Schoof's algorithm and isogeny cycles

Jean-Marc Couveignes[1] and François Morain[2]

[1] U. M. R. d'Algorithmique Arithmétique
Université de Bordeaux, 351 Cours de la Libération, F-33400 Talence, France
& GRECC, D.M.I., E.N.S., 45 rue d'Ulm, F-75230 Paris Cedex 05, France
[2] Laboratoire d'Informatique, École Polytechnique
F-91128 Palaiseau Cedex, France

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. A new structure appears, called "isogeny cycle". We investigate some properties of this structure.

1 Introduction

Let E be an elliptic curve over a primitive finite field $\mathbb{F}_p$ where p is a large prime integer. (We are not dealing with the case of small characteristic here.) The curve is given by some equation $\mathcal{E}(X,Y) = 0$ in Weierstrass form

$$\mathcal{E}(X,Y) = Y^2 - X^3 - AX - B$$

so that a generic point on the curve is given by $(X,Y) \,\mathbf{mod}\, \mathcal{E}$. Let m be the number of points of E. It is well known that $m = p + 1 - t$, with t an integer satisfying $|t| < 2\sqrt{p}$. If p is small the problem of computing the cardinality of E is easy: one can simply enumerate all the points on E. When p is moderately large, say $p \approx 10^{30}$ (see [5]), one can use Shanks's baby-steps giant-steps method. When p is larger, say p up to 10^{200}, one must use Schoof's algorithm, or more precisely the improvements of Atkin and Elkies to the basic scheme.

As a matter of fact, Schoof's algorithm computes $t \bmod \ell$ for sufficiently many small primes ℓ, performing arithmetic modulo polynomials of degree $(\ell^2 - 1)/2$. The basic algorithm can be extended to the case of prime powers ℓ^n as well. In Elkies's improvements, a prime ℓ can be either good or bad. When ℓ is good, one can compute $t \bmod \ell$ more rapidly than in Schoof's basic approach, performing arithmetic modulo polynomials of degree $(\ell - 1)/2$. Moreover, one can in this case compute $t \bmod \ell^n$ pretty much as in Schoof's case. However, one can do better in this case. The purpose of this paper is to explain how one can compute $t \bmod \ell^n$ within the same time complexity as the original $t \bmod \ell$, in the case of good primes. For this, 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 an algorithm that enables one to compute $t \bmod \ell^n$. We note that our method has some common points with that of [10], but in a different context.

From a historical point of view, we note that Atkin gave some improvements to Schoof's algorithm as early as 1986 [1], coming up with the match and sort approach in 1988 [2]. In 1989, Elkies [8], 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's scheme and made it very practical, his record (March 1994) being computing the cardinality of $E_I : Y^2 = X^3 + 105X + 78153$ modulo $10^{275} + 693$. Morain has also recently implemented the algorithm and obtained similar results using a distributed implementation [12]; his record (December 1993) is the computation of the cardinality of $E_X : Y^2 = X^3 + 4589X + 91128$ modulo $10^{249} + 1291$. We give a table explaining this record at the end of the paper. Recently, Schoof has written an account of the relevant theory in [14]. Some algorithmic details are given in [11].

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

2.1 The basic scheme

We refer to [13]. Let ℓ be some small prime number. For theoretical reasons we need that $\ell < p$. (In practice, p is around 10^{200} while ℓ is always smaller than 500.)

We recall that if π denotes the Frobenius action on the curve, π induces an automorphism of the ℓ-torsion space $E[\ell]$ which extends to Tate's module $T_\ell(E)$. The ring of endomorphisms of the curve contains $\mathbb{Z}[\pi]$ and π satisfies the following degree 2 equation

$$\pi^2 - t\pi + p = 0,$$

where t is related to the cardinality of the curve by

$$\#E = p + 1 - t.$$

Of course, the same equality 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 recurrence formulae. Then, a non zero ℓ-torsion point on E is given by

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

so that, for any $\lambda \,\mathbf{mod}\, \ell$ a residue modulo ℓ, one can test whether the trace of π is λ by checking the following identity, written in homogeneous coordinates:

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

For some λ the above equality will hold thus giving $t \,\mathbf{mod}\, \ell$. If one does the same computation for enough primes ℓ_i (i.e., such that $\prod_i \ell_i > 4\sqrt{p}$), 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 $(\ell^2-1)/2$. In practice one cannot hope to compute $t \bmod \ell$ for $\ell > 31$.

2.2 Elkies's ideas

The whole theoretical background for this section can be found in [9], particularly chapters 12 and 13.

The center of Elkies's ideas [8] is that if $\mathrm{disc}(\pi) = t^2 - 4p$ is a non-zero square modulo ℓ (the zero case works as well but in a slightly different way) then π has two rational distinct eigenvalues τ_1 and τ_2 in $\mathbb{F}_p$ and even in $\mathbb{Z}_p$. Then, Tate's module decomposes as a sum of the two corresponding rational eigensubspaces

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

and the ℓ-torsion as well. Such a prime ℓ is called good, and bad in the other case.

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

$$E \xrightarrow{I_u} E_u \ , 1 \le u \le \ell + 1$$

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 subspaces 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. Namely, the ℓ-torsion polynomial will have two (non necessarily irreducible) factors h_1 and h_2 of degree $(\ell-1)/2$, each corresponding to a eigenvalue. We have two isogeneous curves E_i, for $i = 1, 2$, given by some equations $\mathcal{E}_i(X, Y) = 0$ where

$$\mathcal{E}_i(X, Y) = Y^2 - X^3 - A_i X - B_i$$

together with two isogenies $I_1 : E \longrightarrow E_1$ and $I_2 : E \longrightarrow E_2$, with kernel $T_1^E \cap E[\ell]$ and $T_2^E \cap E[\ell]$. And for $P = (X, Y) \,\mathbf{mod}\, \mathcal{E}$ a point on E,

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

for $i = 1, 2$.

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.

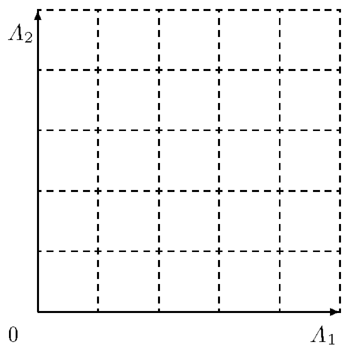

Fig. 1. The 5-torsion structure

A non zero point in $T_1^E \cap E[\ell]$ is given by $(X, Y) \,\mathbf{mod}\, (\mathcal{E}(X, Y), h_1(X))$, 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

$$X^{(\ell^d-1)/2} \,\mathbf{mod}\, f_\ell^E$$

for some integer d. Nevertheless, the coefficients of h_1 and h_2 are modular functions over $\Gamma_0(\ell)$ and thus can be computed from analytic evaluation in $\mathbb{C}$. Indeed, one considers their Fourier expansion at infinity to find out some modular equation of degree $\ell + 1$. The coefficients of those equations being integers can be reduced modulo p. The existence of some rational eigenvalues to the Frobenius implies the existence of some roots in $\mathbb{F}_p$ to the modular equations. In fact, we have even better, since the modulo p decomposition type of such modular equations gives the permutation type of π seen as a permutation of $\mathbb{P}_1(\mathbb{F}_p)$ thus providing some knowledge about the (non necessarily rational) eigenvalues: the multiplicative order of their quotient. This is the original remark of Atkin. One gets conditions over the residues modulo ℓ_i of the cardinality and then tries to glue up all this knowledge thanks to a sieving process. Note that this is heavier but it works all the time, even if all the small primes we choose are bad.

Note that the whole method splits in two steps:

- Look for some rational root modulo p of the degree $\ell+1$ modular equations, and build h_1 from it if there is some. Otherwise factor the modular equation completely and deduce the (several) possible values of $t \,\mathbf{mod}\, \ell$ (bad case).
- If you have found some h_1, compute $(X^p, Y^p) \,\mathbf{mod}\, (\mathcal{E}, h_1)$ and then, look for some $\tau \,\mathbf{mod}\, \ell$ such that $(X^p, Y^p) = [\tau](X, Y) \,\mathbf{mod}\, (\mathcal{E}, h_1(X))$ which gives the actual value of $t \,\mathbf{mod}\, \ell$ (good case).

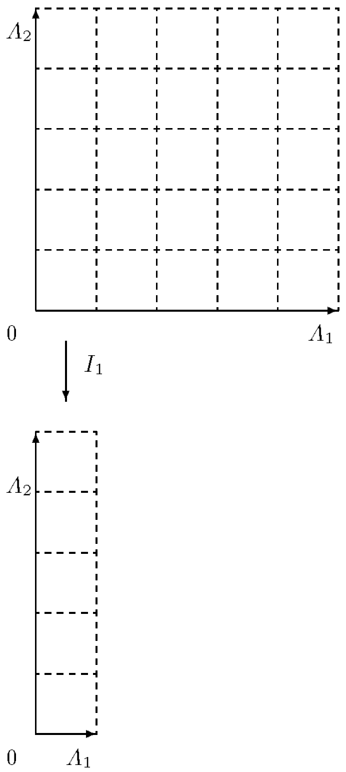

Fig. 2. Isogenies for $\ell = 5$

Note that in both steps we are dealing with polynomials of degree $\ell + 1$ and $(\ell - 1)/2$ which is much smaller than $(\ell^2 - 1)/2$.

Remark: We are not very explicit here about which equation to use. One may think about using the classical modular equation (or rather its quotient by Atkin-Lehner's involution). In this case, the solutions to those equations stand for the isogeneous curves and *not* for the isogenies themselves. It may be that there are two isogenies with distinct kernel and of the same degree, going to the same isogeneous curve. In this case, the endomorphism ring of E must have a non-integer element of norm ℓ^2, which is rather unlikely. Anyway, we can then use another modular equation, such as those given in [6].

2.3 Computing $h_1(X)$

Over $\mathbb{C}$. Let ℓ be a fixed odd prime. Suppose first 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 equation of E is $Y^2 = X^3 + AX + B$. 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 $k \geq 3$:

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

The ℓ-th division polynomial is then simply

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

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, and in particular $W_\ell(j(\tau)) = j(-1/\ell\tau) = j(\ell\tau)$.

In Atkin's approach, one first determines a modular equation for $X_0(\ell)$, that is to say an algebraic relation

$$\Phi_\ell(X, Y) = 0$$

which relates a function $F(q)$ on $\Gamma_0(\ell)$ and the modular invariant $j(q)$ (with $q = \exp(2i\pi\tau)$). One knows that

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

where the C_r's have integer coefficients and $C_{\ell+1}(Y) = 1$. Starting from

$$\Phi_\ell(X, j(\tau)) = 0$$

one can compute $F(\tau)$ and then all quantities p_1, A_1 and B_1 can be deduced from this in an algebraic way.

Remark. 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 $\Phi_\ell(W_\ell(F_1), Y) = \Phi_\ell(\ell^s/F_1, Y)$, 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 $\Phi_\ell(W_\ell(F_1), Y) = \Phi_\ell(F_1, Y)$.

Over $\mathbb{F}_p$. Now, modulo p, if ℓ is a good prime, then $\Phi_\ell(X, j(E)) \equiv 0 \,\mathbf{mod}\, p$ has (in general) two distinct roots and we can use the previous algebraic relations modulo p and deduce from this an isogeneous curve E_1 and the polynomial $h_1(X)$ which is the desired factor of $f_\ell^E(X)$ modulo p.

3 Walking along the rational cycles of isogeneous 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 isogeneous curves, the eigenvalues of the Frobenius are the same. Since the eigenspaces T_1^E and T_2^E are independent, I_1 induces a bijection between T_2^E and the corresponding eigensubspace on E_1 and reciprocally I_2 induces a bijection between T_2^E and the corresponding eigensubspace on E_2.

The existence of two distincts 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. We call I_{11} and I_{12} those isogenies and E_{11} and E_{12} the image curves. 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^* either equals I_{11} either equals I_{12}. By consideration of the restriction to T_1^E we see that

$$I_1^* = I_{12}.$$

We could express that by saying that the two rational directions are not only independent but dual.

We show all that on Figure 1.

Now, if E is a curve over $\mathbb{F}_p$ such that $t^2 - 4p$ is a non zero square mod ℓ we can build two periodic sequences of isogeneous curves over $\mathbb{F}_p$. These sequences define two permutations $\mathcal{I}_1$ and $\mathcal{I}_2$ on the set of elliptic curves over $\mathbb{F}_p$, classified up to $\mathbb{F}_p$-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.

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

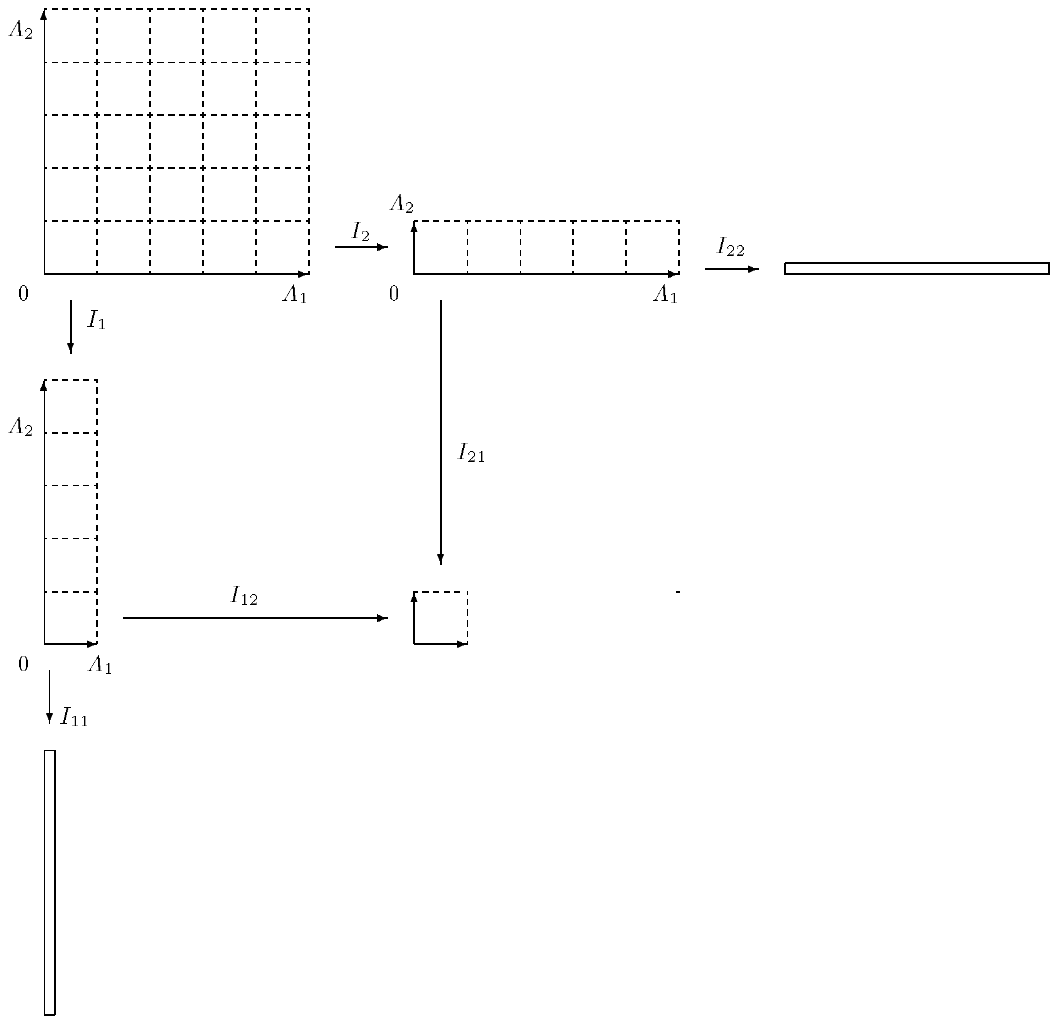

Fig. 3. Action of the isogenies

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

These series are computed in the following way. We use some modular equation $\Phi_\ell(X, Y)$. Let's call j_0 the invariant of E and let's solve $\Phi_\ell(X, j_0) = 0$ over $\mathbb{F}_p$. 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's now solve the equation $\Phi_\ell(X, j_1) = 0$ over $\mathbb{F}_p$. We find two rational distinct simple roots, one of them being $W_\ell(F_1)$ and corresponding 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 $\Phi_\ell(X, j_{11}) = 0$, etc.

Since the field is finite, the two series 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 have $(p+1) - \#E = t = 3$. 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].

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 $F_1 = 37$ and corresponds to $\tau_2 = 4$.

3.3 Application to Schoof's algorithm

For example, 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. We then note that $T_1^E \cap E[\ell^2] = I_1^{-1}(T_1^{E_1} \cap E_1[\ell])$ so that the factor we are looking for is obtained by plugging I_1 into h_{11}. And so on ...

In this way one can compute factors of degree $\ell^{k-1}(\ell-1)/2$ to 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 Implementation

4.1 Computing h_1 and I_1

The way Atkin's approach works, one first solves $\Phi_\ell(X, j_0) \equiv 0 \,\mathbf{mod}\, p$ for a root F_1 and then one computes j_1 as a root of

$$\Phi_\ell(W_\ell(F_1), Y) \equiv 0 \,\mathbf{mod}\, p.$$

Each solution y yields a putative factor $h_y(X)$ of $f_\ell^E(X)$. We check this factor by checking that $[\ell](X, Y) = 0 \,\mathbf{mod}\, (\mathcal{E}(X, Y), h_y(X))$. Once we know a proper factor h_1 of f_ℓ^E, we proceed to find I_1. We know that

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

where $k_1(X)$ is a polynomial of degree ℓ with coefficients in $\mathbb{F}_p$. 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.

4.2 Examples

Let us work out an example. Let's take $E : Y^2 = X^3 + 2X + 3 \,\mathbf{mod}\, 97$. 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

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

One computes $j_0 = j(E) = 36$ and $\Phi_5(X, 36)$ factors 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

$$\Phi_5(5^3/F_1, Y) \,\mathbf{mod}\, p$$

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

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

A factor of $f_{25}^E(X)$ is then the numerator of $h_1(I_1(X))$ namely

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

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

$$\Phi_5(X, j_1) \equiv (X + 61)(X + 5)(X^4 + 61X^3 + 58X^2 + 13X + 2) \equiv 0 \,\mathbf{mod}\, p.$$

We note that a solution to this is $W_\ell(F_1) = \ell^3/F_1 \equiv 36 \bmod p$. 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

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

4.3 An improved strategy

It is easy to see that the algorithm works also if we replace h_1 by a factor of h_1. In that case, a factor of degree d of $f_\ell^{E_1}$ can be lifted to a factor of degree $d\ell$ of $f_{\ell^2}^E$. A good strategy for using the isogeny idea is given in the following algorithm. We suppose that E is given modulo p and ℓ is an odd prime.

1. find the roots of $\Phi_\ell(X, j(E))$;
2. if Φ_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) find the order d_i of τ_i modulo ℓ; if d_i is even, divide by 2; [d_i is now the smallest field $\mathbb{F}_{p^{d_i}}$ containing abscissa of points of ℓ-division]
   (d) let $d = \min(d_1, d_2)$ and τ the associated eigenvalue; [d is now the degree of a factor of f_ℓ^E of minimal degree, see [3]]
   (e) if d is small enough, then factor the factor associated with d and compute $t \bmod \ell^n$ for small n using arithmetic modulo a polynomial $h_{\ell^n}(X)$ of degree $d\ell^{n-1}$, using the fact that the eigenvalue k is congruent to τ modulo ℓ.

4.4 Experimental results

The second author has implemented the Schoof-Elkies-Atkin algorithm in C, using the `BigNum` package. The details of this implementation will be described in a forthcoming article [12].

His latest record (March 1994) concerns the curve:

$$E_X : Y^2 = X^3 + 4589 * X + 91128$$

modulo $p = 10^249 + 1291$. Its cardinality is $m = p + 1 - t$ where t is

812863330901169485115745076523086320636188340265983567
838360703200862059524324760065812460397083331158180143539300866556 1929.

It took 1027 CPU hours on several DecAlpha's to perform the job, 641 of which were needed for the computation of various $X^p \bmod f(X)$. We give in Table 1 the ℓ-primes used, together with a code, which says that ℓ was an **A**tkin prime, an **E**lkies prime of a **S**choof prime (a Schoof prime is a small Atkin prime for which the original algorithm could be used). If ℓ is an Elkies prime, the third column contains the values $(t \bmod \ell^n, k_1, o_1, k_2, o_2)$ where k_1 and k_2 are the eigenvalues and o_1 and o_2 their respective orders. If ℓ is an Atkin prime, then we put the ratio of the possible number of t modulo ℓ versus $\ell - 1$. (See [3] for the importance of that quantity.) More details will be given in [12].

5 The case $\ell = 2$

5.1 The equation $X^2 - tX + p \equiv 0 \bmod 2^n$

Let us first consider the set of solutions $\mathcal{X}_n$ of the equation

$$(R_n) \quad X^2 - tX + p \equiv 0 \bmod 2^n \tag{1}$$

with p odd. The following tables give the solutions of this equation for small n.

Lemma 1. *Equation* (R_1) *has solutions modulo* 2 *if and only if* $t \equiv 0 \bmod 2$ *and in this case* $\mathcal{X}_1 = \{1\}$.

Lemma 2. *Equation* (R_2) *has solutions if and only if* $t \equiv p + 1 \bmod 4$, *in which case* $\mathcal{X}_2 = \{1, 3\}$.

As is customary, one wants to compute the solutions of (R_{n+1}) starting from (R_n). Let x_n be a solution of (R_n) and put

$$t_n \equiv t \bmod 2^n, 0 \leq t_n < 2^n, \quad p_n \equiv p \bmod 2^n, 0 \leq p_n < 2^n.$$

We look for a solution $x_{n+1} = x_n + \xi 2^n$, $\xi \in \{0, 1\}$. The following result is immediate.

ℓ^n	type		ℓ^n	type		ℓ^n	type	
2^5	E	(9)	89	A	0.27	211	A	0.50
3^3	S	(26)	97	A	0.44	223	A	0.03
5^2	S	(4)	101	E	$(75, 66, 100, 9, 50)$	227	E	$(201, 160, 113, 41, 226)$
7	S	(0)	103	A	0.02	233	A	0.31
11^3	E	$(730, 1, 1, 3, 5)$	107	A	0.17	239	E	$(120, 46, 238, 74, 238)$
13	S	(8)	109	E	$(47, 9, 27, 38, 9)$	257	E	$(231, 196, 128, 35, 64)$
17^3	E	$(707, 11, 16, 16, 2)$	113	E	$(93, 27, 112, 66, 112)$	269	E	$(256, 76, 268, 180, 67)$
19	S	(9)	127	E	$(38, 119, 14, 46, 126)$	281	E	$(92, 42, 280, 50, 35)$
23	S	(12)	131	A	0.15	283	E	$(53, 123, 282, 213, 282)$
29^2	E	$(91, 24, 7, 9, 14)$	137	E	$(6, 110, 136, 33, 136)$	293	E	$(211, 81, 73, 130, 292)$
31^2	E	$(104, 29, 10, 13, 30)$	139	E	$(45, 7, 69, 38, 69)$	311	E	$(117, 51, 62, 66, 310)$
37	A	0.50	149	A	0.27	317	E	$(112, 308, 79, 121, 79)$
41	A	0.30	151	A	0.48	331	E	$(175, 19, 165, 156, 165)$
43^2	E	$(375, 11, 7, 20, 42)$	157	E	$(17, 71, 39, 103, 52)$	347	E	$(267, 56, 173, 211, 346)$
47	E	$(38, 8, 23, 30, 46)$	163	E	$(35, 155, 27, 43, 81)$	353	E	$(335, 303, 176, 32, 88)$
53	E	$(4, 18, 52, 39, 52)$	167	E	$(73, 30, 166, 43, 166)$	373	E	$(325, 266, 186, 59, 186)$
59	E	$(23, 3, 29, 20, 29)$	173	E	$(152, 56, 86, 96, 43)$	379	E	$(364, 333, 189, 31, 378)$
61	A	0.50	179	E	$(2, 64, 89, 117, 89)$	383	E	$(349, 308, 382, 41, 382)$
67	E	$(14, 40, 11, 41, 66)$	181	A	0.40	431	E	$(56, 171, 215, 316, 430)$
71	E	$(40, 4, 35, 36, 35)$	191	A	0.17	439	E	$(24, 200, 219, 263, 438)$
73	A	0.50	193	A	0.50	443	E	$(338, 72, 442, 266, 442)$
79^2	E	$(2660, 55, 3, 77, 78)$	197	A	0.03	449	E	$(333, 384, 448, 398, 112)$
83	A	0.15	199	A	0.40			

Table 1. Data for E_X mod $10^{249} + 1291$

Proposition 3. *Let $n \geq 1$. Write*

$$p_{n+1} = p_n + \pi 2^n, \pi \in \{0, 1\}, \quad t_{n+1} = t_n + \tau 2^n, \tau \in \{0, 1\}$$

and $x_n^2 - t_n x_n + p_n = K 2^n$. Then x_{n+1} is a solution of (R_{n+1}) (for any choice of ξ) if and only if

$$K + \pi + \tau \equiv 0 \bmod 2.$$

For example, one obtains the following result for $n = 3$ starting from the solutions corresponding to $n = 2$.

Lemma 4. *For $n = 3$, one gets*

t	p	$\mathcal{X}_3$	t	p	$\mathcal{X}_3$
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	$\{1, 5\}$

It is clear from the result that if (R_n) has a solution, this does not imply that (R_{n+1}) does. In some cases, one can do better.

Proposition 5. *Assume $n \geq 3$. If $t_n \equiv 0 \bmod 4$ 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. Writing $x_{n+1} = x_n + 2^{n-1}\xi$ and with the notations as above, one finds that $K + (1 - t_n/2)\xi + \rho + \tau$ should be 0 modulo 2, which always yields a solution in ξ if $t_n/2 \equiv 0 \bmod 2$. □

5.2 Computing I_1 and h_1

We first note the important result.

Theorem 6. *If $X^2 - tX + p \equiv 0 \bmod 2^n$ has a solution, then $f^E_{2^n}(X)$ has a factor of degree 2^{n-2}.*

The methods described by Atkin enables 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 [15] using continued fractions and thus h_1.

The results of the preceding section has important consequences for our purpose. As a matter of fact, using Atkin's approach, one has to find the roots of $\Phi_2(X, J_1)$ which is of degree 3, so has 1 or 3 roots. Since $X = 2^{12}/F_1$ is already a root, this leaves us with 0 or 2 roots for F_{11}.If there are two roots, we can proceed to find E_{11}, but we are not sure which one it is, and sometimes we have to backtrack. When there are no more roots for a certain depth, this means that $X^2 - tX + p \bmod 2^n$ has no roots for this n. This implies new restrictions on t. We will give examples next.

5.3 Example

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

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

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

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

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 in the following. Take $E = [1, 3]$ modulo $p = 1009$. One finds that

$$\Phi_2^c(X, 269) \equiv (X - 484)(X - 994)(X - 492) \bmod p.$$

In what follows, we list the depth of the search, followed by the value of F. Here is the beginning of it

$$0(484), 1(198), 2(--), 1(446), 2(--), 0(492), 1(483), 2(--), 1(281), 2(--),$$

$$0(994), 1(225), 2(649), 3(289), 4(644), 5(--), 4(233), 5(--), \ldots$$

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 $n \geq 8$.

The above example shows that the implementation of this part of the algorithm is rather tricky: we first find the longest path in our tree, then compute the isogenies and then the division polynomials. We also use the informations we have gathered to perform the final computations.

6 Conclusions

We have shown how to use small prime powers in Schoof's algorithms. This raises interesting questions concerning isogeny cycles. Our approach should also work for the new approach used by the first author for extending Atkin's ideas to small characteristic [7].

Also, we never considered the degenerate cases where the modular equation has only one root modulo p, or splits completely modulo p. These cases can also be treated, in some cases as in the $\ell = 2$ case. We will describe this somewhere else.

Acknowledgments. The first author is a member of the "Option Recherche du Corps des Ingénieurs de l'Armement; the second author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

References

1. A. O. L. Atkin. Schoof's algorithm. Preprint, 1986.
2. A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Preprint, 1988.
3. A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (ii). Preprint, 1992.
4. A. O. L. Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–67, July 1993.

5. Johannes Buchmann and Volker Müller. Computing the number of points of elliptic curves over finite fields. In S. M. Watt, editor, *ISSAC '91*, pages 179–182, 1991. Proceedings of the International Symposium on Symbolic and Algebraic Computation, July 15–17, Bonn, Germany.
6. Leonard S. Charlap, Raymond Coley, and David P. Robbins. Enumeration of rational points on elliptic curves over finite fields. Draft, 1991.
7. Jean-Marc Couveignes. Thesis. Manuscript, 1994.
8. Noam D. Elkies. Explicit isogenies. Manuscript, 1991.
9. D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer, 1987.
10. 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*, pages 217–242, Nagoya, 1986. Nagoya Univ. Katata (Japan).
11. François Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. Submitted for publication of the Actes des Journées Arithmétiques 1993, March 1994.
12. François Morain. Implantation de l'algorithme de Schoof-Elkies-Atkin. Preprint, January, 1994.
13. R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.
14. René Schoof. Counting points on elliptic curves over finite fields. Submitted for publication of the Actes des Journées Arithmétiques 1993, March 1994.
15. H. M. Stark. Class-numbers of complex quadratic fields. In W. Kuyk, editor, *Modular functions of one variable I*, volume 320 of *Lect. Notes in Math.*, pages 155–174. Springer Verlag, 1973. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.