Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 255–282*

Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques

par François MORAIN

Résumé. Nous décrivons dans cet article les algorithmes nécessaires à une implantation efficace de la méthode de Schoof pour le calcul du nombre de points sur une courbe elliptique dans un corps fini. Nous tentons d'unifier pour cela les idées d'Atkin et d'Elkies. En particulier, nous décrivons le calcul d'équations pour $X_0(\ell)$, ℓ premier, ainsi que le calcul efficace de facteurs des polynômes de division d'une courbe elliptique.

Abstract. We describe the algorithms that are needed for an efficient implementation of Schoof's method for computing the number of points on en elliptic curve over a finite field. We try to unify the ideas of Atkin and Elkies. In particular, we describe the computation of equations for $X_0(\ell)$, ℓ a prime number, as well as the efficient computation of factors of the division polynomials of an elliptic curve.

1. Introduction

Soit E une courbe elliptique définie sur un corps fini $K = \mathbb{F}_{p^n}$ de caractéristique p. Depuis le travail de Schoof [20], on sait qu'on peut calculer la cardinalité de $E(K)$ en temps polynomial en la taille du corps. Toutefois, il a fallu les améliorations d'Atkin et d'Elkies pour rendre l'algorithme praticable sur des corps de taille raisonnable, en caractéristique p grande. Ce n'est que tout récemment, grâce aux travaux de Couveignes [6], que l'algorithme fonctionne en petite caractéristique (voir aussi [14, 15] pour les recherches en cours concernant l'implantation efficace de ces idées).

Cet article complète l'article [21], en donnant les versions les plus optimisées de certains des algorithmes qui y sont donnés. Nous renvoyons le

1991 *Mathematics Subject Classification.* 11G20, 11F11.
Key words and phrases. Courbes elliptiques, corps finis, algorithme de Schoof, formes modulaires, équations modulaires, polynômes de division.
Manuscrit reçu le 4 octobre 1993.
Manuscrit reçu le 1er janvier 1995, dernière version le 27 juin 1995.
L'auteur est mis à disposition du LIX par la Délégation Générale pour l'Armement. Cette étude a été faite dans le cadre de la convention n°0044193 entre le CELAR et le LIX.

lecteur au même article pour comprendre les motivations de ces calculs. Nous tentons d'unifier dans cet article les travaux d'Atkin [1, 2] et d'Elkies [10] (voir aussi [4]).

L'algorithme de Schoof utilise de manière essentielle les polynômes de ℓ-division de la courbe E, pour ℓ premier. Ces polynômes, notés $f_\ell(X)$ sont de dégré élevé ($O(\ell^2)$), ce qui rend l'utilisation directe de l'algorithme problématique. La clef de la version pratique de l'algorithme de Schoof est l'utilisation des propriétés des courbes $X_0(\ell)$. Soit $\Phi_\ell(X,Y)$ une équation de $X_0(\ell)$ et $j(E)$ l'invariant de E. La factorisation du polynôme $\Phi_\ell(X, j(E))$ caractérise les sous-groupes cycliques de E et ainsi les degrés des facteurs du polynôme f_ℓ. Il existe des cas favorables pour lesquels f_ℓ a un facteur g_ℓ de degré $O(\ell)$, ce qui rend les calculs pratiquables. On trouve alors ce facteur g_ℓ en utilisant une méthode ingénieuse due à Atkin.

L'architecture de cet article est la suivante. La deuxième section concerne le calcul d'équations pour $X_0(\ell)$ et pour $X_0^*(\ell)$, le quotient de $X_0(\ell)$ par l'involution d'Atkin-Lehner. On décrit les algorithmes de calcul dus en partie à Atkin pour cela. La troisième section présente des algorithmes de calcul de facteur de polynômes de torsion en utilisant ces équations. Ensuite, on présente sous une forme condensée l'algorithme du calcul du nombre de points, appelé en abrégé SEA (Schoof–Elkies–Atkin). Les améliorations récentes de l'algorithme sont aussi évoquées. Nous nous concentrons sur le cas de corps premier de grande caractéristique, renvoyant à [6, 14, 15] pour les autres cas. Nous illustrons nos propos avec des exemples numériques représentatifs, tirés de notre propre implantation. Un exemple commenté est donné à la dernière section : il s'agit du calcul du nombre de points modulo un nombre premier de 500 chiffres décimaux.

2. Calcul d'équations modulaires

2.1. Rappels. Les résultats donnés ici sont classiques. On en trouvera les démonstrations dans [19] par exemple.

Dans tout ce qui suit, on note $\mathcal{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ le demi-plan de Poincaré. Pour $\tau \in \mathcal{H}$, on note $q = \exp(2i\pi\tau)$. Nous emploierons la même notation pour une fonction $f(q) = f(\tau)$ qui est en fait une fonction de q. On définit encore $\hat{\mathbb{C}}$ le compactifié de $\mathbb{C}$ et

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}.$$

On rappelle que l'invariant modulaire j admet un développement du type

$$j(\tau) = j(q) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n$$

où les c_n sont des entiers positifs. Ces coefficients peuvent se calculer par la méthode donnée dans [16], ou mieux encore en utilisant l'expression de $j(q)$ en fonction des fonctions de Weber et de la fonction η. De toute façon, ces calculs doivent être faits modulo de petits nombres premiers comme nous le verrons plus loin.

Soit ℓ un nombre premier. Le groupe

$$\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1, \ \ell \mid c \right\}$$

est un sous-groupe d'indice $\mu = \ell + 1$ dans Γ. Les classes de $\Gamma/\Gamma_0(\ell)$ sont engendrées par

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et les

$$\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$$

pour $0 \leq k < \ell$. On note $X_0(\ell)$ la surface de Riemann $\mathcal{H}^*/\Gamma_0(\ell)$, et $g(\ell)$ son genre.

Proposition 2.1. *On a*

$$g(\ell) = \begin{cases} 0 & \text{si } \ell = 2 \text{ ou } 3, \\ (\ell - 13)/12 & \text{si } \ell \equiv 1 \bmod 12, \\ (\ell - 5)/12 & \text{si } \ell \equiv 5 \bmod 12, \\ (\ell - 7)/12 & \text{si } \ell \equiv 7 \bmod 12, \\ (\ell + 1)/12 & \text{si } \ell \equiv 11 \bmod 12. \end{cases}$$

On définit l'involution d'Atkin-Lehner w_ℓ associée à la matrice

$$W_\ell = \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}.$$

Si $f(q)$ est une fonction modulaire, on notera $f^* = f|w_\ell = f \circ w_\ell$.

Une des propriétés intéressantes de w_ℓ est la suivante.

Proposition 2.2. *L'involution w_ℓ normalise $\Gamma_0(\ell)$, c'est-à-dire*

$$w_\ell \Gamma_0(\ell) w_\ell^{-1} = \Gamma_0(\ell).$$

Démonstration. Il suffit de remarquer que

$$\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & -c/\ell \\ -\ell b & a \end{pmatrix}.$$

□

L'involution w_ℓ transforme les classes de $\Gamma/\Gamma_0(\ell)$ par multiplication à gauche par W_ℓ en

$$\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}, \begin{pmatrix} 1 & k \\ \ell & 0 \end{pmatrix}.$$

Nous noterons ces matrices M_∞, M_0, ..., $M_{\ell-1}$.

PROPOSITION 2.3. *Soit h le nombre de classes de $\mathbb{Q}(\sqrt{-\ell})$. Le nombre de points fixes de w_ℓ est*

$$a(\ell) = \begin{cases} h & \text{si } \ell \equiv 1 \bmod 4, \\ 2h & \text{si } \ell \equiv 7 \bmod 8, \\ 4h & \text{si } \ell \equiv 3 \bmod 8. \end{cases}$$

On pose $X_0^*(\ell) = X_0(\ell)/w_\ell$.

THÉORÈME 2.1. *La courbe $X_0^*(\ell)$ est encore une surface de Riemann de genre*

$$g^*(\ell) = \frac{g(\ell)+1}{2} - \frac{a(\ell)}{4}.$$

COROLLAIRE 2.1. *On a $g^*(\ell) = 0$ pour $\ell \le 31$ ou $\ell \in \{41, 47, 59, 71\}$.*

2.2. Calcul d'équation modulaire "canonique" pour $X_0(\ell)$. Nous allons montrer comment calculer une équation pour $X_0(\ell)$, c'est-à-dire une équation polynomiale du type $\Phi(f(q), j(q)) = 0$ où f est une fonction sur $\Gamma_0(\ell)$.

Notons tout de suite qu'on pourrait se contenter d'utiliser le fait que $j^* = j(\ell\tau)$ est une fonction sur $X_0(\ell)$. L'équation liant j à j^*, notée encore $\Phi_\ell(F, J)$, a des coefficients énormes. Par exemple,

$$\begin{aligned} \Phi_3(F,J) \;=\;& F^4 + J^4 - F^3J^3 + 2232\,(F^3J^2 + F^2J^3) \\ & -1069956\,(F^3J + FJ^3) + 36864000\,(F^3 + J^3) \\ & +2587918086F^2J^2 + 8900222976000\,(F^2J + FJ^2) \\ & +452984832000000\,(F^2 + J^2) - 770845966336000000FJ \\ & +1855425871872000000000\,(F + J). \end{aligned}$$

Ces problèmes sont liés essentiellement au fait que la fonction j^* a un pôle d'ordre trop grand à l'infini. Tout le but de cette section est de montrer comment trouver des fonctions d'ordre plus petit, et ce de façon canonique.

Soit $\eta(q)$ la fonction de Dedekind

$$\eta(\tau) = \eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

On pose $s = 12/\mathrm{pgcd}(12, \ell - 1)$, $v = s(\ell - 1)/12$ et on choisit

$$f(\tau) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s} = \ell^s q^v + \sum_{n=v+1}^{\infty} a_n q^n.$$

PROPOSITION 2.4. *La fonction $f(\tau)$ est une fonction sur $\Gamma_0(\ell)$.*

On note $\Phi_\ell^c(F, J)$ l'équation polynomiale liant $f(q)$ à $j(q)$: pour tout q, $\Phi_\ell^c(f(q), j(q)) = 0$. Ce polynôme peut s'écrire

$$(F - f(\tau)) \prod_{k=0}^{\ell-1} (F - f(-1/(1 + k\tau)))$$

dont les coefficients sont des polynômes en $j(q)$.

2.2.1. Un premier algorithme. D'après la proposition 2.2, la fonction $f^* = \ell^s/f$ est encore une fonction sur $\Gamma_0(\ell)$. Le polynôme

$$P(Y, J) = (Y - \ell^s/f(\tau)) \prod_{k=0}^{\ell-1} (Y - f((\tau + k)/\ell))$$

a donc aussi comme coefficients des polynômes en $j(q)$. Par suite, on peut écrire :

$$s_r(\tau) = s_r(q) = \sum_{k=0}^{\ell-1} f((\tau + k)/\ell)^r$$

et

$$S_r(\tau) = S_r(q) = (\ell^s/f(\tau))^r + s_r(\tau).$$

Les S_r, comme les C_k sont des polynômes en J. Nous prouvons maintenant :

PROPOSITION 2.5. *Les fonctions s_r sont à coefficients dans $\mathbb{C}(q)$.*

Démonstration. On développe f^r en série :

$$f(q)^r = \sum_{n=rv}^{\infty} a(n, r) q^n.$$

Soit ζ une racine ℓ-ième de l'unité. On a

$$f((\tau + k)/\ell) = \sum_{n=v}^{\infty} a_n q^{n/\ell} \zeta^k.$$

On pose $w = q^{1/\ell}$. Par suite

$$s_r(q) = \sum_{k=0}^{\ell-1} \left(\sum_{n=vr}^{\infty} a(n, r) w^n \zeta^{kn} \right) = \sum_{n=vr}^{\infty} a(n, r) w^n \left(\sum_{k=0}^{\ell-1} \zeta^{kn} \right).$$

La somme à l'intérieur est nulle sauf quand $\ell \mid n$ auquel cas elle vaut ℓ. Par suite :

$$s_r(q) = \ell \sum_{\ell n \geq vr}^{\infty} a(\ell n, r) q^n.$$

$\square$

Posons

$$\prod_{k=0}^{\ell-1} (Y - f((\tau + k)/\ell)) = \sum_{r=0}^{\ell} c_r Y^r.$$

On déduit de ce qui précède :

COROLLAIRE 2.2. *Pour tout* r, *la valuation de* $s_r(q)$ *(resp.* $c_r(q)$*) est* $\lceil vr/\ell \rceil$.

COROLLAIRE 2.3. *Pour tout* r, $1 \leq r \leq \ell+1$, *on a* $\deg(C_r(J)) \leq v - \lceil rv/\ell \rceil$.

On trouve les coefficients de ces polynômes en comparant leurs développements en série avec ceux des puissances de $j(q)$. La connaissance des S_r pour $1 \leq r \leq \ell+1$ permet de reconstruire les coefficients $C_k(J)$ à l'aide des formules de Newton : avec $C_0(j) = 1$ on a

$$-rC_r(J) = \sum_{k=1}^{r} S_k C_{r-k}(J)$$

pour tout r compris entre 1 et $\ell + 1$.

Exemple. Prenons $\ell = 5$. Dans ce cas, on a $s = 3$, $v = 1$. On commence par calculer

$$\begin{aligned}
s_1 &= 196875\, q + 21493750\, q^2 + 864300000\, q^3 + O(q^4),\\
s_2 &= 40625000\, q + 40233984375\, q^2 + 8493675000000\, q^3 + O(q^4),\\
s_3 &= 1845703125\, q + 12030117187500\, q^2 + 9376364531250000\, q^3 + O(q^4),\\
s_4 &= 29296875000\, q + 1309990234375000\, q^2 + 3270692929687500000\, q^3 + O(q^4),\\
s_5 &= 152587890625\, q + 69695434570312500\, q^2\\
&\qquad + 529629196472167968750\, q^3 + O(q^4).
\end{aligned}$$

Ajoutant les puissances de $f^*(q)$, on obtient :

$$S_1(q) = q^{-1} - 6 + 196884q + 21493760q^2 + \cdots$$

ce qui conduit à $S_1(q) = j(q) - 750$. De même :

$$S_2(q) = q^{-2} - 12q^{-1} + 54 + 40624912q + 40233984276q^2 + \cdots$$

dans lequel on reconnait $S_2 = j(q)^2 - 1500j(q) + 168750$. On trouve encore

$$\begin{aligned}
S_3(q) &= j(q)^3 - 2250j(q)^2 + 1096875j(q) - 39843750,\\
S_4(q) &= j(q)^4 - 3000j(q)^3 + 2587500j(q)^2 - 587500000j(q) + 9433593750,\\
S_5(q) &= j(q)^5 - 3750j(q)^4 + 4640625j(q)^3 - 2105468750j(q)^2\\
&\qquad + 263964843750j(q) - 2233886718750,
\end{aligned}$$

et finalement

$$\begin{aligned} S_6(q) &= j(q)^6 - 4500j(q)^5 + 7256250j(q)^4 - 5015625000j(q)^3 \\ &\quad +1378740234375j(q)^2 - 105908203125000j(q) \\ &\quad +528991699218750. \end{aligned}$$

On utilise les formules de Newton et on trouve :

$$\begin{aligned} P(Y,J) &= Y^6 + (-J+750)Y^5 + 196875Y^4 + 20312500Y^3 \\ &\quad +615234375Y^2 + 7324218750Y + 30517578125. \end{aligned}$$

Faisant $Y = 5^3/X$, on trouve

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

2.2.2. Amélioration de l'algorithme. Une autre manière de procéder consiste à reconstituer les coefficients du polynôme

$$Q(Y,q) = \prod_{k=0}^{\ell-1} (Y - f((\tau+k)/\ell)) = \sum_{r=0}^{\ell} c_r(q) Y^r$$

à partir des fonctions s_r. Une fois cela fait, on calcule les coefficients de $P(Y,J)$ en développant l'expression $(Y - f^*(q))Q(Y,q)$. Cette façon de faire est très économe en mémoire et très efficace quand ℓ est grand. Le calcul des s_r se fait à partir du développement de $f(q)^r$, à l'ordre $\ell v + c$, et les séries qui en résultent ont v termes. Le calcul des c_r se fait encore sur des séries ayant v termes, et celui des C_r également.

Exemple. Reprenons le cas $\ell = 5$. Après avoir calculé les s_i comme précédemment, on obtient d'abord :

$$\begin{aligned} c_1 &= -196875\,q - 21493750\,q^2 - 864300000\,q^3 + O\left(q^4\right), \\ c_2 &= -20312500\,q - 737109375\,q^2 - 15255468750\,q^3 + O\left(q^4\right), \\ c_3 &= -615234375\,q - 11015625000\,q^2 - 135019531250\,q^3 + O\left(q^4\right), \\ c_4 &= -7324218750\,q - 74462890625\,q^2 - 563964843750\,q^3 + O\left(q^4\right), \\ c_5 &= -30517578125\,q - 183105468750\,q^2 - 823974609375\,q^3 + O\left(q^4\right). \end{aligned}$$

et on obtient

$$C_1 = c_1 - f^*(q) = -q^{-1} + 6 - 196884\,q - 21493760\,q^2 - 864299970\,q^3 + O\left(q^4\right)$$

dans lequel on reconnaît le début du développement de $-J + 750$.

2.2.3. Un cas plus simple : quand $X_0(\ell)$ est de genre 0. Quand $X_0(\ell)$ a genre 0, i.e., $\ell \in \{2, 3, 5, 7, 13\}$, on sait qu'il existe une équation du type

$$f(q)^{\ell+1} + \sum_{k=0}^{\ell} c_k f(q)^k - j(q)f(q) = 0.$$

On récrit cela comme

$$j(q)f(q) = f(q)^{\ell+1} + c_\ell f(q)^\ell + \cdots + c_0.$$

Faisant agir w_ℓ, on obtient :

$$j^*(q) = j(q^\ell) = (\ell^s/f(q))^\ell + c_\ell(\ell^s/f(q))^{\ell-1} + \cdots + c_1 + c_0 f(q)/\ell^s.$$

Il suffit de remplacer j^* et f par leurs développements en série pour retrouver les coefficients c_k.

2.3. Calcul d'équation pour $X_0^*(\ell)$. L'ordre des fonctions canoniques, v, augmente rapidement avec ℓ et cela conduit à stocker des polynômes de grand degré en J. Pour pallier cet inconvénient, on préfère travailler avec des fonctions sur $\Gamma_0^*(\ell) = \Gamma_0(\ell) \cup w_\ell \Gamma_0(\ell)$, dont $\Gamma_0(\ell)$ est un sous-groupe. Une telle fonction est encore une fonction sur $\Gamma_0(\ell)$. L'avantage, c'est qu'il est possible de travailler avec des fonctions d'ordre très petit par rapport à ℓ.

2.3.1. Calcul de fonction sur $\Gamma_0^*(\ell)$: la méthode d'Atkin. Pour certaines valeurs de ℓ, on trouve des fonctions particulières pour $\Gamma_0^*(\ell)$, par exemple dans [11]. La manière classique de procéder est de chercher des formes modulaires de même poids sur $\Gamma_0^*(\ell)$ et de les quotienter pour obtenir des fonctions. À titre d'exemple, donnons une fonction sur $X_0^*(11)$. On pose

$$\theta_{a,b,c}(q) = \sum_{m,n} q^{am^2+bmn+cn^2}.$$

Une fonction sur $X_0^*(11)$ est donnée par

$$\left(\frac{\theta_{1,1,3}(q)}{\eta(q)\eta(q^{11})}\right)^2 - 1 = q^{-1} + 5 + 17q + 46q^2 + 116q^3 + \cdots .$$

L'implantation des idées d'Elkies-Atkin nécessite la construction de fonctions sur $X_0^*(\ell)$ pour ℓ premier jusqu'à 1000. Il est alors souhaitable d'avoir un algorithme de génération de ces fonctions. Atkin a mis au point pour cela une méthode appelée “blanchiment”.

Calcul de l'équation supersingulière. On sait (cf. [22, p. 137]) qu'une courbe elliptique $E/\overline{\mathbb{F}}_\ell$ supersingulière est définie sur $\mathbb{F}_{\ell^2}$. On appelle $H_\ell(X)$ le polynôme de $\mathbb{F}_\ell[X]$ dont les racines sont les invariants des courbes supersingulières, et $H_\ell^*(X)$ le polynôme ne contenant que les facteurs quadratiques de $H_\ell(X)$.

Proposition 2.6. *Le degré de H_ℓ (resp. H_ℓ^*) est $g(\ell)$ (resp. $2g^*(\ell)$).*

Introduisons la fonction hypergéométrique

$$F(a,b;c;x) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n} \quad \frac{x^n}{n!}$$

où $(k)_n = k(k+1)\cdots(k+n-1)$ est la *factorielle montante.*

Théorème 2.2 (Atkin). *Si $\ell \equiv 1 \bmod 4$, on a*

$$F(1/12, 5/12; 1, 1728/J) \equiv G(1/J)G(1/J^\ell)G(1/J^{\ell^2})\cdots \bmod \ell$$

où G est un polynôme de degré $g(\ell)$. Si $\ell \equiv 3 \bmod 4$, on a

$$F(7/12, 11/12; 1, 1728/J) \equiv G(1/J)G(1/J^\ell)G(1/J^{\ell^2})\cdots \bmod \ell.$$

Dans les deux cas

$$H_\ell(X) = X^{g(\ell)}G(1/X).$$

On trouvera dans [3, p. 143–144] une table donnant les polynômes $H_\ell(X)$ pour $\ell \leq 307$.

Théorie. Pour ce qui suit, on pourra se reporter à [17] ou [7, Th. 6.9 pp. DeRa - 144]. Soit $f(q)$ une fonction sur $\Gamma_0^*(\ell)$ avec un pôle d'ordre m à l'infini avec un développement du type $kq^{-m} + \cdots$. Alors f est congrue à un polynôme en j modulo ℓ. Notons $P(j)$ ce polynôme. Soit $H(X)$ un facteur de $H_\ell^*(X)$. Alors

$$P(X) \equiv a(H) \bmod (H(X), \ell)$$

où $a(H) \in \mathbb{F}_\ell$. Autrement dit,

$$P(X)^\ell \equiv P(X) \bmod (H_\ell^*(X), \ell)$$

ou encore $P(X)$ est dans le noyau de la matrice de Berlekamp associée à $H_\ell^*(X)$.

Soit alors Q la matrice dont la k-ième colonne contient les coefficients de $X^{\ell(k-1)} \bmod (H_\ell^*(X), \ell)$ sur la base $(1, X, X^2, \dots)$. Soit $A_\ell(X)$ un polynôme du noyau de $Q - I$ de degré minimum. Une fonction $f(q)$ de plus petite valence sur $\Gamma_0^*(\ell)$ vérifie ainsi

$$f(q) \equiv A_\ell(J) = J^v + a_{v-1}J^{v-1} + \cdots + a_1 J \bmod \ell$$

et

$$f(q) = q^{-v} + \cdots .$$

Supposons maintenant que $(\ell+1)/24 > v$. On calcule

$$g(q) = f(q)\eta(q)\eta(q^\ell) \bmod \ell = q^{(\ell+1)/24}(q^{-v} + g_{-v+1}q^{-v+1} + \cdots + g_0 + \sum_{n \geq 1} g_n q^n)$$

en prenant pour les g_n les plus petits résidus modulo ℓ. La fonction g, regardée sur $\mathbb{Z}$, est une forme parabolique de poids 1 pour un certain caractère ε. D'après le théorème de Serre-Deligne [8, Th. 9.1], les coefficients de $g(q)$ vérifient :

$$|g_n| \leq d_\ell(n)$$

où $d_\ell(n)$ compte le nombre de diviseurs de n premiers avec ℓ. Donc, les coefficients de g trouvés modulo ℓ sont considérés être les coefficients de g dans $\mathbb{Z}$, du moins à l'ordre qui nous intéresse. Il est alors possible d'identifier g comme étant une combinaison linéaire de fonctions theta binaires tordues par certains caractères.

La fonction f cherchée est alors

$$f(q) = \frac{g(q) - c\eta(q)\eta(q^\ell)}{\eta(q)\eta(q^\ell)}$$

où c est une constante de $\mathbb{F}_\ell$, que l'on prend égale à g_0.

Remarque. Les seuls cas pour lesquels $\ell \leq 1000$ et $(\ell+1)/24 > v$ sont les suivants : $(\ell, v) \in \{(11,1),(17,1),(19,1),(37,2),(43,2),(67,3),(163,7)\}$. D'un point de vue pratique, on utilise l'équation canonique pour $\ell \leq 43$, et des fonctions *ad hoc* pour 67 et 163, obtenues par combinaison linéaire d'opérateurs de Hecke agissant sur une fonction theta bien choisie.

Exemple. Soit $\ell = 73$. On trouve :

$$H_{73}(X) = 7 + 39X + 38X^2 + 9X^3 + 68X^4 + 60X^5 + X^6$$

soit

$$(1) \quad H_{73}^*(X) = (X^2 + 57X + 8)(X^2 + 68X + 9) \\ \equiv X^4 + 52X^3 + 24X^2 + 35X + 72 \bmod 73.$$

On calcule la matrice Q dont la k-ième colonne contient les coefficients de $X^{73(k-1)} \bmod (H_{73}^*, 73)$ sur la base $(1, X, X^2, X^3)$:

$$\begin{pmatrix} 1 & 62 & 53 & 18 \\ 0 & 57 & 34 & 8 \\ 0 & 16 & 26 & 45 \\ 0 & 37 & 67 & 62 \end{pmatrix}.$$

On recherche alors le noyau de $Q - I$, ce qui nous donne

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 43 \\ 32 \\ 1 \end{pmatrix}.$$

Seul le deuxième vecteur nous intéresse. La fonction que nous cherchons est donc :

$$f_0 \equiv j^3 + 32j^2 + 43j \bmod 73.$$

Maintenant, on calcule $g(q) = f_0(q)\eta(q)\eta(q^{73}) \bmod 73$:

$$g(q) = q^{(73+1)/24}(q^{-3} + q^{-1} - 1 + 2q + \cdots).$$

On retranche alors le terme $-\eta(q)\eta(q^{73})$ pour trouver

$$f(q) = (g(q) + \eta(q)\eta(q^{73}))/\eta(q)\eta(q^{73})$$

soit

$$f(q) = q^{-3} + q^{-2} + 3q^{-1} + 4 + 8q + 11q^2 + 19q^3 + \cdots$$

Soit $\varepsilon(n, m)$ la fonction qui vaut $+1$ si $n \bmod 6 \in \{0, 1, 5\}$ et -1 sinon. On trouve que $x^{-37/24+3}g(q) + \eta(q)\eta(q^{73})$ est congrue à la fonction

$$\begin{aligned} G(q) &= \frac{1}{2} \sum_{\substack{n,m=-\infty \\ n^2+73m^2 \equiv 1 \bmod 12}}^{\infty} \varepsilon(n, m) q^{((n^2+73m^2)-1)/12} \\ &= 1 + q^2 + q^4 + q^6 + 2q^9 + q^{10} + q^{14} + 2q^{18} + q^{24} + \cdots . \end{aligned}$$

2.3.2. Calcul du polynôme minimal. La méthode décrite dans la section 2.2.1 est utilisable, en particulier la méthode décrite à la section 2.2.2. Quand on dispose de beaucoup de mémoire centrale, on peut utiliser une deuxième méthode, proposée elle aussi par Atkin.

Soit $f(q)$ une fonction sur $\Gamma_0^*(\ell)$. Le polynôme minimal de f est :

$$\Phi_\ell^*(F, J) = (F - f(\tau)) \prod_{k=0}^{\ell-1} (F - f((\tau + k)/\ell)) = F^{\ell+1} + \sum_{r=0}^{\ell} C_r(J) F^k$$

avec $C_r(J) \in \mathbb{Q}[J]$. Par application de l'involution d'Atkin-Lehner, on a également :

$$\Phi_\ell^*(f^*(q), j^*(q)) = \Phi_\ell^*(f(q), j(q^\ell)) = 0.$$

En utilisant le lemme 2.2, on trouve cette fois que

PROPOSITION 2.7. *Le degré de $C_r(J)$ est au plus $2v$ pour tout r.*

On détermine d'abord

$$-C_1(j(\tau)) = f(\tau) + \sum_{k=0}^{\ell-1} f((\tau+k)/\ell)$$

comme à la section précédente. Il est facile de voir que

$$-C_1(j(q)) = q^{-v} + \cdots$$

ce qui conduit à $C_1(J) = -J^v + \cdots$.

Une fois ceci fait, on utilise le lemme suivant :

LEMME 2.1. *L'équation $a\ell + bv = m$, pour $0 \leq m \leq 2\ell v$, a au plus une seule solution (a, b) vérifiant $0 \leq a \leq 2v$, $0 \leq b < \ell$. Cette solution est donnée par $b \equiv m/v \bmod \ell$ et $a = (m - bv)/\ell$ quand cette quantité est positive ou nulle.*

On calcule $R_1(q) = f^{\ell+1}(q) + C_1(j(q^\ell))f^\ell(q)$ comme une série en q, ce qui nous donne

$$R_1(q) = -q^{-2v\ell} + \cdots$$

On cherche alors les termes ${J^*}^a F^b$ qui contiennent le terme $q^{-2v\ell}$. Autrement dit, on cherche a et b tels que $a\ell + bv = 2v\ell$ et d'après le lemme, une seule solution existe, qui est $a = 2v$, $b = 0$.

On calcule alors $R_2(q) = R_1(q) + j(q^\ell)^{2v}$ comme une série en q et on applique le même principe à la détermination du coefficient suivant.

Le calcul se poursuit jusqu'à la détermination des coefficients de $C_{\ell+1}(J)$. À la fin du calcul, le reste, considéré comme une série en q, doit avoir tous ses coefficients nuls, à l'ordre utilisé. Le lemme (2.1) fournit de plus un test infaillible. Si la valuation de R est m, mais que l'équation $a\ell + bv = m$ ne donne pas de solutions, alors le calcul est faux.

Dans la pratique, on précalcule les puissances de f en tant que série dans un tableau et on effectue les produits $j(q^\ell)^a f(q)^b$ à la demande, ce qui est relativement rapide car la série $j(q^\ell)^a$ est creuse, la distance entre deux termes étant ℓ. Compte tenu des paramètres, les séries sont calculées à l'ordre $\ell(2v+1)$.

Exemple. Reprenons le cas $\ell = 11$. On commence par déterminer

$$-C_1(J) = J - 684,$$

ce qui veut dire que les premiers termes de Φ_{11}^* sont $F^{12} - (J - 684)F^{11}$, qui sont rangés dans P. On calcule

$$R(q) = f(q)^{12} + C_1(j(q^{11}))f(q)^{11} = -q^{-22} + \cdots .$$

Pour annuler le terme en q^{-22}, il faut rajouter un terme en ${J^*}^2$:

$$R(q) := R(q) + j(q^{11})^2 = -55q^{-21} + \cdots$$

et

$$P := P + J^2.$$

Le terme suivant ne peut provenir que de $J^* F^{10}$, c'est-à-dire

$$R(q) := R(q) + 55 j^*(q) f(q)^{10}$$

et

$$P := P + 55JF^{10}.$$

On continue ainsi jusqu'à trouver

$$R(q) = O(q^{17}).$$

Finalement, on obtient

$$\begin{aligned}
\Phi_{11}^*(F,J) \quad = \quad & F^{12} + F^{11}(-J + 684) + F^{10}(55J + 157410) \\
& + F^9(-1188J + 12515580) + F^8(12716J + 75763215) \\
& + F^7(-69630J + 76077144) + F^6(177408J - 207606564) \\
& + F^5(-133056J - 34321320) + F^4(-132066J + 418524975) \\
& + F^3(187407J - 477130500) + F^2(-40095J + 270641250) \\
& + F(-24300J - 82012500) + J^2 + 6750J + 11390625.
\end{aligned}$$

La méthode décrite est efficace, si on stocke les séries F^a pour $1 \leq a \leq \ell$, ce qui conduit à un stockage de l'ordre de $\ell(\ell(2v+1)+c) = O(\ell^2)$ ce qui est énorme quand ℓ augmente.

2.3.3. Cas où $X_0^*(\ell)$ est de genre 0. Dans le cas où $X_0^*(\ell)$ est de genre 0, i.e., $\ell \leq 31$ ou $\ell \in \{41, 47, 59, 71\}$, on sait que

$$\Phi_\ell^*(F,J) = 0$$

où le degré en F est $\ell + 1$ et le degré en J est 2. Autrement dit :

$$J^2 - S(F)J + P(F) = 0$$

avec S et P de degré $\ell + 1$. On sait aussi que J et J^* sont les racines de cette équation. Autrement dit

$$j(q) + j(q^\ell) = S(f(q)), \qquad j(q)j(q^\ell) = P(f(q)).$$

Il suffit de remplacer $j(q)$ et $j(q^\ell)$ par leurs développements en série et d'identifier les coefficients de S et P à l'aide du développement de $f(x)$.

2.3.4. Remarque sur les calculs. Les calculs d'équations modulaires ne sont pas faits en entiers, mais plutôt modulo de petits nombres premiers, pour lesquels les opérations élémentaires se font rapidement. Les coefficients sont reconstruits l'un après l'autre à l'aide du théorème chinois. Les séries considérées ayant beaucoup de termes, il est nécessaire d'utiliser des algorithmes de multiplication rapide, comme l'algorithme de Karatsuba et la FFT [12]. Notons que l'algorithme le plus rapide, décrit à la section 2.2.2, calcule les quantités $f(q)^k$ l'une après l'autre. On économise de la mémoire dans la FFT en gardant en mémoire deux FFT consécutives.

Atkin recalcule à la volée les équations nécessaires. Nous préférons quant à nous précalculer ces équations et les stocker. Il faut 41 Moctets pour stocker toutes les équations correspondant à $\ell \leq 500$. Dans notre implantation, il a fallu 165 heures de temps CPU sur DecAlpha pour construire Φ^*_{499}.

On peut se demander comment nous pouvons vérifier les calculs faits. La façon la plus convaincante est d'utiliser les propriétés de factorisation des $\Phi(F, J)$ modulo p. Pour cela, on calcule des nombres de points sur des courbes E modulo de petits nombres premiers p et on choisit une valeur de j pour laquelle la décomposition est remarquable : cela se fait en utilisant la proposition 4.1 de [21], en connaissant t. On factorise alors $\Phi(X, j) \bmod p$ et on compare les résultats. Le type de décomposition est si atypique que cela suffit pour se convaincre.

3. Implantation de l'algorithme SEA

L'algorithme de Schoof utilise les propriétés des points de ℓ-torsion modulo p. En particulier, tous les calculs doivent être faits modulo le polynôme de ℓ-division noté $f_\ell(X)$. L'idée d'Elkies est de remplacer les calculs modulo ce polynôme par des calculs modulo un facteur de ce polynôme, quand cela est possible.

3.1. Description schématique. L'algorithme procède ainsi. Pour $\ell \leq L$, on effectue les opérations suivantes.

(1) On calcule une équation de $X_0(\ell)$, soit $\Phi_\ell(X, J)$.
(2) On recherche si $\overline{\Phi}(X) = \Phi_\ell(X, j(E)) \bmod p$ a des racines modulo p ; si oui, on peut utiliser les idées d'Elkies et calculer un facteur $g_\ell(X)$ de $f_\ell(X)$ par la méthode d'Atkin (décrite ci-dessous) ; on recherche alors la valeur propre k telle que

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

dans $\mathbb{F}_p[X, Y]/(g_\ell(X), Y^2 - (X^3 + AX + B))$, ce qui donne $t \equiv k + p/k \bmod \ell$. Le nombre ℓ est dit *nombre premier d'Elkies*.

(3) Si $\overline{\Phi}(X)$ n'a pas de racine modulo p, on détermine les classes de t possibles en déterminant le type de factorisation de $\overline{\Phi}(X) \bmod p$. Le nombre ℓ est dit *nombre premier d'Atkin.*

On s'arrête quand le produit des nombres premiers ℓ dépasse la borne $4\sqrt{p}$.

3.2. Utilisation de calculs sur les formes modulaires. On note $\mathbb{L}(\omega_1, \omega_2)$ le réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ avec $\tau = \omega_2/\omega_1 \in \mathcal{H}$. Identifions la courbe E à $\mathbb{C}/\mathbb{L}(\omega_1, \omega_2)$. Comme expliqué dans [21], le calcul d'un facteur $g_\ell(X)$ du polynôme de division $f_\ell(X)$ se réduit essentiellement au calcul des coefficients de la courbe $\hat{E} = \mathbb{C}/\mathbb{L}(\omega_1/\ell, \omega_2)$ d'équation $y^2 = x^3 + \hat{A}x + \hat{B}$, ainsi qu'à celui de

$$p_1 = \sum_{r=1}^{(\ell-1)/2} \wp(r\omega_1/\ell).$$

Il est facile de voir que la courbe $\hat{E}$ est isomorphe à $\tilde{E} = \mathbb{C}/\mathbb{L}(\omega_1, \ell\omega_2)$. Notons tout de suite que $j^* = \tilde{j}$.

On utilise les notations de [21]. Soit $E_k(q)$ la série d'Eisenstein d'ordre k. On a les formules

$$\hat{A} = -3\ell^4 E_4(\ell\tau) = -3\ell^4 \tilde{E}_4, \tag{2}$$

$$\hat{B} = -2\ell^6 E_6(\ell\tau) = -2\ell^6 \tilde{E}_6, \tag{3}$$

$$p_1 = \frac{\ell}{2}(\ell E_2(\ell\tau) - E_2(\tau)) = \frac{\ell}{2}(\ell\tilde{E}_2 - E_2). \tag{4}$$

On fera désormais les conventions $2i\pi = 1$ et $f'(q) = q df/dq$. Rappelons les formules :

$$J = \frac{E_4^3}{\Delta}, \qquad J - 1728 = \frac{E_6^2}{\Delta}, \tag{5}$$

$$\frac{J'}{J} = -\frac{E_6}{E_4}, \qquad \frac{J'}{J-1728} = -\frac{E_4^2}{E_6}, J' = -\frac{E_4^2 E_6}{\Delta}, \tag{6}$$

$$\frac{\Delta'}{\Delta} = E_2, \frac{3{E_4}'}{E_4} = E_2 - \frac{E_6}{E_4}, \frac{2{E_6}'}{E_6} = E_2 - \frac{E_4^2}{E_6}, \tag{7}$$

$$12{E_2}' = E_2^2 - E_4. \tag{8}$$

Le but de cette section est de trouver des formules algébriques pour les quantités p_1, $\tilde{E}_4$, $\tilde{E}_6$. Ces formules seront encore valables modulo p.

3.2.1. Le cas canonique. On rappelle que

$$F = f(q) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s}$$

est racine d'une équation du type

$$\Phi(F, J) = 0.$$

On commence par calculer $\tilde{\Delta}$ par

$$\tilde{\Delta} = (F^{12/s}\Delta)/\ell^{12}.$$

On calcule ensuite

$$Z = \frac{F'}{F} = s(\ell\tilde{E}_2 - E_2)/12 \tag{9}$$

soit $p_1 = (6\ell/s)Z$.

Détermination de $\tilde{E}_4$. On différencie l'équation

$$\Phi(F, J) = 0.$$

On pose

$$\partial_F = \frac{\partial\Phi}{\partial F}, \, \partial_J = \frac{\partial\Phi}{\partial_J}.$$

On obtient

$$F'\partial_F + J'\partial_J = 0.$$

On remplace alors J' à l'aide de (6) et F' à l'aide de (9) :

$$ZF\partial_F = \frac{E_6}{E_4}J\partial_J$$

ce que l'on récrit, en introduisant les notations $D_F = F\partial_F$, $D_J = J\partial_J$ et $E_0 = E_6/(E_4 Z)$, en

$$D_J E_0 - D_F = 0.$$

On différencie cette relation et on obtient :

$$E_0(J'\partial_J + J(F'\partial_{FJ} + J'\partial_{JJ})) + E_0{}'J\partial_J - (F'\partial_F + F(F'\partial_{FF} + J'\partial_{FJ})) = 0.$$

On remplace de nouveau F' et J' par leurs valeurs. On trouve

$$\begin{gathered} E_0(-E_6/E_4(D_J + J^2\partial_{JJ}) + ZFJ\partial_{FJ}) + E_0{}'D_J \\ -(Z(D_F + F^2\partial_{FF}) - E_6/E_4 FJ\partial_{FJ}) = 0. \end{gathered}$$

Pour simplifier, on pose $D_{FF} = F\partial_F(D_F) = D_F + F^2\partial_F$, $D_{FJ} = FJ\partial_{FJ}$. On trouve alors après simplification :

$$2\frac{E_6}{E_4}D_{FJ} - \frac{E_0E_6}{E_4}D_{JJ} + E_0{}'D_J - ZD_{FF} = 0. \tag{10}$$

Nous allons maintenant chercher une relation faisant intervenir $\tilde{E}_4$ et ${E_0}'$, ce qui nous donnera $\tilde{E}_4$ après élimination de ${E_0}'$. Pour ce faire, on commence par différencier

$$E_0 = \frac{E_6}{E_4 Z}.$$

On trouve

$$\frac{{E_0}'}{E_0} = \frac{{E_6}'}{E_6} - \frac{{E_4}'}{E_4} - \frac{Z'}{Z}. \tag{11}$$

Mais par ailleurs :

$$Z' = \frac{s}{12}(\ell^2 \tilde{E}_2{}' - {E_2}') = \frac{s}{12^2}(\ell^2(\tilde{E}_2^2 - \tilde{E}_4) - (E_2^2 - E_4))$$

en appliquant deux fois (8). Il ne reste plus qu'à reporter la valeur de Z' dans (11) pour finalement trouver :

$$\ell^2 \tilde{E}_4 = E_4 + \frac{12Z}{s}\left(12\frac{{E_0}'}{E_0} + 6\frac{E_4^2}{E_6} - 4\frac{E_6}{E_4} + 12\frac{Z}{s}\right). \tag{12}$$

L'élimination de ${E_0}'$ entre (10) et (12) permet de trouver $\tilde{E}_4$.

Détermination de $\tilde{E}_6$. Notons pour commencer que nous avons $\tilde{J}$ à l'aide de (5). Ensuite, on différencie

$$\Phi(F^*, J^*) = \Phi(F^*, \tilde{J}) = 0$$

ce qui donne

$$F^{*\prime}\partial_F \Phi(F^*, \tilde{J}) + \ell \tilde{J}' \partial_J \Phi(F^*, \tilde{J}) = 0.$$

On écrit alors $F^{*\prime} = -F^* F'/F = -F^* Z$ et on trouve

$$\frac{\tilde{J}'}{\tilde{J}} = Z\frac{D_{F^*}}{\ell D_{\tilde{J}}} \tag{13}$$

ce qui nous donne $\tilde{E}_6$.

Exemple numérique. On considère la courbe $y^2 = x^3 + x + 1 \bmod 101$ et on choisit $\ell = 7$. Dans ce cas, on a $v = 1$ et $s = 2$.

Le polynôme Φ_7^c a pour valeur :

$$\Phi_7^c(F, J) = F^8 - JF + 28F^7 + 322F^6 + 1904F^5$$
$$+5915F^4 + 8624F^3 + 4018F^2 + 748F + 49.$$

On calcule $J = 34$. Modulo 101, on trouve que

$$\Phi_7^c(F, 34) = (F + 81)(F + 17)(F^6 + 31F^5 + 48F^4 + 64F^3 + 5F^2 + 99F + 56).$$

On choisit $F = 20$ ce qui donne immédiatement $\tilde{F} = 7^2/20 = 58$. On en déduit $\tilde{\Delta} = (F^6\Delta)/7^{12} = 87$. On calcule alors

$$D_F = 3, D_J = 27, D_{FF} = 28, D_{JJ} = 27, D_{FJ} = 27.$$

D'autre part, on a $E_4 = -1/3 = 67$, $E_6 = -1/2 = 50$. On obtient d'abord $Z = 64$, puis $\tilde{E}_4 = 72$. Enfin, on trouve $\tilde{J} = 90$ et $\tilde{E}_6 = 45$. D'où l'équation de la courbe isogène $\tilde{A} = 19$, $\tilde{B} = 26$ et $p_1 = 31$.

3.2.2. Le cas de $X_0^*(\ell)$. On part cette fois d'une équation du type

$$\Psi(F, J) = 0 \tag{14}$$

où F représente une fonction sur $\Gamma_0^*(\ell)$.

Notons tout de suite que par application de w_ℓ, on obtient

$$\Psi(F, \tilde{J}) = 0. \tag{15}$$

Cette fois, nous devons rechercher les racines de cette équation de degré $2v - 1$ en $\tilde{J}$. Pour chaque valeur de $\tilde{J}$, on calcule alors les quantités $\tilde{E}_4$, $\tilde{E}_6$ et Z pour finalement calculer le facteur de $f_\ell(X)$, qu'il faudra vérifier par les méthodes décrites plus loin.

Détermination de $\tilde{E}_4$ et $\tilde{E}_6$. On différencie une première fois (14) :

$$F'\partial_F\Psi + J'\partial_J\Psi = 0$$

d'où l'on tire

$$F' = \frac{E_6}{E_4}\frac{J\partial_J\Psi}{\partial_F\Psi}. \tag{16}$$

On différencie ensuite (15)

$$F'\partial_F\Psi(F, \tilde{J}) + \ell\tilde{J}'\partial_J\Psi(F, \tilde{J}) = 0$$

d'où l'on obtient

$$\tilde{J}' = -\tilde{J}\frac{\tilde{E}_6}{\tilde{E}_4} = -F'\frac{\partial_{\tilde{F}}}{\ell\partial_{\tilde{J}}}.$$

Il ne reste plus qu'à remplacer F' par sa valeur (16) pour trouver la valeur de $\tilde{E}_6/\tilde{E}_4$. Une fois cela fait, on calcule $\tilde{E}_4$ par

$$\tilde{E}_4 = \frac{\tilde{J}}{\tilde{J} - 1728}\left(\frac{\tilde{E}_6}{\tilde{E}_4}\right)^2$$

puis $\tilde{E}_6$ par multiplication.

Détermination de p_1. On différencie (14) une deuxième fois :

$$F''\partial_F + {F'}^2\partial_{FF} + 2F'J'\partial_{FJ} + J''\partial_J + {J'}^2\partial_{JJ} = 0.$$

On calcule alors J'' par différenciation de (6) :

$$J'' = -J\left(-\frac{E_6^2}{E_4^2} + \frac{E_2E_6}{2E_4} + \frac{E_6^2}{3E_4^2} - \frac{E_4}{2}\right).$$

On injecte cette valeur dans la relation précédente et on remplace J' par sa valeur. On trouve alors :

$$\frac{F''}{F'} = \frac{1}{\partial_F}\left(-F'\partial_{FF} + 2J\partial_{FJ}\frac{E_6}{E_4} - \frac{E_6^2}{F'E_4^2}(J\partial_J + J^2\partial_{JJ})\right)$$

$$+\frac{J\partial_J}{F'\partial_F}\left(\frac{E_2E_6}{6E_4} + \frac{E_6^2}{3E_4^2} - \frac{E_4}{2}\right).$$

On utilise alors (16) pour simplifier cette relation :

$$(17)\quad \frac{F''}{F'} = \frac{1}{\partial_F}\left(-F'\partial_{FF} + 2J\partial_{FJ}\frac{E_6}{E_4} - \frac{E_6^2}{F'E_4^2}(J\partial_J + J^2\partial_{JJ})\right) + \frac{E_2}{6} + \frac{E_6}{3E_4} - \frac{E_4^2}{2E_6}.$$

On effectue le même travail à partir de (15) :

$$(18)\quad \frac{F''}{F'} = \frac{1}{\partial_{F*}}\left(-F'\partial_{FF*} + 2\ell\tilde{J}\partial_{FJ*}\frac{\tilde{E}_6}{\tilde{E}_4} - \ell^2\frac{\tilde{E}_6^2}{F'\tilde{E}_4^2}(\tilde{J}\partial_{J*} + \tilde{J}^2\partial_{JJ*})\right) + \ell\left(\frac{\tilde{E}_2}{6} + \frac{\tilde{E}_6}{3\tilde{E}_4} - \frac{\tilde{E}_4^2}{2\tilde{E}_6}\right)$$

où il faut lire

$$\partial_{FF*} = \frac{\partial^2\Psi}{\partial F\partial F}(F,\tilde{J}).$$

Soustrayant (17) de (18), on voit apparaître $\ell\tilde{E}_2 - E_2$ et donc p_1.

Exemple numérique. Reprenons la courbe d'équation $y^2 = x^3 + x + 1 \bmod 101$. Prenons cette fois $\ell = 23$. On trouve

$$\begin{aligned}
\Psi(F,J) \equiv\ & F^{32} + (100J+5)F^{31} + (31J+96)F^{30} + (32J+85)F^{29} \\
& +(73J+20)F^{28} + (70J+25)F^{27} + (41J+20)F^{26} \\
& +(79J+83)F^{25} + (35J+80)F^{24} + (49J+28)F^{23} \\
& +(15J+16)F^{22} + (93J+18)F^{21} + (85J+64)F^{20} \\
& +(16J+69)F^{19} + (70J+46)F^{18} + (19J+19)F^{17} \\
& +(8J+47)F^{16} + (17J+16)F^{15} + (60J+81)F^{14} \\
& +(100J+89)F^{13} + (51J+63)F^{12} + (3J+49)F^{11} \\
& +(75J+0)F^{10} + (62J+5)F^{9} + (3J+3)F^{8} + (22J+4)F^{7} \\
& +(76J+74)F^{6} + (33J+99)F^{5} + (92J+13)F^{4} \\
& +(59J+28)F^{3} + (40J+22)F^{2} \\
& +(19J+28)F^{1} + (J^2+88J+17)
\end{aligned}$$

ce qui, après substitution de $J = 34$, donne pour racines $F = 20$ et $F = 42$. Choisissant $F = 20$, on en déduit que $\tilde{J}$ est racine de

$$J^2 + 65J + 68.$$

Or $J = 34$ est aussi une racine de ce polynôme, donc $\tilde{J} = 2$. On trouve alors $F' = 66$, puis $\tilde{E}_4 = 46$, $\tilde{E}_6 = 5$, $Z = 62$.

3.3. Calcul des coefficients de $g_\ell(X)$. Posons $d = (\ell-1)/2$. On peut calculer

$$g_\ell(X) = \prod_{r=1}^{d}(X - \wp(r\omega_1/\ell)) = X^d + \sum_{i=0}^{d-1} a_i X^i$$

comme dans [21, Th. 5.3] ou bien on peut développer la relation considérée, comme dans [10] (également [4]). Soient $\wp(z)$ et $\hat{\wp}(z)$ les fonctions de Weierstrass associées respectivement aux courbes E et $\hat{E}$. On a

$$\frac{d^{2k}\wp(z)}{dz^{2k}} = \mu_k(k+1)\wp^{k+1} + \cdots + \mu_k(0)$$

avec les μ_i dans $\mathbb{Z}[A,B]$, et de même pour $\hat{\wp}$. Avec les notations de [21], on a

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

avec

$$c_1 = -A/5, \quad c_2 = -B/7,$$

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

pour $k \geq 3$ et de même pour $\hat{\wp}$. Posant

$$p_i = \sum_{r=1}^{(\ell-1)/2} \wp(r\omega_1/\ell)^i$$

on montre alors que

$$(2k)!(\hat{c}_k - c_k) = 2(\mu_k(0)p_0 + \cdots + \mu_k(k+1)p_{k+1})$$

pour $k \geq 1$ et en particulier [1]

$$\begin{aligned} A - \hat{A} &= 5(6p_2 + 2Ap_0), \\ B - \hat{B} &= 7(10p_3 + 6Ap_1 + 4Bp_0), \end{aligned}$$

ce qui permet de calculer les p_i de proche en proche et de terminer avec les sommes de Newton.

3.3.1. Vérification de $g_\ell(X)$. La façon la plus simple de vérifier que $g_\ell(X)$ est bien un facteur de f_ℓ est de calculer $\ell(X, Y)$ dans

$$\mathbb{F}_p[X, Y]/(g_\ell(X), Y^2 - (X^3 + AX + B)).$$

Si $g_\ell(X)$ est bien un facteur, alors cette quantité doit valoir O_E.

Cette manière de procéder est relativement couteuse. Une approche probabiliste consiste à remarquer que si g_ℓ est bien un facteur, alors les p_i sont les sommes de puissances des racines de g_ℓ et elles doivent vérifier en particulier :

$$p_{d+i} + a_{d-1}p_{d-1+i} + \ldots + a_1 p_{1+i} + a_0 p_i \equiv 0 \bmod p$$

pour tout $i > 0$. Si cette relation n'est pas vraie pour une valeur de i, alors g_ℓ n'est pas le facteur attendu.

En pratique, on utilise d'abord cette idée (typiquement pour tous les $i \leq 4$), puis on prouve que le facteur est bon à l'aide de la première méthode.

3.3.2. Exemple numérique. Considérons toujours $E : y^2 = x^3 + x + 1 \bmod 101$ et $\ell = 7$. On a vu que $\tilde{A} = 19$, $\tilde{B} = 26$ et $p_1 = 31$. On trouve alors que

$$g_7(X) = X^3 + 70X^2 + 47X + 10$$

qui est bien un facteur de $f_7(X)$.

[1]Les formules données ci-dessous corrigent celles de [4].

3.4. Recherche des valeurs possibles de $t \bmod \ell$**.** Si ℓ est un nombre premier d'Elkies, dans le cas général, $\Phi_\ell(F, J)$ a deux racines distinctes F_1 et F_2 et s facteurs de degré r tel que $rs = \ell - 1$. D'autre part, d'après [21], s doit être tel que
$$\left(\frac{p}{\ell}\right) = (-1)^s.$$

Si ℓ est un nombre premier d'Atkin, $\Phi(F, J)$ se factorise comme un produit de s facteurs irréductibles de degré r où r est l'ordre de α/β, avec α et β les racines de $X^2 - tX + p \equiv 0 \bmod \ell$ dans $\mathbb{F}_{\ell^2}$. On a donc $rs = \ell + 1$ et on utilise aussi le fait que
$$\left(\frac{p}{\ell}\right) = (-1)^s.$$

D'un point de vue pratique, on dispose de $X_p = X^p \bmod (\overline{\Phi}, p)$ où $\overline{\Phi}$ est le polynôme $\Phi_\ell(X, j(E))$ dont on a éventuellement enlevé les facteurs linéaires. Avec cela, r est le plus petit entier compatible avec les conditions précédentes, pour lequel
$$\operatorname{pgcd}(X^{p^r} - X, \overline{\Phi}) = \overline{\Phi} \bmod p.$$

Si ℓ est un nombre premier d'Atkin, on détermine un ensemble $\mathcal{T}_\ell$ de valeurs possibles de $t \bmod \ell$. Ces informations peuvent être utilisées avec les autres valeurs de t connues, dans un processus de tri-recherche décrit dans [1]. Utiliser ces informations permet de réduire notablement la taille des ℓ utilisés. Notons que les ℓ intéressants sont ceux pour lesquels $\ell + 1$ a beaucoup de diviseurs et r est petit. Si r est trop grand, l'ensemble $\mathcal{T}_\ell$ est trop grand et les calculs à faire sont trop nombreux.

3.5. Utilisation de l'algorithme original de Schoof. Supposons que ℓ soit un nombre premier d'Atkin. Si ℓ est petit, on peut songer à utiliser la formulation originale de l'algorithme d'Atkin, i.e., chercher $t \bmod \ell$ tel que
$$(X^{p^2}, Y^{p^2}) + p(X, Y) = t(X^p, Y^p)$$
dans $\mathbb{F}_p[X, Y]/(Y^2 - (X^3 + AX + B), f_\ell(X))$.

Soit r le degré du plus petit facteur de $\overline{\Phi}$. Comme remarqué par Dewaghe [9], le polynôme de ℓ division a s facteurs de degré $r(\ell - 1)/2$. On peut calculer un de ces facteurs de la façon suivante. Soit $P(X)$ un facteur de degré r de $\overline{\Phi}$. On utilise alors les formules d'Elkies en prenant comme racine de $\overline{\Phi}$, la quantité $X \bmod P(X)$. On calcule ainsi un facteur de degré $(\ell - 1)/2$ de $f_\ell(X)$ dans $\mathbb{F}_{p^r}$, d'où l'on déduit un facteur de $f_\ell(X)$ dans $\mathbb{F}_p$ par conjugaison. Remarquons qu'une façon agréable de procéder consiste à calculer les quantités p_i pour $i \leq r(\ell - 1)/2$ et à calculer les conjugués de ces valeurs pour retrouver ensuite les coefficients du polynôme.

3.6. Recherche de la valeur propre. Une fois r trouvé, il est facile d'en déduire les valeurs possibles de $t \bmod \ell$. Dans le cas des nombres premiers d'Elkies, d'en déduire les valeurs possibles des valeurs propres, ce qui réduit les calculs de comparaison de la phase finale : on peut alors chercher à évaluer tous les $k(X, Y)$ possibles en cherchant une chaîne d'addition passant par tous les k.

Une autre stratégie possible consiste à utiliser l'algorithme des pas de bébés et des pas de géants pour trouver k, ce qui donne une méthode en $O(\sqrt{\ell})$, qui est rentable pour ℓ assez grand.

Dans certains cas, il n'est pas nécessaire de comparer (X^p, Y^p) à $(X_k, Y_k) = k(X, Y)$, mais seulement Y^p à Y_k, ce qui économise le calcul de X^p.

Théorème 3.1 (Atkin). *On suppose qu'on a trouvé k tel que $Y^p = Y_k$. Alors k est la valeur propre cherchée si l'une des deux conditions suivantes est satisfaite : $\ell \equiv 2 \bmod 3$ ou le coefficient de degré $(\ell - 3)/2$ de $g_\ell(X)$ est non nul.*

Des améliorations récentes ont été apportées par Müller dans [18]. Ces améliorations sont d'autant plus efficaces qu'on les combine avec celles de Dewaghe [9].

4. Un exemple commenté

Le record actuel (janvier 1995) est dû à l'auteur et nous donnons quelques précisions ci-dessous.

Soit $p = 10^{499} + 153$ et soit E la courbe d'équation

$$Y^2 = X^3 + 4589X + 91128 \bmod p.$$

Le nombre de points de E est

```
 9999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999
44682874946393430837023469796815125401276025967453
13431934003682988725862007054255557388439383741349
85777620270659468449641006111967762792620320150837
67465239137548918259039320818106478783274195638932
66793169565046034050773489405593091850135305821185
```

Les calculs ont été faits sur plusieurs DecAlpha (du LIX et à l'INRIA) et se sont terminés le 26 janvier 1995. Il a fallu 2900 heures pour le calcul de X^p et 4200 en tout.

Dans le cas où ℓ est de type A (c'est par exemple le cas de $\ell = 271$), on peut tenter de recourrir à l'algorithme original de Schoof en utilisant l'approche de Dewaghe [9].

Dans les tableaux qui suivent, on donne des renseignements complémentaires sur $t \bmod \ell^n$. Si ℓ est de type E, on donne les valeurs propres de ϕ ainsi que leurs ordres sous la forme (t, k_1, d_1, k_2, d_2). Dans le cas A, on donne le rapport entre $n/(\ell - 1)$ où n est le nombre de classes possibles de $t \bmod \ell$ (plus le rapport est petit, plus ℓ est utile). Une étoile indique que le nombre premier ℓ a été retenu pour la phase de tri-recherche. Noter que tous les nombres premiers ne sont pas présents : la recherche de toutes les valeurs est parfois coûteuse et n'est intéressante que si $\ell + 1$ a beaucoup de diviseurs.

5. Conclusion

Nous avons tenté de donner un aperçu des techniques à mettre en œuvre pour compter le nombre de points sur une courbe elliptique modulo p. D'autres améliorations ont été apportées récemment, en particulier en ce qui concerne l'utilisation des puissances des nombres premiers d'Elkies. Nous renvoyons à [5] pour cela. Signalons pour finir que, dans le cas de la caractéristique 2, le record actuel est le calcul de la cardinalité d'une courbe elliptique dans $\mathbb{F}_{2^{601}}$, détenu par Lercier.

Remerciements. L'auteur tient à remercier O. Atkin pour son aide précieuse lors de l'implantation de l'algorithme et pour ses réponses aux nombreuses questions que l'auteur lui a posées ; B. Edixhoven pour ses éclaircissements concernant les propriétés de la courbe $X_0(\ell)$; R. Schoof pour de fructueuses discussions concernant SEA et pour avoir mis à sa disposition son article [21].

Bibliographie

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

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

[3] B. J. Birch et W. Kuyk (Réd.), *Modular functions of one variable IV*, Lecture Notes in Math., vol. 476, Springer, 1975, Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.

[4] L. S. Charlap, R. Coley, et D. P. Robbins, *Enumeration of rational points on elliptic curves over finite fields*, Manuscrit, 1991.

[5] J.-M. Couveignes et F. Morain, *Schoof's algorithm and isogeny cycles*, ANTS-I (L. Adleman et M.-D. Huang, Réd.), Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, 1994, p. 43–58.

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

[7] P. Deligne et M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable II (P. Deligne et W. Kuyk, Réd.), Lecture Notes in Math., vol. 349, Springer, 1973, Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972, p. 143–316.

[8] P. Deligne et J,-P, Serre, *Formes modulaires de poids* 1, Ann. scient. Éc. Norm. Sup. **7** (1974), 507–530.

[9] L. Dewaghe, *Remarques sur l'algorithme SEA*, en préparation, décembre 1994.

[10] Noam D. Elkies, *Explicit isogenies*, Manuscrit, 1991.

[11] R. Fricke, *Lehrbuch der Algebra, III*, F. Vieweg and Sohn, Braunschweig, 1928.

[12] D. E. Knuth, *The Art of Computer Programming: Seminumerical algorithms*, Addison-Wesley, 1981.

[13] F. Lehmann, M. Maurer, V. Müller, et V. Shoup, *Counting the number of points on elliptic curves over finite fields of characteristic greater than three*, ANTS-I (L. Adleman et M.-D. Huang, Réd.), Lecture Notes in Comput. Sci., vol. 877, Springer-Verlag, 1994, p. 60–70.

[14] R. Lercier et F. Morain, *Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm*, Rapport de Recherche LIX/RR/95/09, École Polytechnique, septembre 1995.

[15] R. Lercier et F. Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, Advances in Cryptology – EUROCRYPT '95 (L. C. Guillou et J.-J. Quisquater, réd.), Lecture Notes in Comput. Sci., no. 921, 1995, p. 79–94.

[16] K. Mahler, *On a class of non-linear functional equations connected with modular functions*, J. Austral. Math. Soc. Ser. A **22** (1976), 65–120.

[17] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[18] V. Müller, *Looking for the eigenvalue in Schoof's algorithm*, en préparation, octobre 1994.

[19] B. Schoeneberg, *Elliptic modular functions*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 203, Springer–Verlag, 1974.

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

[21] René Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux, **7** (1995), 219–254.

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

ℓ^n	type		ℓ^n	type	
2^7	E	(25)	199	E	$(89, 138, 22, 150, 198)$
3^5	S	(116)	211	A	0.25
5^5	E	$(844, 1, 1, 3, 4)$	223	E	$(113, 34, 37, 79, 222)$
7^4	E	$(1355, 5, 6, 6, 2)$	227	E	$(111, 46, 226, 65, 113)$
11	S	(3)	229	E	$(188, 153, 57, 35, 228)$
13^3	E	$(1756, 11, 12, 3, 3)$	233	A	0.31
17^2	E	$(263, 10, 16, 15, 8)$	239	A	0.07
19	S	(18)	241	A	0.46
23^2	E	$(109, 6, 11, 11, 22)$	251	E	$(192, 206, 250, 237, 125)$
29^2	E	$(836, 9, 14, 15, 28)$	257	A	0.33
31	S	(9)	263	A	0.03
37	A	0.50	269	E	$(224, 181, 268, 43, 134)$
41	S	(4)	271	S	(184)
43	A	0.48	281	A	0.33
47	E	$(41, 13, 46, 28, 23)$	283	A	0.50
53	A	0.35	293	A	0.29
59	E	$(8, 56, 58, 11, 58)$	307	A	0.20
61^2	E	$(893, 19, 30, 20, 5)$	311	E	$(21, 246, 310, 86, 62)$
67	A	0.24	313	E	$(243, 109, 312, 134, 104)$
71	A	0.34	317	A	0.33
73	A	0.50	331	E	$(227, 90, 330, 137, 330)$
79	A	0.41	337	E	$(60, 184, 48, 213, 336)$
83	A	0.07	347	A	0.16
89	E	$(0, 32, 11, 57, 22)$	349	E	$(179, 61, 116, 118, 29)$
97	E	$(83, 41, 96, 42, 32)$	353	E	$(279, 73, 88, 206, 352)$
101	E	$(19, 45, 50, 75, 100)$	359	A	0.27
103	A	0.47	367	E	$(242, 244, 183, 365, 366)$
107	E	$(0, 98, 106, 9, 53)$	373	E	$(89, 6, 372, 83, 93)$
109	A	0.37	379	E	$(126, 183, 126, 322, 21)$
113	A	0.32	383	E	$(210, 238, 191, 355, 382)$
127	E	$(43, 120, 63, 50, 21)$	389	E	$(231, 43, 388, 188, 388)$
131	E	$(95, 84, 13, 11, 65)$	397	E	$(244, 251, 396, 390, 396)$
137	A	0.32	401	A	0.33
139	A	0.35	409	A	0.39
149	E	$(121, 52, 148, 69, 74)$	419	A	0.06
151	E	$(28, 13, 150, 15, 150)$	421	E	$(24, 337, 210, 108, 210)$
157	E	$(98, 103, 52, 152, 156)$	431	A	0.17
163	A	0.25	433	E	$(192, 257, 216, 368, 432)$
167	E	$(26, 151, 166, 42, 83)$	439	E	$(375, 144, 73, 231, 438)$
173	E	$(100, 31, 86, 69, 172)$	443	E	$(391, 356, 13, 35, 13)$
179	E	$(176, 55, 178, 121, 89)$	449	A	0.27
181	E	$(168, 68, 60, 100, 90)$	457	E	$(173, 76, 57, 97, 456)$
191	A	0.17	461	A	$--$
193	E	$(59, 22, 192, 37, 192)$	463	E	$(110, 19, 462, 91, 231)$
197	E	$(193, 64, 98, 129, 28)$	467	E	$(210, 247, 466, 430, 233)$

TAB. 1 - . Données pour le record

ℓ^n	type		ℓ^n	type	
479	A	$--$	739	A	$--$
487	A	$--$	743	E	$(22, 575, 371, 190, 742)$
491	A	0.16	751	A	$--$
499	E	$(334, 404, 249, 429, 498)$	757	A	$--$
503	A	$--$	761	A	$--$
509	A	$--$	769	A	$--$
521	E	$(233, 29, 13, 204, 65)$	773	E	$(74, 35, 193, 39, 193)$
523	E	$(280, 70, 261, 210, 522)$	787	A	$--$
541	E	$(482, 481, 135, 1, 1)$	797	A	$--$
547	E	$(83, 465, 546, 165, 91)$	809	E	$(243, 55, 808, 188, 808)$
557	A	$--$	811	E	$(17, 718, 810, 110, 270)$
563	A	$--$	821	A	$--$
569	E	$(554, 440, 568, 114, 71)$	823	A	$--$
571	E	$(345, 158, 95, 187, 190)$	827	E	$(650, 171, 413, 479, 59)$
577	E	$(250, 275, 72, 552, 288)$	829	A	$--$
587	E	$(584, 500, 586, 84, 293)$	839	A	$--$
593	A	$--$	853	E	$(760, 654, 426, 106, 142)$
599	A	$--$	857	A	$--$
601	A	$--$	859	E	$(388, 105, 858, 283, 858)$
607	E	$(414, 500, 606, 521, 606)$	863	A	$--$
613	E	$(487, 223, 612, 264, 153)$	877	A	$--$
617	E	$(8, 166, 14, 459, 308)$	881	A	$--$
619	E	$(252, 397, 206, 474, 309)$	883	E	$(672, 207, 882, 465, 441)$
631	A	$--$	887	E	$(753, 664, 443, 89, 886)$
641	E	$(118, 17, 640, 101, 640)$	907	A	$--$
643	E	$(367, 27, 214, 340, 321)$	911	E	$(219, 806, 91, 324, 65)$
647	A	$--$	919	E	$(313, 614, 34, 618, 306)$
653	E	$(402, 123, 326, 279, 326)$	929	A	$--$
659	E	$(193, 658, 2, 194, 47)$	937	A	$--$
661	A	$--$	941	A	$--$
673	A	$--$	947	E	$(438, 55, 473, 383, 473)$
677	A	$--$	953	A	$--$
683	A	$--$	967	A	$--$
691	E	$(272, 105, 230, 167, 345)$	971	E	$(627, 600, 194, 27, 485)$
701	E	$(278, 39, 700, 239, 28)$	977	A	$--$
709	A	$--$	983	E	$(701, 804, 491, 880, 491)$
719	E	$(160, 77, 718, 83, 359)$	991	A	$--$
727	A	$--$	997	A	$--$
733	E	$(420, 482, 732, 671, 732)$			

TAB. 2 - . Données pour le record (suite)

François MORAIN
Laboratoire d'Informatique (LIX)
École Polytechnique
91128 Palaiseau Cedex, France
e-mail: morain@polytechnique.fr