

## REMARKS ON THE SCHOOF-ELKIES-ATKIN ALGORITHM

L. DEWAGHE

**ABSTRACT.** Schoof's algorithm computes the number  $m$  of points on an elliptic curve  $E$  defined over a finite field  $\mathbb{F}_q$ . Schoof determines  $m$  modulo small primes  $\ell$  using the characteristic equation of the Frobenius of  $E$  and polynomials of degree  $O(\ell^2)$ . With the works of Elkies and Atkin, we have just to compute, when  $\ell$  is a "good" prime, an eigenvalue of the Frobenius using polynomials of degree  $O(\ell)$ . In this article, we compute the complexity of Müller's algorithm, which is the best known method for determining one eigenvalue and we improve the final step in some cases. Finally, when  $\ell$  is "bad", we describe how to have polynomials of small degree and how to perform computations, in Schoof's algorithm, on  $x$ -values only.

### 1. INTRODUCTION

Let  $E$  be an elliptic curve defined over the finite field  $\mathbb{F}_q$  of large characteristic  $p$ . The set of  $\mathbb{F}_q$ -points of  $E$ , denoted  $E(\mathbb{F}_q)$ , is a finite abelian group [20].

In 1985, Schoof [17] gave a deterministic polynomial-time algorithm for computing  $\#E(\mathbb{F}_q)$ . The algorithm determines the characteristic equation of the Frobenius  $\pi$  of  $E$ , acting on the  $\ell$ -torsion points  $E[\ell]$  of  $E$ , for  $\ell$  prime. But, working on  $E[\ell]$  uses computations on polynomials modulo the  $\ell$ -th division polynomial  $f_\ell$ , and this is not practical, due to the size of  $f_\ell$ .

In 1991, Elkies [10] showed how to perform computations in the kernel of an isogeny of degree  $\ell$ , by computing a factor of degree  $d = (\ell - 1)/2$  of  $f_\ell$ . This idea works for nearly half the primes  $\ell$ , called *Elkies primes*. For such an  $\ell$ , the algorithm has just to compute an eigenvalue of  $\pi$  acting on  $E[\ell]$ .

Atkin [1] had given in 1988 the *sort and match* method used now for "bad" primes  $\ell$ . Then he made the algorithm practical for very large finite fields [2] and the method became the SEA (for Schoof-Elkies-Atkin) algorithm.

For the last improvements in this scope, see [5], [6] and [12] and for the case  $p$  small, see [7] and the implementation in [13].

In this article we compute, for an Elkies prime  $\ell$ , the complexity of the best asymptotic method used for computing an eigenvalue of  $\pi$  over  $E[\ell]$  and we show then how to avoid, in some cases, the computation with  $y$ -coordinates of points. Finally, for a bad prime  $\ell$ , we explain how to obtain a proper factor of  $f_\ell$  and show then how to avoid again, in Schoof's algorithm, computations with  $y$ -coordinates of points.

---

Received by the editor May 11, 1996 and, in revised form, October 2, 1996 and February 19, 1997.

1991 *Mathematics Subject Classification.* Primary 14H52, 14K02, 11Y16.

*Key words and phrases.* Elliptic curves, finite fields, Schoof algorithm, division polynomials, computational number theory.

These results have enabled Morain [15] to compute  $\#E(\mathbb{F}_p)$ , for  $p$  prime of 500 digits (this is the actual record).

## 2. THE SEA ALGORITHM

**2.1. Elliptic curve over  $\mathbb{F}_q$ .** Let  $E$  be a non-supersingular elliptic curve given by an affine equation  $\mathcal{F}(x, y) = 0$  where

$$\mathcal{F}(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

with the  $a_i$ 's in  $\mathbb{F}_q$ .

The set  $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q, \mathcal{F}(x, y) = 0\} \cup \{O_E\}$  is an abelian group and the law, denoted  $\oplus$ , has  $O_E = [0 : 1 : 0]$  as neutral element. We denote by  $f_n$  the  $n$ -th division polynomial in  $x$ . The degree of  $f_n$  is  $(n^2 - 1)/2$  if  $n$  is odd. The group of  $n$ -torsion points,  $E[n] = \{P \in E(\mathbb{F}_q) \mid nP = O_E\}$  can be represented by  $\mathbb{F}_q[x, y]/(f_n(x), \mathcal{F}(x, y))$  (see [18]).

The morphism  $\pi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$ ,  $(x, y) \mapsto (x^q, y^q)$  of  $E$  satisfies  $\pi^2 - t\pi + q = 0$  over  $E(\mathbb{F}_q)$ , with  $t \in \mathbb{Z}$ , satisfying  $|t| \leq 2\sqrt{q}$ . Recall :  $\#E(\mathbb{F}_q) = q + 1 - t$ . When  $\ell$  is an odd prime number (see [6] for  $\ell = 2$ ), we consider the restriction  $\pi_\ell$  of  $\pi$  to  $E[\ell]$ , which satisfies  $\pi_\ell^2 - \tau\pi_\ell + k = 0$  over  $E[\ell]$  with  $t \equiv \tau \pmod{\ell}$  and  $q \equiv k \pmod{\ell}$ . Now, if  $\ell \neq p$ ,  $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ , so we can view  $E[\ell]$  as a vector space over  $\mathbb{F}_\ell$  and  $x^2 - \tau x + k$  as the characteristic equation of  $\pi_\ell$ . We denote by  $G_1, G_2, \dots, G_{\ell+1}$  the  $(\ell + 1)$  cyclic subgroups of  $E(\mathbb{F}_q)$ , of order  $\ell$ .

**2.2. The SEA algorithm.** Schoof [17] determines  $\#E(\mathbb{F}_q) = q + 1 - t$  by searching for a match among the  $\ell$  equations  $(x^{q^2}, y^{q^2}) \oplus k(x, y) = \tilde{\tau}(x^q, y^q)$ ,  $0 \leq \tilde{\tau} \leq \ell - 1$ , over  $E[\ell]$ .

Elkies works in the kernel  $G_i$  of one of the  $\ell + 1$  isogenies  $E \xrightarrow{\ell_i} E_i$ ,  $1 \leq i \leq \ell + 1$ , of degree  $\ell$ . When  $D = \tau^2 - 4k$  is a square modulo  $\ell$  the eigenvalues of  $\pi_\ell$  are in  $\mathbb{F}_\ell$  and  $\ell$  is called an Elkies prime. Hence, in this case, the eigenspaces are  $\mathbb{F}_q$ -rational and the corresponding isogenies are defined over  $\mathbb{F}_q$  and if we let  $E[\ell]_\lambda$  be an eigenspace with  $P_\lambda$  a generator, we have  $h_\ell(x) = \prod_{i=1}^d (x - x(iP_\lambda)) \in \mathbb{F}_q[x]$  and

$$E[\ell]_\lambda = \langle P_\lambda \rangle = \mathbb{F}_q[x, y]/(h_\ell(x), \mathcal{F}(x, y)).$$

Let  $\Phi_\ell(x, y) = 0$  be the canonical equation of the modular curve  $X_0(\ell)$  (see [2], [15] for a simpler equation). We know that  $\ell$  is an Elkies prime if and only if  $\Phi_\ell(j(E), x) = 0$  has a root in  $\mathbb{F}_q$ .

For  $p \neq 2, 3$  and  $\ell$  an Elkies prime, the formulas of Atkin [2], [15] give, from a root of  $\Phi_\ell(j(E), x) = 0$  in  $\mathbb{F}_q$ , the value of  $p_1 = \sum_{i=1}^d x(iP_\lambda)$  and the coefficients of the corresponding  $E_i$ . So [10], one can compute the  $p_k = \sum_{i=1}^d x^k(iP_\lambda)$  for  $1 \leq k \leq d$  and hence  $h_\ell$  by Newton's formula if  $\ell \ll p$ .

If  $p = 2$  or  $3$  or  $\ell \approx p$  see Couveignes' work [7] and also [13].

Once  $h_\ell$  is known, we have to search a match among the  $\ell - 1$  equations  $(x^q, y^q) = \tilde{\lambda}(x, y)$ ,  $1 \leq \tilde{\lambda} \leq \ell - 1$ , over  $E[\ell]_\lambda$ .

If  $D$  is not a square modulo  $\ell$ , then  $\ell$  is called an *Atkin prime* and the  $G_i$ 's are  $\mathbb{F}_{p^e}$ -rational where  $e$  is the smallest integer  $n$  for which  $\pi_\ell^n$  is in  $\mathbb{F}_\ell$ .

## 3. LOOKING FOR ONE EIGENVALUE

**3.1. Computing  $\lambda \pmod{\ell}$ .** We compute the complexity of the algorithm of Müller [16] which computes  $\lambda \pmod{\ell}$ . Müller uses an integer  $k_{opt} \approx \lceil \sqrt{d} \rceil$  such that for all

$\lambda$  in  $\mathbb{F}_\ell^*$ , there are integers  $i, j$  with  $1 \leq i, j \leq k_{opt}$  such that  $\lambda \equiv \pm i/j \pmod{\ell}$ . So, he compares  $j(x^q, y^q)$  and  $i(x, y)$  using division polynomials, which means comparisons of rational functions.

The elementary operation is taken to be the cost of one multiplication of two elements in  $\mathbb{F}_q$ . Let  $M(d)$  be the number of operations needed to compute the multiplication of two polynomials of degree  $d$  (see [11]).

**Proposition 1.** *Müller's method takes  $O(M(d) \log q) + O(\sqrt{d}M(d)) + O(d^2)$  operations and  $O(d\sqrt{d})$  space.*

*Proof.* The computation of  $x^q \bmod h_\ell(x)$  requires  $O(M(d) \log q)$  operations and the computation of the  $k_{opt}$  first division polynomials requires  $O(\sqrt{d}M(d))$  operations.

The  $x(j(x^q, y^q))$  are computed using the recursive formulae of division polynomials in  $x^q$  (see [8]). This requires  $O(\sqrt{d}M(d))$  operations, which is more efficient than modular compositions  $x(j(x, y)) \circ x^q$  (see [4], [19]).

To compare two rational functions modulo  $h_\ell(x)$  in  $\mathbb{F}_q[x]$ , one can test the match using a random linear map [16] and then verify polynomial equality. So, the comparisons of coordinates takes  $O(2M(d)) + O(2d^2)$  operations.  $\square$

**3.2. The sign of  $\lambda \bmod \ell$ .** Suppose we have integers  $i, j$  such that  $j\pi_\ell = \pm i$  over  $E[\ell]_\lambda$ , where  $\ell$  is an Elkies prime. We have  $\lambda \equiv \pm \lambda_0 \pmod{\ell}$  with  $\lambda_0 \equiv ij^{-1} \pmod{\ell}$ . For  $\mu \in \mathbb{F}_{\ell^2}^*$ , we call *semi-order* of  $\mu$ , denoted  $s(\mu)$ , the order of  $\mu$  in  $\mathbb{F}_{\ell^2}^*/(\pm 1)$ .

- If  $p \neq 2$ ,  $E$  has an equation of the form  $y^2 = \mathcal{G}(x) := x^3 + a_2x^2 + a_4x + a_6$ .

**Theorem 1.** *Let  $h_\ell$  be the factor of  $f_\ell$  corresponding to  $\lambda$  and  $g_\ell$  be a factor of degree  $s(\lambda_0)$  of  $h_\ell$  and let  $r$  be  $\text{Resultant}(g_\ell, \mathcal{G})$ . Then  $\lambda = \lambda_0^{s(\lambda_0)}(\frac{r}{q})\lambda_0$ . When  $\ell \equiv 3 \pmod{4}$ , one can take  $g_\ell = h_\ell$ .*

*Proof.* For  $s(\lambda_0)$  odd, we have  $\pi_\ell^{s(\lambda_0)} = \pm \lambda_0^{s(\lambda_0)} Id$  over  $E[\ell]_\lambda$ . If  $\pi_\ell^{s(\lambda_0)} = Id$ , then  $E[\ell]_\lambda \subset E(\mathbb{F}_{q^{s(\lambda_0)}})$ ; hence, for all  $P$  in  $E[\ell]_\lambda$ ,  $\mathcal{G}(x(P))$  is a square in  $\mathbb{F}_{q^{s(\lambda_0)}}$ , and since  $\prod_{i=1}^{s(\lambda_0)} (\mathcal{G}(x_i)) = r$ , with  $x_i$  the roots of  $g_\ell$ ,  $r$  is a square in  $\mathbb{F}_q$ . Whereas, if  $\pi_\ell^{s(\lambda_0)} = -Id$  over  $E[\ell]_\lambda$ , then  $(\frac{r}{q}) = -1$ .  $\square$

Note that, if  $\ell \equiv 1 \pmod{4}$ , then one can compute  $\lambda_0$  using  $h_\ell$  and then determine  $\lambda$ , if  $s(\lambda_0) = s(\pm \lambda_0)$  is odd, using a factor of  $h_\ell$ .

- If  $p = 2$ , let  $y^2 + xy = x^3 + B$  (with  $B \in \mathbb{F}_{2^m}$ ) be an equation of  $E$  (see [14]).

**Proposition 2.** *Let  $h_\ell$  be a factor of  $f_\ell$  corresponding to  $\lambda = \pm \lambda_0$ . If  $h_\ell$  has a factor  $g_\ell = x^{s(\lambda_0)} - \tilde{s}_1 x^{s(\lambda_0)-1} + \dots + (-1)^{s(\lambda_0)} \tilde{s}_{s(\lambda_0)}$  of odd degree  $s(\lambda_0)$ , then*

$$\lambda = \begin{cases} \lambda_0^{s(\lambda_0)} \lambda_0 & \text{if } \text{Tr}(\tilde{s}_1 + B(\tilde{s}_{s(\lambda_0)-1}^2 - 2\tilde{s}_{s(\lambda_0)}\tilde{s}_{s(\lambda_0)-2})/\tilde{s}_{s(\lambda_0)}^2) = 0, \\ -\lambda_0^{s(\lambda_0)} \lambda_0, & \text{otherwise.} \end{cases}$$

When  $\ell \equiv 3 \pmod{4}$ , one can take  $g_\ell = h_\ell$ .

*Proof.* The equation  $X^2 + X = \gamma$  has a root in an extension  $\mathbb{F}_{2^n}$  if and only if  $\text{Tr}(\gamma) = 0$  (see [9]). Hence the points of  $E[\ell]_\lambda = \langle P = (x, y) \rangle$  are in  $\mathbb{F}_{q^{s(\lambda_0)}}$  if and only if  $\text{Tr}(\gamma_i) = 0$ , where  $x_i = x(iP)$  and  $\gamma_i = x_i + B/x_i^2$ . Finally, computing  $\sum_{i=1}^{s(\lambda_0)} \text{Tr}(\gamma_i)$  gives the desired result.  $\square$

## 4. ELKIES' METHOD FOR ATKIN PRIMES

**4.1. Computing a factor of  $f_\ell$ .** Assume that  $q = p$  prime,  $\neq 2, 3$  and that  $\ell$  is an Atkin prime with  $\ell \ll p$ .

The  $(\ell + 1)$  curves  $E_i$  are defined over  $\mathbb{F}_{p^e}$ , hence  $f_\ell$  has a factor of degree  $d$  over  $\mathbb{F}_{p^e}$  and so by conjugation we can find a factor of degree  $ed$  over  $\mathbb{F}_p$ .

First, we compute a monic irreducible factor  $M_\ell(x)$  of degree  $e$  of  $\Phi_\ell(j(E), x)$  in  $\mathbb{F}_p[x]$ . We denote by  $x_i$ ,  $i = 1, 2, \dots, e$ , the roots of  $M_\ell(x) = 0$  in  $\mathbb{F}_{p^e}$ . Then, in  $\mathbb{F}_p[x]/M_\ell(x)$ , we determine  $ed$  polynomials  $p_k(x) = \sum_{j=0}^{e-1} a_{j,k}x^j$  of degree  $e-1$ , (see [2], [10]) and since, for  $1 \leq k \leq ed$ , we have

$$p_k \stackrel{\text{def}}{=} \sum_{i=1}^e p_k(x_i) = \sum_{i=1}^e \left( \sum_{j=0}^{e-1} a_{j,k} x_i^j \right) = \sum_{j=0}^{e-1} a_{j,k} \left( \sum_{i=1}^e x_i^j \right) = \sum_{j=0}^{e-1} a_{j,k} \tilde{p}_j$$

with  $\tilde{p}_j = \sum_{i=1}^e x_i^j$  computed from the symmetric functions of  $M_\ell(x)$ , a factor of degree  $ed$  of  $f_\ell$  can be computed.

**Example.** We consider the elliptic curve  $y^2 = x^3 + 2x + 41$  over  $\mathbb{F}_{59}$  with  $j = 31$ . We determine a factor of the division polynomial  $f_5$  of  $E$ . Over  $\mathbb{F}_{59}$ ,  $x^3 + 41x^2 + 45x + 32$  is a factor of  $\Phi_5(x, 31)$ . We obtain

$p_1(x)$	$56x^2 + 31x + 41$	$p_4(x)$	$16x^2 + 11x + 6$
$p_2(x)$	$46x^2 + 22x + 26$	$p_5(x)$	$51x^2 + 41x + 17$
$p_3(x)$	$21x^2 + 20x + 39$	$p_6(x)$	$34x^2 + 41x$

And  $p_0 = 2$ ,  $p_1 = 38$ ,  $p_2 = 28$ ,  $p_3 = 22$ ,  $p_4 = 7$ ,  $p_5 = 38$ ,  $p_6 = 21$ , hence  $x^6 + 21x^5 + 13x^3 + 10x^2 + 3x + 55$  is a factor of  $f_5$  over  $\mathbb{F}_{59}$ .

**4.2. Computing  $t \bmod \ell$ .** We show how, when  $\ell$  is an Atkin prime, we can test the equation  $\pi_\ell^2 + k = \tilde{\tau}\pi_\ell$  in  $\tilde{\tau}$  by computing only  $x$ -coordinates of points. We recall first that if

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3) \quad \text{and} \quad (x_1, y_1) \ominus (x_2, y_2) = (x_4, y_4),$$

then we have

$$(x_3 + x_4)(x_1 - x_2)^2 = S(x_1, x_2) \quad \text{and} \quad x_3x_4(x_1 - x_2)^2 = P(x_1, x_2)$$

with

$$S(x_1, x_2) = (x_1 + x_2)(a_1a_3 + 2a_4 + 2x_1x_2) + x_1x_2(a_1^2 + 4a_2) + 4a_6 + a_3^2,$$

and

$$P(x_1, x_2) = (x_1x_2 - a_4)(x_1x_2 - a_4 - a_1a_3) - (x_1 + x_2 + a_2)(a_3^2 + 4a_6) - a_1^2a_6.$$

So the values  $x_3$  and  $x_4$  are solutions of the quadratic equation  $E(X) = NX^2 - SX + P$  with  $N(x_1, x_2) = (x_1 - x_2)^2$ .

Following Müller's idea, we introduce the integers  $i, j$  and  $k_{opt}$  with the equation  $i\pi_\ell^2 + ik = j\pi_\ell$ . We search a value  $j$  for which  $x(j\pi_\ell)$  is a root of  $E(X) = 0$  given by  $S(x_i^{q^2}, x_{ik})$ ,  $P(x_i^{q^2}, x_{ik})$  and  $N(x_i^{q^2}, x_{ik})$ .

Indeed, if  $x(i\pi_\ell^2 + ik) = x(j\pi_\ell)$ , then, for some  $\tau_0$ ,  $\pi_\ell^2 + k = \pm\tau_0\pi_\ell$  over  $E[\ell]$ , so  $\tau \equiv \pm\tau_0 \bmod \ell$ . Whereas, if  $x(i\pi_\ell^2 - ik) = x(j\pi_\ell)$ , then  $\pi_\ell^2 - k = \pm\tau_0\pi_\ell$  and  $\pi_\ell = 2k/(\tau \pm \tau_0)$ , which is impossible since  $\ell$  is an Atkin prime.

Hence, we avoid the computation of  $y^{q^2}$  and  $y^q$  and obtain  $t \equiv \pm\tau_0 \bmod \ell$ .

**4.3. The sign of  $t \bmod \ell$ .** Since  $\pi_\ell$  satisfies the equation  $x^2 - \tau x + k = 0$ , we have  $\pi_\ell^n = Q_n \pi_\ell + P_n$  with  $P_n$  and  $Q_n$  some polynomials in  $\tau$  and  $k$ . We have  $P_n = -kQ_{n-1}$  and moreover the polynomial  $Q_n$  contains only even powers of  $\tau$  if  $n$  is odd and only odd powers otherwise [3]. On the other hand,  $\pi_\ell^e = P_e$  and the value of  $e$  does not depend on the sign of  $\tau$ . Hence, when  $e$  is odd, we have  $P_e(\pm\tilde{\tau}, k) = \pm P_e(\tilde{\tau}, k)$ , so  $\pi_\ell^e = \pm P_e(\tau_0, k)$ . Let  $w_0$  be  $P_e(\tau_0, k)$ .

**Proposition 3.** *Assume  $p \neq 2$ ,  $e$  odd; let  $h_\ell$  be a factor of degree  $ed$  of  $f_\ell$ ,  $g_\ell$  be a factor of degree  $es(w_0)$  of  $h_\ell$  and  $r$  be  $\text{Resultant}(g_\ell, \mathcal{G})$ . Then, when  $s(w_0)$  is odd, we have  $t \equiv (\frac{r}{q})w_0^{s(w_0)}\tau_0 \bmod \ell$ . When  $\ell \equiv 3 \bmod 4$ , one can take  $g_\ell = h_\ell$ .*

*Proof.* We have  $\pi_\ell^e = \pm w_0 \text{Id}$  over  $E[\ell]$ ; hence, if  $s(w_0)$  is odd, then  $\pi_\ell^{es(w_0)} = \pm w_0^{s(w_0)} \text{Id}$  over  $E[\ell]$  and, if  $d$  is odd, then  $\pi_\ell^{ed} = \pm w_0^d \text{Id} = \pm (\frac{w_0}{\ell}) \text{Id}$  over  $E[\ell]$ .  $\square$

From  $\pi_\ell^2 = \tau_0 \pi_\ell + k$ , we easily compute  $w_0 = P_e(\tau_0, k)$ . The decomposition type of  $h_\ell$  is determined by computing  $s(w_0)$ .

**Example.** Let us consider the curve  $y^2 = x^3 + 4312x + 9167$  over  $\mathbb{F}_{12853}$ . If  $\ell = 19$ , then we have  $e = 5$  and using a factor  $h_{19}$  of degree 45 of  $f_{19}$  we obtain  $t \equiv \pm 7 \bmod 19$ . We compute  $r = \text{Resultant}(x^3 + 4312x + 9167, h_{19}) = 11226$ ; since  $(\frac{r}{p}) = 1$  and  $w_0 = P_5(7, 9) = 4$ , we have  $t \equiv 7 \bmod 19$ .

If  $\ell = 13$ , then  $e = 7$  and  $\tau_0 = 5$ . Since  $w_0 = P_7(5, 9) = 10$ , and  $s(10) = 3$ , the polynomial  $h_{13}$  has an irreducible factor  $g_{13}$  of degree 21. We obtain  $r = \text{Resultant}(x^3 + 4312x + 9167, g_{13}) = 9515$  and  $(\frac{r}{p}) = -1$ , so we have  $t \equiv 5 \bmod 13$ .

**Proposition 4.** *Let  $h_\ell$  be a factor of degree  $ed$  of  $f_\ell$ . If  $p = 2$  and  $e$  is odd, then, when  $s(w_0)$  is odd, we have*

$$\tau = \begin{cases} w_0^{s(w_0)}\tau_0 & \text{if } \text{Tr}(\tilde{s}_1 + B(\tilde{s}_{es(w_0)-1}^2 - 2\tilde{s}_{es(w_0)}\tilde{s}_{es(w_0)-2})/\tilde{s}_{es(w_0)}^2) = 0, \\ -w_0^{s(w_0)}\tau_0 & \text{otherwise,} \end{cases}$$

with  $\tilde{s}_i$  the symmetric functions of a factor  $g_\ell$  of  $h_\ell$  of degree  $es(w)$ . When  $\ell \equiv 3 \bmod 4$ , one can take  $g_\ell = h_\ell$ .

#### ACKNOWLEDGMENT

The author would like to thank François Morain for his help during the realization of this work.

#### REFERENCES

- [1] A. O. L. Atkin, *The number of points on an elliptic curve modulo a prime (I)*. Draft, 1988.
- [2] A. O. L. Atkin, *The number of points on an elliptic curve modulo a prime (II)*. Draft, 1992.
- [3] R. C. Bose, S. Chowla, C. R. Rao, *On the integral order (mod  $p$ ) of quadratics  $x^2 + ax + b$ , with applications to the construction of minimum functions over  $GF(p^2)$ , and to some number theory results*, Bull. Calcutta Math. Soc., 36 (1944), pp. 153–174. MR **6**:256b
- [4] R. P. Brent, H. T. Kung, *Fast algorithms for manipulating formal power series*, J. Assoc. Comput. Mach., **25**, 581–595, 1978. MR **58**:25090
- [5] J.-M. Couveignes, F. Morain, *Schoof's algorithm and isogeny cycles*, In L. Adleman and M.-D. Huang, editors, ANTS-I, volume 877 of Lecture Notes in Comput. Sci., pages 43–58. Springer-Verlag, 1994. MR **95m**:11147
- [6] J.-M. Couveignes, L. Dewaghe, F. Morain, *Isogeny cycles and Schoof's algorithm*, Preprint 1995.
- [7] J.-M. Couveignes, *Quelques calculs en théorie des nombres*, Thèse, Université de Bordeaux I, July 1994.

- [8] L. Dewaghe, *Nombre de points d'une courbe elliptique sur un corps fini*, Thèse, Université de Lille I, 1996.
- [9] R. J. McEliece, *Finite fields for computer scientists and engineers*, Kluwer Boston 1987. MR **88h**:11091
- [10] N. D. Elkies, *Explicit Isogenies*, Draft, 1991.
- [11] D. E. Knuth, *The Art of Computer Programming : Seminumerical Algorithms*, Addison-Wesley, 1981. MR **83i**:68003
- [12] R. Lercier and F. Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, In L. C. Guillou and J.-J. Quisquater, editors, *Advances in cryptography - EUROCRYPT'95*, number 921 of *Lecture Notes in Comput. Sci.* pp. 79-94, 1995. MR **96h**:11060
- [13] R. Lercier, F. Morain, *Counting points on elliptic curves over  $\mathbb{F}_p^n$  using Couveignes's algorithm*. Research Report LIX/RR/95/09, Ecole polytechnique - LIX, September 1995.
- [14] A. Menezes, S. Vanstone and R. Zuccherato, *Counting points on elliptic curves over  $\mathbb{F}_{2^m}$* , *Math. Comp.* 60, 407-420, 1993. MR **93f**:11098
- [15] 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. MR **97i**:11069
- [16] V. Müller, *Looking for the eigenvalue in Schoof's algorithm*, In preparation, October 1994.
- [17] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod  $p$* , *Math. Comp.* 44, 483-494, 1985. MR **86e**:11122
- [18] R. Schoof, *Counting points on elliptic curves over finite fields*, *J. Théor. Nombres Bordeaux* 7 (1995), 219-254. MR **97i**:11070
- [19] V. Shoup, *A new polynomial factorization algorithm and its implementation*, *J Symbolic Comput.* (1995) Vol 20, 363-397. MR **97d**:12011
- [20] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics*, Springer, 1986. MR **87g**:11070

UNIVERSITÉ DE LILLE I, UFR DE MATHÉMATIQUES, 59655 VILLENEUVE D'ASCQ CEDEX, FRANCE  
*E-mail address*: dewaghe@gat.univ-lille1.fr