r=1}^{(\ell-1)/2} (X - \wp(r/\ell))$$

which has coefficients in an extension of degree $\ell + 1$ of $\mathbb{Q}(A, B)$. We let

$$p_k = \sum_{r=1}^{(\ell-1)/2} \wp(r/\ell)^k.$$

Elkies shows how to compute all p_k's using only p_1, p_2 and p_3. He also shows that p_1 can be obtained as a root of a degree $\ell+1$ equation, whereas p_2 and p_3 can be obtained from the coefficients A_1 and B_1 of the curve $E_1 = \mathbb{C}/(\frac{1}{\ell}\mathbb{Z} + \tau\mathbb{Z})$ which is isogenous to E. We make the important remark that the periods of E_1 are the image of that of E by the Atkin-Lehner involution, $W_\ell(F(\tau)) = F(-1/\ell\tau)$ for any function F (of weight 0), and in particular $W_\ell(j(\tau)) = j(-1/\ell\tau) = j(\ell\tau)$.

In Atkin's approach, one uses any modular relation between $j(x)$ and a function $F(x)$ on $\Gamma_0(\ell)$. Atkin distinguishes between two types of modular equations: the "canonical" one and the "star" one. In the first case, one uses the function $\mathcal{F}_\ell(\tau) = \ell^s(\eta(\ell\tau)/\eta(\tau))^{2s}$ where $s = 12/\gcd(12, \ell - 1)$. As Atkin shows, with this function, it is easy to compute $j_1 = j(\ell\tau)$ using $F_1 = \mathcal{F}_\ell(\tau)$ without finding the roots of $\Phi_\ell^c(W_\ell(F_1), Y) = \Phi_\ell(\ell^s/F_1, Y)$, but on the other hand the valence of $\mathcal{F}_\ell$ grows linearly as a function of ℓ. In the star case, one uses a function with smallest possible valence on $X_0^*(\ell) = X_0(\ell)/W_\ell$. This has the advantage of having a very small valence, but we have then to compute the roots of $\Phi_\ell^*(W_\ell(F_1), Y) = \Phi_\ell^*(F_1, Y)$. One can compute all quantities p_1, A_1 and B_1 using algebraic relations as explained in the references. We will denote by Ψ_ℓ any modular equation.

2.4. **Over $\mathbb{F}_q$.** Let E be any elliptic curve. As above, the roots of $\Psi_\ell(X, j(E))$ define elliptic curves over an extension field $\mathbb{F}_{q^e}$ which are ℓ-isogenous to E over $\mathbb{F}_{q^e}$. The splitting of $\Psi_\ell(X, j(E))$ is described by Galois theory and can be of the form: $(11r \ldots r)$, in which case there are two curves defined over $\mathbb{F}_q$ – this is the good case; $(r \ldots r)$ – this is the bad case; (1ℓ) or $(1 \ldots 1)$ – two pathological cases (see section 6). In each of the first two cases, r is the order of α/β where α and β are the roots of $X^2 - tX + q = 0$ in $\mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$.

Now suppose we are in the good case. We have to distinguish two cases: the first one (referred to later on as CaseLarge) is when one can use the Weierstrass equation form of E and p is large

enough compared to ℓ to be able to use the formulas of section 2.3 that involve small denominators. This in turn implies $p \geq c\ell$ for some small constant c. The second case, CaseSmall, corresponds to $p < c\ell$ and encompasses the case $p = 2$ or $p = 3$ where we cannot use the Weierstrass normal form. In this case, one must use Couveignes's algorithms [7, 17, 9] or Lercier's method [16] to compute I_1.

2.5. **The algorithm in brief.** We summarize the results given above as follows:
procedure FindTModL(E, p, ℓ)

1. compute a modular equation $\Psi_\ell(X, Y)$;
2. **if** $\Psi_\ell(X, j(E))$ has two roots in $\mathbb{F}_q$ **then**
   (a) compute h_1 using the techniques described above;
   (b) find the eigenvalue τ, $0 < \tau < \ell$ such that
   $$(X^q, Y^q) = [\tau](X, Y) \bmod (\mathcal{E}(X, Y), h_1(X))$$
   in $\mathbb{F}_q$;
   (c) compute $t \equiv (\tau^2 + q)/\tau \bmod \ell$.

If $\Psi_\ell(X, j(E))$ has 1 or $\ell+1$ roots, then we know that $t^2 \equiv 4q \bmod \ell$ (see [3]). In the case where Ψ_ℓ has no roots, one can use restrictions on t given by the splitting of Ψ. See the references given for more details.

3. Walking along the rational cycles of isogenous curves

3.1. **Theory.** We now suppose that $\pi \in GL(T_\ell)$ has two distinct rational eigenvalues τ_1 and τ_2. We notice that, since the two isogenies I_1 and I_2 are rational, they commute with π. This implies that on the isogenous curves, the eigenvalues of the Frobenius are the same, so we can define $T_i^{E_j}$ for i, $j \in \{1, 2\}$ as the eigenspace of the Tate module of E_j associated to the eigenvalue τ_i. Since the eigenspaces T^{E_1} and T^{E_2} are independent, I_1 induces a bijection between T^{E_2} and the corresponding eigenspace on E_1 and reciprocally I_2 induces a bijection between T^{E_1} and the corresponding eigenspace on E_2.

The existence of two distinct rational eigenvalues has another interesting consequence. It is that E_1 again has two rational isogenies of degree ℓ, one associated to each of the two eigenvalues τ_1 and τ_2. We call I_{j1} and I_{j2} the isogenies from E_j associated to τ_1 and τ_2 respectively. On the other hand, we know that, since I_1 is rational, the dual isogeny I_1^* must be rational as well (by uniqueness of it). Therefore I_1^* equals either I_{11} or I_{12}. Because $I_1^* \circ I_1$ is the multiplication by ℓ, the kernel of I_1^* has intersection 0 with $T_1^{E_1}$ (otherwise $I_1^* \circ I_1$ would have points of order ℓ^2 in its kernel). Therefore, I_1^* is not I_{11} and so it is I_{12}. We could express that by saying that the two rational directions are not only independent but dual. We show all that on Figure 2.
Now, if E is a curve over $\mathbb{F}_q$ such that $t^2 - 4q$ is a nonzero square mod ℓ we can build two periodic sequences of isogenous curves over $\mathbb{F}_q$. These sequences define two permutations $\mathcal{I}_1$ and $\mathcal{I}_2$ on the set of elliptic curves over $\mathbb{F}_q$, classified up to $\mathbb{F}_q$-isomorphisms. The permutation $\mathcal{I}_i$ is generated by the quotient of E by τ_i and the two permutations are inverse of each other:

$$E \xrightarrow{I_1} E_1 \xrightarrow{I_{11}} E_{11} \xrightarrow{I_{111}} \cdots$$

$$E \xrightarrow{I_2} E_2 \xrightarrow{I_{22}} E_{22} \xrightarrow{I_{222}} \cdots$$

These series are computed in the following way. We use some modular equation $\Psi_\ell(X, Y)$, as in section 2. Let us call j_0 the invariant of E and let us solve $\Psi_\ell(X, j_0) = 0$ over $\mathbb{F}_q$. If we are in the "good case" we have two rational distinct simple roots F_1 and F_2, from which we compute two curves E_1 and E_2 of respective invariants j_1 and j_2. Let us now solve the equation $\Psi_\ell(X, j_1) = 0$ over $\mathbb{F}_q$. We find two rational distinct simple roots, one of them being $W_\ell(F_1)$ and corresponding

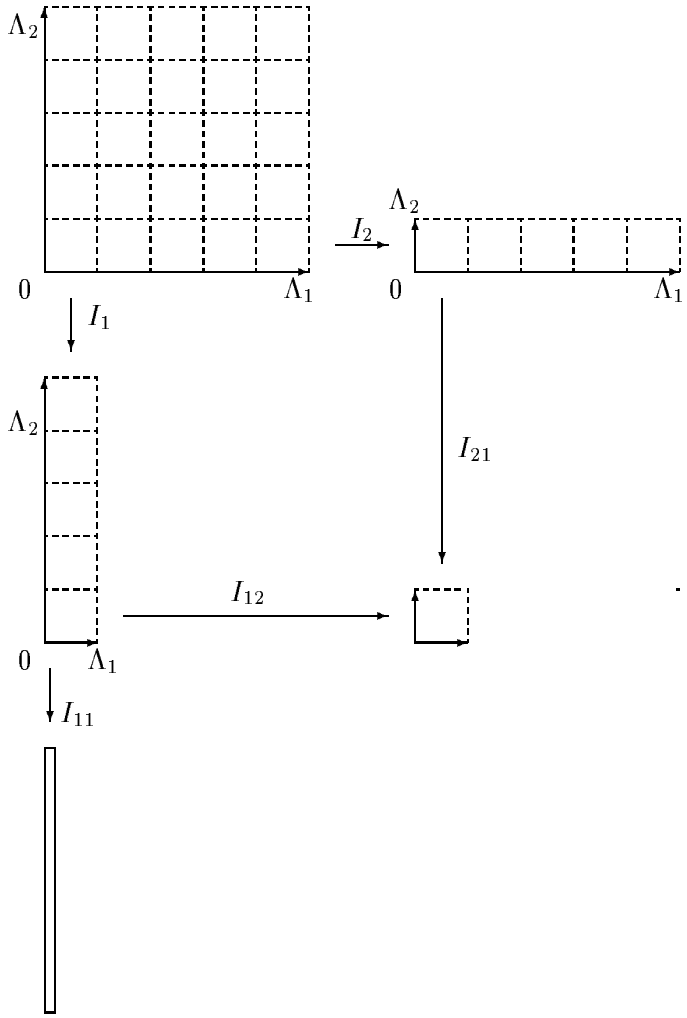


FIGURE 2. Action of the isogenies

to the dual isogeny I_1^*. We choose the other one and call it F_{11}, yielding E_{11}. We go on, solving the equation $\Psi_\ell(X, j_{11}) = 0$, etc.

Since the field is finite, the two sequences of curves are periodic and they provide an explicit description of the two rational subspaces of Tate's module.

3.2. **Example.** Let $p = 101$ and consider all the (classes of) curves E for which $(p+1) - \#E = t = 3$. There are 8 of them and the following table gives their invariant and a representative for each class. These curves were obtained by brute force, but they could have been obtained by noting that $3^2 - 4 \times 101 = -395$, implying that all curves have complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-395})$ and therefore their j-invariant are the roots of the 8-degree Weber polynomial as in [4]. We note $E = [a, b]$ for the curve of equation $Y^2 = X^3 + aX + b$.

j	E	j	E	j	E	j	E
2	$[68, 79]$	10	$[19, 59]$	15	$[56, 41]$	20	$[27, 18]$
34	$[13, 51]$	56	$[3, 2]$	82	$[53, 37]$	90	$[49, 100]$

Starting from $E_0 = [68, 79]$, $J_0 = 2$, using $\ell = 7$, one first finds

$$\Phi_7^c(X, 2) \equiv (F + 84)(F + 64)(F^6 + 82F^5 + 81F^4 + 49F^3 + 32F^2 + 34F + 68) \bmod 101.$$

We choose $F_1 = 17$ and find $\tau_1 = 6$. The permutation $\mathcal{I}_1$ is then given in

E	$j(E)$	$F(E)$
$[68, 79]$	2	17
$[27, 68]$	82	14
$[50, 89]$	56	33
$[31, 28]$	10	9
$[45, 15]$	34	20
$[47, 87]$	90	100
$[42, 63]$	20	43
$[97, 32]$	15	45
$[56, 31]$	2	

The other permutation starts using $F_2 = 37$ and corresponds to $\tau_2 = 4$.

3.3. **Application to Schoof's algorithm.** The factor of $f_\ell^E(X)$ corresponding to $T_1^E \cap E[\ell]$ is h_1, the denominator of I_1. Now, if we want the factor of $f_{\ell^2}^E$ corresponding to $T_1^E \cap E[\ell^2]$, we proceed in the following way. We first compute the polynomial h_{11} which is the denominator of I_{11}, in the same way we computed h_1 except that we replace E by E_1 and pay attention not to confuse I_{11} with $I_1^* = I_{12}$. Indeed we consider the isogeny from E_1 associated with τ_1. Since $I_1(T_1^E \cap E[\ell^2]) = T_1^{E_1} \cap E_1[\ell]$, one has $I_{11} \circ I_1(T_1^E \cap E[\ell^2]) = O_{E_{11}}$ and therefore $\mathrm{Ker}(I_{11} \circ I_1) \subset E[\ell^2]$. In this way, we obtain a factor of $f_{\ell^2}^E$ as the numerator of $h_{11} \circ I_1$. We can iterate this scheme and compute a factor of degree $\ell^{k-1}(\ell - 1)/2$ if ℓ is odd (see section 6.4 for $\ell = 2$) of the polynomial $f_{\ell^k}^E$ and then, using Schoof's idea compute the cardinality of E modulo ℓ^k rather than just ℓ. This allows us to take more advantage of the small good primes.

4. First algorithm and its implementation

4.1. **Presentation of the algorithm.** The algorithm runs as follows:

procedure ComputeTModLn(E, p, ℓ, $nmax$)
{computes t mod ℓ^n for $n \leq nmax$ when ℓ is an Elkies prime}

1. find the roots of $\Psi_\ell(X) = \Psi_\ell(X, j(E))$ in $\mathbb{F}_q$;
2. **if** Ψ_ℓ has two distinct rational roots **then**
   (a) compute the equation $\mathcal{E}_1(X, Y) = 0$ of E_1 and I_1 and deduce from this a factor h_1 of f_ℓ^E using E_1;
   (b) find the eigenvalue τ_1;
   (c) **for** $n := 2$ **to** $nmax$ **do**
      (i) (find next curve) find the root F_n of $\Psi_\ell(X, j(E_{n-1}))/(X - W_\ell(F_{n-1}))$; deduce from this the equation $\mathcal{E}_n$ of E_n;
      (ii) compute the isogeny I_n between E_{n-1} and E_n and the factor h_n of $f_\ell^{E_n}$;
      (iii) (compute new factor) set h to the numerator of $h_n \circ I_{n-1} \circ \cdots \circ I_2 \circ I_1$; {at this point h is a factor of $f_{\ell^n}^E$ of degree $\ell^{n-1}(\ell - 1)/2$ };
      (iv) (find eigenvalue modℓ^n) find λ, $0 \leq \lambda < \ell$ such $\tau_n = \tau_{n-1} + \lambda\ell^{n-1}$ is such that $(X^q, Y^q) = [\tau_{n-1}](X, Y) \oplus [\lambda](\ell^{n-1}(X, Y))$ in $\mathbb{F}_q[X, Y]/(\mathcal{E}_n(X, Y), h(X))$.

4.2. **Computing h_1 and I_1.** One first solves $\Psi_\ell(X, j_0) \equiv 0$ in $\mathbb{F}_q$ for a root F_1 and then one computes j_1 as a root of $\Psi_\ell(W_\ell(F_1), Y)$ over $\mathbb{F}_q$. (Note that in the case $q = p$ large, one can do better in the canonical case, see the references already given.) Each solution y yields a putative factor $h_y(X)$ of $f_\ell^E(X)$ that is then checked by testing whether $\ell(X, Y) = 0 \bmod (\mathcal{E}(X, Y), h_y)$. The computation of h_y differs in the cases of p large and p small.

4.2.1. *The case* CaseLarge. In this case, we are dealing with curves of the form $Y^2 = X^3+AX+B$. We must distinguish the case $\ell = 2$ and ℓ odd.

In the case ℓ odd, one computes first h_y (using the techniques described above) and then the isogeny. The isogeny is of the form:

$$I_1(X,Y) = \left(\frac{k_1(X)}{h_1(X)^2}, \frac{g_1(X,Y)}{h_1(X)^3}\right)$$

where $k_1(X)$ is a polynomial of degree ℓ with coefficients in $\mathbb{F}_q$. Let $\wp_1(z)$ denote the Weierstrass function of E_1. Then

$$\wp_1(z) = \frac{k_1(\wp(z))}{h_1(\wp(z))^2}.$$

Replacing $\wp$, $\wp_1$ and h_1 by their value, one deduces easily from this the coefficients of k_1. Alternatively, one can use the improvements of the second author [11] to Vélu's formulas [27] to compute the fraction.

Examples. Let us take $E : Y^2 = X^3+2X+3$ over $\mathbb{F}_{97}$. We use the so-called "canonical" equation of $X_0(5)$, namely the relation between $\mathcal{F}_5(x) = 5^3(\eta(5\tau)/\eta(\tau))^6 = 125(x+6x^2+\cdots)$ and $j(x)$, which is

$$\Phi_5^c(X,Y) = X^6 + 30\,X^5 + 315\,X^4 + 1300\,X^3 + 1575\,X^2 - (Y-750)\,X + 125.$$

One computes $j_0 = j(E) = 36$ and $\Phi_5^c(X,36)$ factors modulo 97 as

$$(X+25)(X+10)(X^4+92X^3+46X^2+67X+49).$$

We choose $F_1 = 87$ and find easily that j_1 is the root of $\Phi_5^c(5^3/F_1, Y) \equiv 0 \bmod p$ that is $j_1 = 48$, from which we deduce from that $E_1 : Y^2 = X^3+96X+83$. We also find that

$$h_1(X) = X^2 + 16X + 30.$$

Now, one has

$$\wp(z) = z^{-2} + 19z^2 + 55z^4 + 88z^6 + 91z^8 + O(z^{10}),$$
$$\wp_1(z) = z^{-2} + 39z^2 + 2z^4 + 22z^6 + 83z^8 + O(z^{10})$$

so that

$$\wp_1(z)h_1(\wp(z))^2 = z^{-10} + 32z^{-8} + 43z^{-6} + 83z^{-4} + 93z^{-2} + 76 + O(z^2)$$

from which we recognize that

$$k_1(X) = X^5 + 32X^4 + 45X^3 + 92X^2 + 18X + 35.$$

Now, we want to compute E_{11} and so we find

$$\Phi_5^c(X, j_1) \equiv (X+61)(X+5)(X^4+61X^3+58X^2+13X+2) \equiv 0 \bmod p.$$

We note that a solution to this is $W_5(F_1) = 5^3/F_1 \equiv 36 \bmod p$. We must discard this one, since we would go back to E_0. So, we take $F_{11} = 92$ and find $E_{11} : Y^2 = X^3+95X+66$, together with

$$h_{11}(X) = X^2 + 81X + 84$$

and

$$I_{11}(X) = \frac{X^5+65X^4+75X^3+85X^2+6X+71}{X^4+65X^3+36X^2+28X+72}.$$

A factor of $f_{25}^E(X)$ is then the numerator of $h_{11}(I_1(X))$ namely

$$X^{10}+48X^9+77X^8+54X^7+38X^5+36X^4+40X^3+3X^2+90X+5.$$

Let us turn our attention to the case $\ell = 2$. The methods described by Atkin enable one to compute the isogenous curve, but not the factor of the division polynomial. However, one can compute the Weierstrass function of the isogenous curve and deduce from this the isogeny I_1 as in [26] using continued fractions and thus h_1. Computational examples will be given in section 6.4.

4.2.2. *The case* CaseSmall. In this case, we compute first the isogeny and deduce from this the factor we are looking for. We refer to [7, 17] for more details. This is also true of the new methods of Lercier and Couveignes. Note that computing isogenies of degree p in characteristic p can be done using [14].

4.2.3. *Analysis.* Let us compare the cost of finding t mod ℓ^n and that of finding t mod ℓ. There are essentially two "new" operations to perform. The first one is the computation of $h_n \circ I_{n-1} \circ \cdots \circ I_2 \circ I_1$, the second the cost of finding the eigenvalue. For this latter problem, the fast techniques of [21] and [12] can be used. As far as the first problem is concerned, we evaluate

$$(((h_n \circ I_{n-1}) \circ \cdots) \circ I_2) \circ I_1$$

so that the basic operation is the computation of the numerator of $A(B/C)$ where A, B and C are polynomials and A has degree d_A. The best we can do is $3d_A$ multiplications of polynomials, if we can store the powers of C.

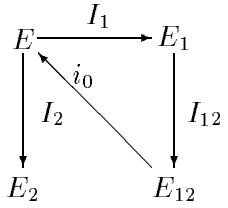
5. Improvements

For the sake of simplicity, we assume ℓ odd and that we are in CaseLarge. We will indicate the suitable modifications for CaseSmall later on.

5.1. **Using the best direction.** It is easy to see that the algorithm works also if we replace h_1 by one of its factors. Let d_1 denote the order of τ_1 in $\mathbb{F}_\ell$, and let $\delta_1 = d_1$ if d_1 is odd, $d_1/2$ otherwise (we call δ_1 the *semi-order* of τ_1). Then h_1 factorizes in $\mathbb{F}_q$ as a product of $(\ell-1)/(2\delta_1)$ factors each of degree δ_1 (see [3]).

Replacing h_1 by any one of these factors, we can compute a factor of degree $\delta_1 \ell^{n-1}$ of $f_{\ell^n}^E$, by lifting a factor of degree δ_1 of $f_\ell^{E[n]}$.

This approach suggests to take the direction of smallest semi-order. We can show that this is not too costly by looking at the following picture:



We summarize the relevant relations between these curves in the following proposition.

Proposition 5.1. *The curve E_1 is built using F_1 and E_2 using F_2. The curve E_{12} is isomorphic to E. More precisely, if $E = [A, B]$, then $E_{12} = [\ell^4 A, \ell^6 B]$ and $i_0 : (X, Y) \mapsto (X/\ell^2, Y/\ell^3)$. Moreover, E_{12} can be built from E_1 using $W_\ell(F_1)$ and $p_1(E_{12}) = -\ell p_1(E)$.*

In this way, it is easy to build a factor of $f_\ell^{E_1}$ in direction 2 from the knowledge of a factor of f_ℓ^E in direction 1. This remark enables us to add a step (b') in algorithm ComputeTModLn:

(b') compute τ_2 and the semi-orders δ_1 and δ_2; **if** $\delta_2 < \delta_1$ **then** replace (E, E_1, h_1, τ_1) by $(E_1, E_{12}, h_{12}, \tau_2)$;

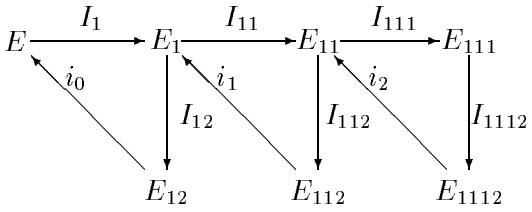
The remaining of the algorithm is not altered. Note that this time, we really work on E_1, which is isogenous to E. In the sequel, we will give two other applications of this change of directions.

5.1.1. *The case* CaseSmall. Changing directions cannot be done as easily when $p \leq 3$. When $p = 2$, we are dealing with curves of equation $Y^2 + XY = X^3 + a_6$ for which $j(E) = 1/a_6$. Since $j(E_{12}) = j(E)$, this leads to $E_{12} = E$. On the other hand, we do not know of any relationship between the first coefficients of the division polynomials, so that the isogeny must be computed from scratch, which can be costly when ℓ is large. When $p = 3$, $E = [a_2, a_6]$ has equation $Y^2 = X^3 + a_2X^2 + a_6$, and one has $E_{12} = [\ell^2 a_2, \ell^6 a_6]$ which turns out to be E since for every odd prime number ℓ, one has $\ell^2 \equiv 1 \bmod 3$.

5.2. A first improved strategy.

5.2.1. *Presentation of the method.* For the sake of simplicity, we will write $E_{1\times n}$ for the n-th curve in direction 1.

The idea described in algorithm ComputeTModLn would require the factorization of $h_{1\times n}(X)$ for each n in order to be really worthwhile. One can do better, namely factor a polynomial once for all. Let us look at the following picture.



Let h_{12} be a factor of the polynomial $f_\ell^{E_1}$, obtained in the direction τ_2. Then the numerator of $h_{12} \circ i_1 \circ I_{112}$ yields a factor h_{112} of $f_{\ell^2}^{E_{11}}$ also in the direction τ_2. Similarily, we get a factor h_{1112} of $f_{\ell^3}^{E_{111}}$ as the numerator of $h_{112} \circ i_2 \circ I_{1112}$.

We remark that all curves $E_{1\times n}$ have the same cardinality and the same eigenvalue in the same direction. Hence, computing $t \bmod \ell^n$ can be done using any curve, and in particular the curve $E_{1\times n}$.

The first improved algorithm runs as follows.

procedure ComputeTModLnBetter(E, p, ℓ, $nmax$)

1. find the roots of $\Psi_\ell(X, j(E))$;
2. **if** Ψ_ℓ has two distinct rational roots **then**
   (a) compute a factor h_1 of f_ℓ^E;
   (b) find the eigenvalue τ_1 and deduce τ_2 from it;
   (c) renumber the directions in such a way that direction 2 is associated with the eigenvalue τ_2 of smallest semi-order; compute the factor h of smallest degree of h_{12} and set $\theta_1 = \tau_2$, $\delta = \delta_2$;
   (d) **for** $n := 2$ **to** $nmax$ **do**
      (i) (find next curve) compute $E_{1\times n}$, $E_{1\times n,2}$ and $I_{1\times n,2}$;
      (ii) (compute new factor) set h to the numerator of $h \circ i_{n-1} \circ I_{1\times n,2}$; {at this point h is a factor of $f_{\ell^n}^{E_{1\times n}}$ of degree $\delta\ell^{n-1}$ };
      (iii) (find eigenvalue modℓ^n) find λ, $0 \leq \lambda < \ell$ such $\theta_n = \theta_{n-1} + \lambda\ell^{n-1}$ is such that $(X^q, Y^q) = [\theta_{n-1}](X, Y) \oplus [\lambda](\ell^{n-1}(X, Y))$ in $\mathbb{F}_q[X, Y]/(\mathcal{E}_{1\times n}(X, Y), h(X))$.

5.2.2. *Example.* Let us consider once again the case $E = [2, 3]$ modulo 97. Having found the factor $h_1(X) = X^2 + 16X + 30$, it is easy to check that $\tau_1 = 2$ and therefore $\tau_2 = 1$. We see that direction 2 is already the best one, so we do not have to renumber the directions. We compute

$$h_{12} = X^2 + 17X + 57 = (X + 56)(X + 58) \bmod 97.$$

We find as above that $E_{11} = [95, 66]$. The curve E_{112} is then $[5^4 \times 95, 5^6 \times 66]$ and we have

$$I_{112} = \frac{X^5 + 63X^4 + 50X^3 + 33X^2 + 3X + 49}{X^4 + 63X^3 + 3X^2 + 12X + 79}.$$

From this, we deduce that h_{112} is the numerator of

$$(X + 56) \circ (I_{112}/5^2)$$

which is

$$X^5 + 8X^4 + 77X^3 + 62X^2 + 22X + 69.$$

We then look for the eigenvalue $1 + \lambda 5$ and find that it is 1.

Going further, we compute $E_{111} = [1, 80]$ and

$$I_{1112} = \frac{X^5 + 28X^4 + 3X^3 + 19X^2 + 21X + 89}{X^4 + 28X^3 + 5X^2 + 42X + 75}$$

yielding h_{1112} as the numerator of

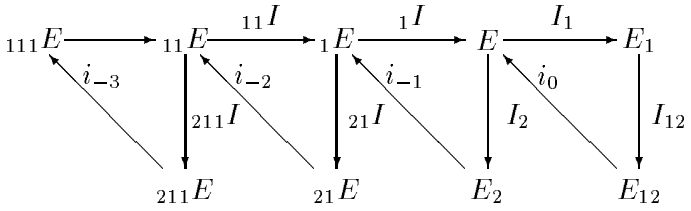
$$h_{112} \circ (I_{1112}/5^2)$$

that is

$$\begin{aligned} h_{1112} \;=\; & X^{25} + 49X^{24} + 75X^{23} + 26X^{22} + 54X^{21} + 16X^{20} + 69X^{19} + 80X^{18} + 78X^{17} \\ & +40X^{16} + 60X^{15} + 12X^{14} + 49X^{13} + 28X^{12} + 61X^{11} + 28X^{10} + 19X^9 \\ & +29X^8 + 60X^7 + 86X^6 + 78X^5 + 48X^4 + 54X^3 + 86X^2 + 22X + 22 \end{aligned}$$

and subsequently the eigenvalue is 101 mod 125.

5.3. **Walking backwards.** Let us come back to our picture between curves and let us start backwards in the cycle. We will note ${}_{d_k,d_{k-1},\ldots,d_1}E$ a curve built backwards following first direction d_1, then d_2, etc. and a similar notation for isogenies.



In this version, we are closer to the basic algorithm. We find that a factor of ${}_1h$ of $f_{\ell^2}^{{}_1E}$ is the numerator of $h_1 \circ {}_1I$. Similarily, we would get a factor of $f_{\ell^3}^{{}_{11}E}$ as the numerator of $h_1 \circ {}_1I \circ {}_{11}I$ or equivalently, as the numerator of ${}_1h \circ {}_{11}I$.

The final algorithm is given below. The invariant of the main loop is (E, E_2, F_2, h). We give the algorithm in a compact form.

procedure ComputeTModLnBackwards(E, p, ℓ, $nmax$)

1. find the roots of $\Psi_\ell(X, j(E))$;
2. if Ψ_ℓ has two distinct rational roots then
   (a) compute a factor h_1 of f_ℓ^E;
   (b) find the eigenvalue τ_1 and deduce τ_2 from it;
   (c) renumber the directions in such a way that direction 1 is associated with the eigenvalue τ_1 of smallest semi-order; compute a factor h of h_1 of smallest degree and set $\theta_1 = \tau_1$, $\delta = \delta_1$;
   (d) compute E_2 using the second root of $\Psi_\ell(X, j(E))$;

(e) **for** $n := 2$ **to** $nmax$ **do**
{at this point E is isogenous to E_2 via F_2 and h contains a factor of degree $\delta\ell^{n-2}$ of $f^E_{\ell^{n-1}}$.}
(i) (find next curve) find ${}_1E$ using proposition 5.1 and set ${}_1F = W_\ell(F_2)$;
(ii) compute the isogeny ${}_1I$ between ${}_1E$ and E;
(iii) (compute new factor) set h to the numerator of $h \circ {}_1I$; {at this point h is a factor of $f^{{}_1E}_{\ell^n}$ of degree $\delta\ell^{n-1}$ };
(iv) (find eigenvalue modℓ^n) find λ, $0 \leq \lambda < \ell$ such that $\theta_n = \theta_{n-1} + \lambda\ell^{n-1}$ satisfies $(X^q, Y^q) = [\theta_{n-1}](X, Y) \oplus [\lambda](\ell^{n-1}(X, Y))$ in $\mathbb{F}_q[X, Y]/({}_1\mathcal{E}(X, Y), h(X))$;
(v) (update data) **if** $n < nmax$ **then**
(A) compute the other root ${}_{21}F$ of $\Psi(X, j({}_1E))$ by computing

$$\gcd(X^q - X, \Psi_\ell(X, j({}_1E))/(X - {}_{21}F))$$

and deduce from this ${}_{21}E$;
(B) set $F_2 = {}_{21}F$, $E_2 = {}_{21}E$ and $E = {}_1E$,

Remarks.

1. We see that when we content ourselves with $nmax = 2$, the computation of ${}_1h$ is essentially free since we alreay know F_2 (no computation of X^q modulo a polynomial is needed).

2. In step (c), we might have to factor h_2 instead of h_1. The first step for this is the computation of X^q mod h_2. This quantity can be evaluated as the abscissa of $\tau_2(X, Y)$ over $\mathbb{F}_q[X, Y]/(\mathcal{E}_2(X, Y), h_2)$, which is faster.

3. There is another way of computing ${}_1E$, which is slightly less efficient. It can be shown that the formulas given in [20] can be inverted to give the corresponding coefficients. This works particularily well if we know the invariant of ${}_1E$ (because there is only one possible value, say).

5.3.1. *Example.* Again, let $E = [2, 3]$, $p = 97$, $\ell = 5$. We already computed $F_1 = 87$, $E_1 = [96, 83]$ and $\tau_1 = 2$, $\tau_2 = 1$. Since we already know the value of $F_2 = 72$, we get $E_2 = [43, 39]$ and $h_2 = X^2 + 14X + 46$.

We renumber the directions in such a way that direction 1 is the best one. We thus have $E_1 = [43, 39]$ and $h_1 = X^2+14X+46 = (X+17)(X+94)$, $\tau_1 = 1$, $\delta = 1$; $E_2 = [96, 83]$ and $F_2 = 87$. We set $h = X + 17$. Walking the isogeny cycle backwards, using ${}_1F = W_5(F_2) = 5^3/F_2 = 36$ we find that ${}_1E = [9, 71]$ and

$${}_1I = \frac{X^5 + 13\,X^4 + 27\,X^3 + 69\,X^2 + 52\,X + 4}{X^4 + 13\,X^3 + 45\,X^2 + 30\,X + 61}$$

from which ${}_{1\times 2}h = X^5 + 30\,X^4 + 54\,X^3 + 58\,X^2 + 77\,X + 71$. Once this is done, we factor

$$\Phi^c_5(X, j({}_1E))/(X - 36) \equiv (X + 5)\left(X^4 + 61\,X^3 + 58\,X^2 + 13\,X + 2\right) \bmod 97$$

and thus ${}_{21}F = 92$, from which ${}_{21}E = [18, 81]$.

The following step yields ${}_{11}E = [32, 95]$ and

$${}_{11}I = \frac{X^5 + 15\,X^4 + 73\,X^3 + 96\,X^2 + 89\,X + 12}{X^4 + 15\,X^3 + 49\,X^2 + 79\,X + 48}$$

from which we deduce that

$$\begin{aligned}{}_{11}h = X^{25} &+ 8\,X^{24} + 69\,X^{23} + 34\,X^{22} + 17\,X^{21} + 29\,X^{20} + 76\,X^{19} + 7\,X^{18} + 86\,X^{17} + 22\,X^{16} + 20\,X^{15} \\ &+ 10\,X^{14} + 64\,X^{13} + 15\,X^{12} + 66\,X^{11} + 82\,X^{10} + 39\,X^9 + 2\,X^8 + 79\,X^7 + 25\,X^6 \\ &+ 66\,X^5 + 52\,X^4 + 43\,X^3 + 29\,X^2 + 16\,X + 44\end{aligned}$$

is a factor of $f^{{}_{11}E}_{5^3}$.

6. Pathological cases

6.1. **Presentation of the problem.** We will make here the assumption that $(q,\ell)=1$. The case $\ell \mid q$ is studied for example in [17].

Elkies' approach works when π has rational $\mathbb{F}_\ell$-eigenvalues. We have seen above how to deal with the case where the eigenvalues are distinct. The pathological cases corresponds to double eigenvalues, which means that $f(X)=X^2-tX+q$ is a square modℓ.

We start with a few basic remarks concerning the action of the Frobenius endomorphism on Tate's module in the case where t^2-4q is zero modulo ℓ. In such a situation one may expect to achieve something provided at least t^2-4q is a square in $\mathbb{Z}_\ell$. Since t^2-4q is not zero (otherwise the curve would be supersingular) we should then have t^2-4q is zero modulo ℓ^2. If t^2-4q is a square in $\mathbb{Z}_\ell$, there do exist two distinct solutions of $X^2-tX+q=0$ in $\mathbb{Z}_\ell$ and two associated eigenspaces of T_ℓ.

Remember that T_ℓ is the limit

$$E[\ell] \leftarrow E[\ell^2] \leftarrow E[\ell^3] \leftarrow \dots .$$

One may ask why one chooses such a fancy definition instead of the more natural union of all $E[\ell^k]$. The point is that T_ℓ is a dimension 2 free module on $\mathbb{Z}_\ell$ whereas $\cup E[\ell^k]$ is a module of infinite type. In particular any base of T_ℓ over $\mathbb{Z}_\ell$ cannot be made of torsion points!

Now that we have eigenspaces in T_ℓ we may expect that we are done. But there is indeed a problem. We are working in the finite quotients $E[\ell^k]$ of T_ℓ and these are not vector spaces apart for the first one which is a vector space over $\mathbb{F}_\ell$. Therefore the existence of roots of X^2-tX+q modulo ℓ^k (for example those obtained by reducing the roots in $\mathbb{Z}_\ell$ modulo ℓ^k) does not imply the existence of corresponding invariant spaces in $E[\ell^k]$. Here we have to be more precise. We call a *full subspace* of $E[\ell^k]$ any submodule which is complete under division by ℓ in $E[\ell^k]$ (if it is non zero, it must contain an element of order ℓ^k). In general, the images in $E[\ell^k]$ of the eigenspaces E_1 and E_2 of π will not be full subspaces but just cyclic subgroups with cardinality a divisor of ℓ^k. We call them *pseudo-eigenspaces.*

In order for π to have rational eigenvalues in $\mathbb{Z}/\ell^n\mathbb{Z}$, $n\geq 2$, it is necessary that $f(X)$ have roots in $\mathbb{Z}/\ell^n\mathbb{Z}$. Define the equation

$$(R_n) \quad f(X)\equiv 0 \bmod \ell^n$$

and denote by $\mathcal{X}_n$ the set of solutions. We give some results concerning this equation in the next section.

Once we know that $\mathcal{X}_n\neq\emptyset$, this does not mean π has full eigenspaces. This problem and the way to study it is given next.

6.2. **Solving $X^2-tX+q\equiv 0 \bmod \ell^n$.** Equation (R_n) has solutions for all n if and only if $f(X)$ has roots in $\mathbb{Z}_\ell$.

Obviously, $\mathcal{X}_n\neq\emptyset$ if and only if the discriminant $\Delta=t^2-4q$ is a square modulo ℓ^n.

Lemma 6.1. *Let us write $\Delta=\ell^a\delta$ where $\ell\nmid\delta$.*

If $n\leq a$, the square roots of Δ are 0 and the $\ell^m\delta$ for $n/2\leq m<n$ and $1\leq\delta<\ell$.

If $n>a$, Δ is a square modulo ℓ^n if and only if a is even and Δ/ℓ^a is a square modulo ℓ^{n-a} and equivalently a square modulo ℓ. In that case, let ρ be any squareroot modulo ℓ^{n-a}; the other (non distinct) roots are $\ell^{a/2}(\pm\rho+s\ell^{n-a})$ for $0\leq s<\ell^a$.

For any particular instance of (t,q), one may build a tree in the following way. Level 0 is the root. Level 1 contains all solutions to (R_1). Then, any level $i\geq 2$ contains the roots of (R_i) that are built from roots at level $i-1$. We draw an arrow from a node N at level $i-1$ to a node N' at level i if and only if $N'\equiv N \bmod \ell^{i-1}$. This tree may be finite or infinite, and have one or more infinite path(s). The infinite paths correspond to the existence of ℓ-adic roots to the equation.

Examples. Take $(t, q) = (-2, 1009)$ and $\ell = 3$. Then the tree is simply that of Figure 3. We have $\Delta = 3^2 \times (-448)$ and -448 is not a square modulo 3.

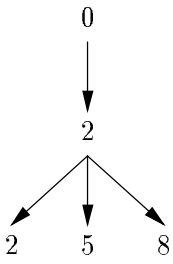


FIGURE 3. Tree associated with $X^2 + 2X + 1009 \bmod 3^n$

As for $(t, q) = (34, 1009)$ and $\ell = 3$, the first five levels are given in Figure 4. Note that the equation $X^2 - 34X + 1009 = 0$ has two distinct solutions in $\mathbb{Z}_3$. The discriminant Δ of this equation is $3^2 \times (-320)$. We have $-320 \equiv 1^2 \bmod 3$. Write $-320 = 1 + 3u$. Then a 3-adic root of Δ is given by the development of

$$3(1 + 3u)^{1/2} = 3\frac{9}{2}u - \frac{27}{8}u^2 + O(u^3).$$

We deduce from this the two 3-adic roots of $X^2 - 34X + 1009 = 0$: they are respectively congruent to 14 and 20 modulo 3^4.

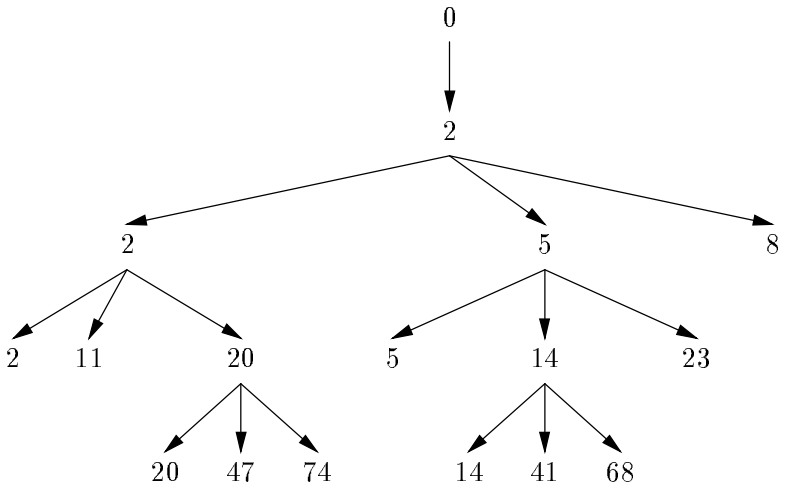


FIGURE 4. Tree associated with $X^2 - 34X + 1009 \bmod 3^n$

In the case $\ell = 2$, one can refine some of the results. We summarize the results for small n below.

Proposition 6.1. *Equation (R_1) has solutions modulo 2 if and only if $t \equiv 0 \bmod 2$ and in this case $\mathcal{X}_1 = \{1\}$. Equation (R_2) has solutions if and only if $t \equiv q + 1 \bmod 4$, in which case $\mathcal{X}_2 = \{1, 3\}$.*

For $n = 3$, one gets

t	q	$\mathcal{X}_3$	t	q	$\mathcal{X}_3$
0	$\{1,3,5\}$	$\emptyset$	4	$\{1,5,7\}$	$\emptyset$
	7	$\{1,3,5,7\}$		3	$\{1,3,5,7\}$
2	$\{3,7\}$	$\emptyset$	6	$\{3,5\}$	$\emptyset$
	1	$\{1,5\}$		1	$\{3,7\}$
	5	$\{3,7\}$		5	$\{1,5\}$

We have also an interesting criterion.

Proposition 6.2. *Assume $n \geq 3$. If $t \equiv 0 \bmod 4$ and x_n is a solution of (R_n), then there exists $\xi \in \{0,1\}$ such that $x_n + 2^{n-1}\xi$ is a solution of (R_{n+1}).*

Proof: We write:

$$f(x_n + 2^{n-1}\xi) \equiv f(x_n) + 2^{n-1}\xi(2x_n - t) \bmod 2^{n+1}$$

or

$$0 \equiv K + \xi(x_n - t/2) \bmod 2.$$

But since (R_n) has a solution, $x_n \equiv 1 \bmod 2$ and the result follows since $t/2$ is supposed to be even. □

6.3. **Testing for eigenspaces.** A pathological case is detected because $t^2 - 4q$ is zero modulo ℓ, which in turn is equivalent to the fact that the modular equation $\Psi_\ell(X, j(E))$ has splitting (1ℓ) or $(11\ldots1)$.

Selecting one of the roots, F_1, we construct E_1 and the following step is to find the roots of $\Psi = \Psi_\ell(X, j(E_1))/(X - W_\ell(F_1))$. It is easy to see that, by Galois theory, Ψ has either 0 or ℓ roots modulo p. In the first case, we cannot do anything more. In the second case, we select a root of this polynomial and go on. In some cases, this root does not work and we have to try another one. In this way, we build a tree which is very similar to the congruence tree described above. We can build this tree using a backtracking procedure, which is quite simple and that we do not want to describe.

Note that for our purposes, we are happy with one long path in the tree and not all the tree.

Example. We take $E = [1,4]$ and $\mathbb{F}_{1009}$. The splitting of $\Phi_3^c(X, j(E))$ is (13) and we compute the tree of Figure 5. Using this, we find that $t \equiv 34 \bmod 3^4$. As a matter of fact, $t = 34$ and this tree corresponds to the congruence tree of Figure 4.

We note the following. Suppose we stop at level $n = 2$. Then, to each solution of $X^2 - 34X + 1009 \equiv 0 \bmod 3^2$ corresponds a factor of degree 3 of f_9/f_3:

2	$X^3 + 916X^2 + 671X + 477$
5	$X^3 + 997X^2 + 522X + 804$
8	$X^3 + 377X^2 + 940X + 618.$

Remarks.

1. Notice that the fact that π has no $\mathbb{F}_\ell$-eigenspace does not imply that $f_{\ell^n}(X)$ has no factor of degree $\ell^{n-1}(\ell-1)/2$. For instance, for $E = [1,3]$ modulo $p = 1009$, one has

$$\frac{f_9}{f_3} \equiv 3\,\left(X^3 + 10\,X^2 + 379\,X + 217\right)\left(X^3 + 490\,X^2 + 274\,X + 713\right)$$
$$\times\left(X^3 + 302\,X^2 + 839\,X + 401\right) P_1 P_2 P_3 \bmod p$$

where P_i has degree 3^2. More generally, $f_{3^n}/f_{3^{n-1}}$ has 3^{n-1} factors of degree 3^{n-1} and 3^{n-1} factors of degree 3^n.

2. Suppose now that we cannot compute E_{11} from E_1. Then it is not useful to try to find ${}_1E$, since it isomorphic to E_1 and we would gain nothing.

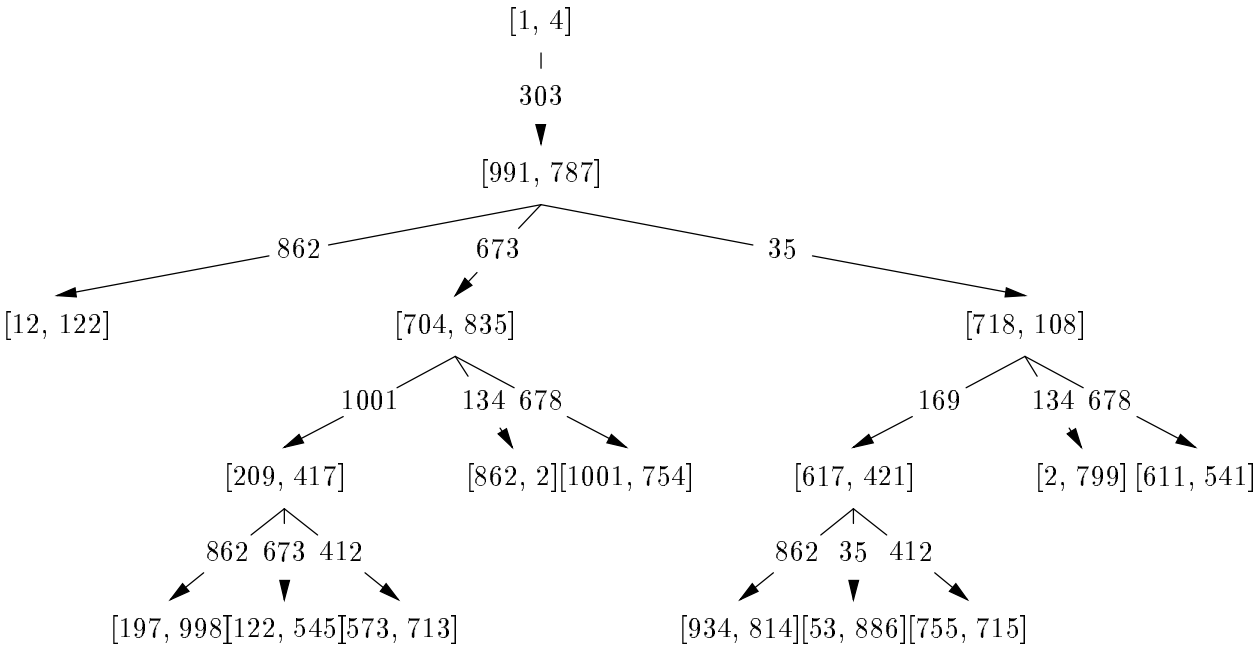


FIGURE 5. Tree associated to $E = [1, 4]$, $p = 1009$, $\ell = 3$.

6.4. **The case $\ell = 2$.** We assume $2 \nmid q$. The case $\ell = 2$ is always pathological, since when $\Phi_2^c(X, Y)$ splits, it has either 0, 1 or 3 root(s) in $\mathbb{F}_q$. What we have said before, including the backtrack approach, is still valid. However, some different results can be stated.

We note the important result.

Theorem 6.1. *Assume q odd and $n \geq 2$. If π has an eigenvalue modulo 2^n, then $f_{2^n}^E(X)$ has a factor of degree 2^{n-2}.*

Proof: We note first that if π has an eigenvalue modulo 2^n, then $t \equiv q + 1 \bmod 4$ by Proposition 6.1. Therefore E has a point of order 4 and f_4 a linear factor. The result follows by composition of isogenies. □

The computation of the isogeny is very explicit here, using Vélu's formulas [27].

Proposition 6.3. *Assume that $E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$ has a rational point of order 2, noted $P = (x_0, 0)$. Let G be the group generated by P. Let $t = 3x_0^2 + 2a_2x_0 + a_4$ and $w = x_0t$. Then an equation of E/G is $E_1 : Y_1^2 = X_1^3 + A_2X_1^2 + A_4X_1 + A_6$ where $A_2 = a_2$, $A_4 = a_4 - 5t$, $A_6 = a_6 - 4a_2t - 7w$. Moreover, the abscissa of the isogeny $I_1 : E \to E_1$ is given by*

$$X_1 = I_1(X) = X + \frac{t}{x - x_0}.$$

We can deduce the value of x_0 from that of F using the following idea.

Proposition 6.4. *Let j be the invariant of E, and F be a root of $\Phi_2^c(X, j) = 0$. Assume first $p = 3$ and $E : Y^2 = X^3 + a_2X^2 + a_6$. Rewrite this in the form $Y^2 = X^3 - cjX^2 + c^3j^2$, using $c = -a_2/j$. Then the abscissa of the point of 2-division is*

$$x_0 = c\frac{(F + 1)^2}{F}.$$

(Note that we cannot have $F = 0$.) Suppose $p > 3$ and $j \neq 1728$. Write the equation of $E : Y^2 = X^3 + a_4X + a_6$ in the form

$$Y^2 = X^3 + \frac{3c^2j}{1728 - j}X + \frac{2c^3j}{1728 - j}$$

with $c = 3a_4/(2a_6)$. The abscissa of a point of 2 torsion is

$$x_0 = -c\frac{F + 16}{F - 8}.$$

Proof: the results follow from elementary resultant computations. □

Example. Let $p = 101$, $E_0 = [77, 69]$. One finds that Φ_2^c factors as

$$\Phi_2^c(X, 22) = (X^2 + 80X + 74)(X + 69) \bmod 101$$

and thus $F_1 = 32$. One finds $E_1 = [58, 34]$, $J_1 = 98$ and the isogeny is

$$I_1 = \frac{X^2 + 4X + 24}{X + 4}$$

and $X + 4$ is indeed a factor of $X^3 + 77X + 69$. We compute

$$\Phi_2^c(X, 98) = (X + 74)(X + 98)(X + 78) \bmod 101.$$

We discard $X = 27 = 2^{12}/F_1$ as usual and we have to choose between 3 and 23. It turns out that we must take $F_{11} = 23$, thus obtaining $E_{11} = [42, 43]$ and

$$I_{11} = \frac{X^2 + 50X + 84}{X + 50}.$$

Now, we compute the numerator of $I_1 + 50$ and find it is $(X + 27)^2$ and $X + 27$ is indeed a factor of $f_4^{E_0}$. After that, $F_{111} = 54$, $E_{111} = [85, 11]$ and a factor of $f_4^{E_1}$ is $X + 86$ so that a factor of $f_8^{E_0}$ is $X^2 + 90X + 65$.

In some other cases, we have to do more computations, as shown by the following example. Take $E = [1, 3]$ modulo $p = 1009$. In Figure 6, we give the tallest subtree of the tree of curves.

As a matter of fact, we cannot go deeper than 6 levels. This means we can compute $t \bmod 2^7$, but not $t \bmod 2^8$, which is coherent with the fact that $t = -50$ and that $X^2 + 50X + 1009 \bmod 2^n$ has no roots for $n \geq 8$ (for the solution of such an equation, see for example [25, II, th. 4.]).

7. Remarks and conclusions

We have shown how to use small prime powers in Schoof's algorithms. The use of small prime powers has proven very useful for the practicality of algorithm SEA. This raises interesting questions concerning isogeny cycles. Our approach works also for the new approach used by the first author for extending Atkin's ideas to small characteristic [7, 16, 9]. This is certainly the case for the first algorithm we gave and when the characteristic is different from 2 and 3. It remains to find the formulas for the Atkin-Lehner involution used in the other two algorithms.

References

[1] A. O. L. Atkin. Schoof's algorithm. Draft, 1986.

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

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

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

[5] J. Buchmann and V. Müller. Computing the number of points of elliptic curves over finite fields. In *ISSAC '91* (1991), S. M. Watt, Ed., pp. 179–182. Proceedings of the International Symposium on Symbolic and Algebraic Computation, July 15–17, Bonn, Germany.

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

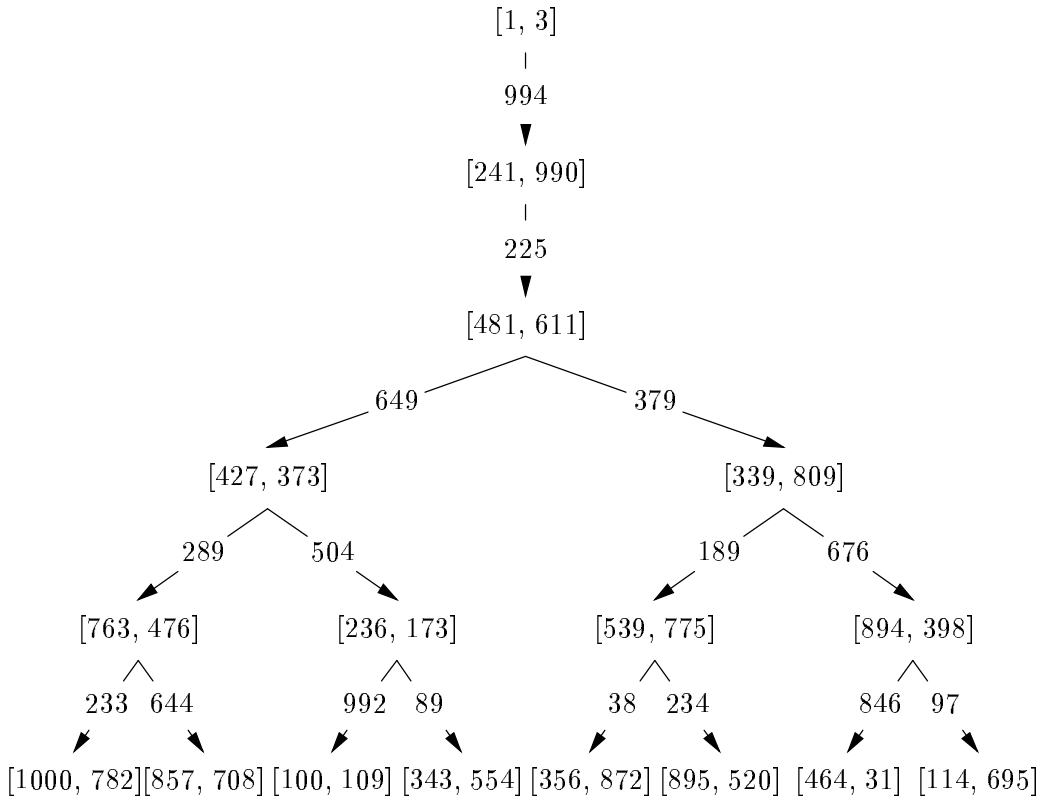


FIGURE 6. Tree associated to $E = [1, 3]$, $p = 1009$, $\ell = 2$.

[7] J.-M. COUVEIGNES. *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, July 1994.
[8] J.-M. COUVEIGNES. Computing isogenies in any characteristic. In preparation, 1995.
[9] J.-M. COUVEIGNES. Computing l-isogenies with the p-torsion. To appear in the Proc. of ANTS-II, Jan. 1996.
[10] J.-M. COUVEIGNES AND F. MORAIN. 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.
[11] L. DEWAGHE. Un corollaire aux formules de Vélu. Preprint, Dec. 1995.
[12] L. DEWAGHE. Remarks on the Schoof-Elkies-Atkin algorithm. Preprint, Jan. 1996.
[13] N. D. ELKIES. Explicit isogenies. Draft, 1991.
[14] H. GUNJI. The Hasse invariant and p-division points of an elliptic curve. *Arch. Math. 27*, 2 (1976), 148–158.
[15] D. HUSEMÖLLER. *Elliptic curves*, vol. 111 of *Graduate Texts in Mathematics*. Springer, 1987.
[16] R. LERCIER. Computing isogenies in characteristic 2. To appear in the Proc. of ANTS-II, available on `http://lix.polytechnique.fr/~lercier/`, Dec. 1995.
[17] R. LERCIER AND F. MORAIN. Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm. Research Report LIX/RR/95/09, École Polytechnique–LIX, Sept. 1995. An improved version is being submitted.
[18] R. LERCIER AND F. MORAIN. Counting the number of points on elliptic curves over finite fields: strategies and performances. In *Advances in Cryptology – EUROCRYPT '95* (1995), L. C. Guillou and J.-J. Quisquater, Eds., vol. 921 of *Lecture Notes in Comput. Sci.*, pp. 79–94. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.
[19] J.-F. MESTRE. La méthode des graphes. Exemples et applications. In *Proc. of the International Conference on class numbers and fundamental units of algebraic number fields* (Nagoya, 1986), Nagoya Univ., pp. 217–242. Katata (Japan).
[20] F. MORAIN. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux 7* (1995), 255–282.
[21] V. MÜLLER. Looking for the eigenvalue in Schoof's algorithm. In preparation, Oct. 1994.

[22] V. Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei.* PhD thesis, Technischen Fakultät der Universität des Saarlandes, 1995.
[23] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp. 44* (1985), 483–494.
[24] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux 7* (1995), 219–254.
[25] J. P. Serre. *Cours d'arithmétique*. PUF, 1970.
[26] H. M. Stark. Class-numbers of complex quadratic fields. In *Modular functions of one variable I* (1973), W. Kuyk, Ed., vol. 320 of *Lecture Notes in Math.*, Springer Verlag, pp. 155–174. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.
[27] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math. 273* (July 1971), 238–241. Série A.

(J.-M. Couveignes) Univ. of Utrecht, Budapestlaan 6, 3508 TA UTRECHT, The Netherlands
E-mail address, J.-M. Couveignes: couveign@math.ruu.nl

(L. Dewaghe) UFR de mathématiques;Université de Lille I., 59655 Villeneuve d'Ascq cedex, France
E-mail address, L. Dewaghe: dewaghe@gat.univ-lille1.fr

(F. Morain) Laboratoire d'Informatique, École Polytechnique, F-91128 Palaiseau Cedex, France
E-mail address, F. Morain: morain@polytechnique.fr