N° d'ordre 1840

THESE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNOLOGIES DE LILLE

pour obtenir

le grade de docteur de l'université

Spécialité : Mathématiques

par

Laurent DEWAGHE

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

Soutenue le 12 Décembre 1996 devant la Commission d'Examen :

Directeur de Recherche : S. FAKIR (Université de Lille I)
Président : J.C DOUAI (Université de Lille I)
Rapporteurs : H. COHEN (Université de Bordeaux I)
J.L NICOLAS (Université de Lyon I)
Membres : F. MORAIN (Ecole polytechnique Paris)
P. MAMMONE (Université de Lens)
A. TREIBICH (Université de Lens)

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

A Nathalie,
Maxime et Quentin.

Remerciements

Je remercie vivement :

- Monsieur le Professeur Sabah Fakir qui a dirigé cette thèse. Son aide et ses conseils m'ont permis de mener à bien ce travail.

- Messieurs les Professeurs Henri Cohen et Jean-Louis Nicolas pour avoir acceptés de rapporter sur ce travail et pour leur présence à la soutenance de cette thèse.

- Monsieur le Professeur Jean-Claude Douai qui a bien voulu présider le jury de cette thèse.

- Monsieur François Morain, chercheur à l'école polytechnique, qui s'est intéréssé de près à mon travail. Je saisis cette occasion pour lui exprimer ma profonde gratitude pour les discussions (via mail) très enrichissantes que j'ai eues avec lui, pour l'accueil chaleureux qu'il m'avait réservé à Paris et pour avoir accepté de faire partie du jury. Cette thèse lui doit beaucoup.

- Messieurs les Professeurs Pasquale Mammone et Armando Treibich qui m'ont fait l'honneur de participer au jury de cette thèse.

- tous ceux qui, de près ou de loin m'ont apporté, à un moment ou à un autre, leur soutien tant moral que matériel du début à la fin de ce travail, particulièrement ma famille, les "habitués" de la salle informatique 238 du batiment M3 pour leur aide et leur sympathie, sans oublier le service de reprographie de l'U.F.R de Mathématiques.

Introduction générale

0.1 Présentation du problème

Dans cette thèse, on étudie le problème de la détermination du nombre de points d'une courbe elliptique définie sur un corps fini. Ce problème n'a pas seulement un intérêt théorique mais également pratique dans le sens où il intervient en cryptographie, domaine dans lequel on travaille avec des corps de très grande caractéristique.

On désigne par $\mathbb{F}_q$ un corps fini de caractéristique p et par $\mathbb{F}_p$ son corps premier.

Notons à titre d'exemples les diverses utilisations suivantes.

0.1.1 Détermination du groupe de torsion d'une courbe elliptique

Rappelons le résultat [40] suivant

Proposition 1 *Soit $E/\mathbb{Q}$ une courbe elliptique et soient p un nombre premier et $m \geq 1$ un entier premier à p. Si la réduction $\tilde{E}/\mathbb{F}_p$ est non singulière alors l'application de réduction*

$$E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{F}_p)$$

est injective.

Ce résultat nous donne en général la méthode la plus rapide pour déterminer le sous-groupe de torsion d'une courbe elliptique défini sur $\mathbb{Q}$. En appliquant la proposition pour différents p, on peut obtenir des informations sur la torsion de $E(\mathbb{Q})$.

Exemple : Considérons la courbe elliptique $E/\mathbb{Q}$ définie par l'équation $y^2 = x^3 + 3$. Son discriminant est $\Delta = -3^5 2^4$, ainsi $\tilde{E}$(modulo p) n'est pas singulière pour $p \geq 5$. On a $\#\tilde{E}(\mathbb{F}_5) = 6$ et $\#\tilde{E}(\mathbb{F}_7) = 13$. Par suite, $E(\mathbb{Q})$ n'a pas de point de torsion non trivial. En particulier, le point $(1, 2) \in E(\mathbb{Q})$ a un ordre infini et donc $E(\mathbb{Q})$ est infini.

0.1.2 Test de primalité

Pour ce propos, signalons la proposition [18] :

Proposition 2 *Soit N un entier premier à 6 et E une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$, P un point de E et n et s deux entiers tels que $s \mid n$. Pour chaque diviseur premier r de s, on note*

$$P_r = [\frac{n}{r}]P = (x_r : y_r : z_r) \ .$$

On suppose que $[n]P = 0_E$ et $pgcd(z_r, N) = 1$ pour tout r. Alors, si p est un diviseur premier de N, on a $\#E(\mathbb{F}_p) \equiv 0 \bmod s$.

Et, on a la conséquence importante :

Corollaire 1 *Si* $s > (\sqrt[4]{N} + 1)^2$ *alors* N *est premier.*

En combinant ce résultat avec un algorithme de calcul de $\#E(\mathbb{F}_p)$ on obtient l'algorithme de primalité de Goldwasser-Killian [18].

0.1.3 Applications en cryptographie

Dans [22] et dans [30] Koblitz et Miller ont suggéré l'utilisation du groupe abelien d'une courbe elliptique sur un corps fini pour implanter les cryptosystèmes à clef révélée. Or la sécurité d'un tel système, c'est à dire la difficulté de le décoder, est basée sur la possibilité de calculer des logarithmes discret sur le groupe fini $E(\mathbb{F}_p)$. Et le meilleur algorithme connu pour ce problème est le calcul d'une racine carrée d'Odlyzko [34] qui a un temps d'exécution proportionnel au plus grand diviseur premier de l'ordre du groupe. On connaît des familles de courbes elliptiques dont l'ordre est trivial à calculer [23]. Par contre, si l'on choisit une courbe elliptique aléatoire sur $\mathbb{F}_p$, alors on a besoin, dans ce cas, d'un algorithme efficace de calcul du nombre de $\mathbb{F}_p$-points.

Notons, finalement, une dernière application, que l'on trouve avec l'algorithme de Schoof [35] de calcul d'une racine carrée dans $\mathbb{F}_p$ et qui nécessite la connaissance de $\#E(\mathbb{F}_p)$.

C'est justement René Schoof [35], en 1985, qui a mis au point un algorithme déterministe de calcul de $\#E(\mathbb{F}_q)$, de temps d'exécution polynomial en $O(\log^8 q)$. Mais cet algorithme n'est pas performant en pratique et ne permet pas d'atteindre les corps dont il est question en cryptographie. Heureusement, la méthode a subi de nombreuses modifications notamment par Elkies [17] et par Atkin [2] ,[3] pour ne citer que les plus importantes. L'algorithme est devenu l'algorithme SEA du nom de ses auteurs Schoof-Elkies-Atkin et est capable de travailler sur des corps de caractéristique très grande. Le tableau suivant traduit l'évolution rapide des résultats obtenus. La taille d'un nombre est ici son nombre de chiffres. Les courbes utilisées sont :

$$\text{LIX} : Y^2 = X^3 + 4589X + 91128 \bmod p$$

$$\text{INRIA} : Y^2 = X^3 + 105X + 78153 \bmod p$$

Cet algorithme est en $O(p^{1+o(1)})$ et est raisonnable pour p ne dépassant pas 10000. Par contre on peut utiliser l'algorithme de Shanks [38] des pas de bébés et des pas de géants pour obtenir une méthode plus rapide.

0.2.2 La méthode de Shanks

La méthode de Shanks permet de déterminer le nombre de points de tout groupe abelien fini (dont on connaît la loi de composition) lorsque l'ordre du groupe admet un majorant connu. C'est le cas pour les courbes elliptiques sur un corps fini $\mathbb{F}_p$ puisque le théorème de Hasse [19] assure que $\mid m - (p+1) \mid \leq 2\sqrt{p}$.

La méthode de Shanks détermine tous les entiers n tels que $\mid n - (p+1) \mid \leq 2\sqrt{p}$ et $[n]P = 0_E$ avec P un point aléatoire sur E en $O(p^{1/4+\epsilon})$.

On prend comme borne supérieure $S = 4\sqrt{p}$ et on pose[1] $r = \lceil \sqrt{S} \rceil = \lceil 2\sqrt[4]{p} \rceil$ et $Q = [r]P$.
Pas de bébés : P,$[2]P$,...,$[r]P = Q$.
Pas de géants : Q,$[2]Q$,...,$[r]Q$,
Puis, on calcule $H_j = [\lfloor p + 1 - 2\sqrt{p} \rfloor]P + [j]Q$ pour $j = 1, \ldots, r$ et on cherche des coïncidences du type $H_j = [i]P$ pour certains i. Si il y a un seul couple (i,j), on a $m = \lfloor p + 1 - 2\sqrt{p} \rfloor + kj - i$ et cela se produit lorsque P est un point d'ordre $\geq 4\sqrt{p}$. Sinon, on choisit un autre point P sur E ou on utilise une idée de Mestre [9] qui consiste à considérer une autre courbe telle que l'existence d'un point d'ordre supérieur à $4\sqrt{p}$ soit assurée.

Cet algorithme devrait être utilisé à la place de la formule de Lang-Trotter (méthode utilisant les symboles de Legendre) dès que la taille de p est supérieure à 10. Mais si la taille de p dépasse 30 ou 40 chiffres il faut utiliser une autre méthode à savoir l'algorithme SEA. Commençons par décrire la méthode de Schoof.

0.2.3 L'algorithme de Schoof

Maintenant, considérons un corps fini quelconque $\mathbb{F}_q$ de caractéristique p.

L'algorithme de Schoof détermine $m = \#E(\mathbb{F}_q)$ en calculant $m \bmod \ell$ pour suffisamment de petits nombres premiers ℓ. Schoof montre comment calculer $m \bmod \ell$ à partir de l'équation caractéristique de l'endomorphisme de Frobenius π de E agissant sur le sous-groupe des points de ℓ-torsion $E[\ell]$ de E. Mais, en travaillant dans $E[\ell]$, l'algorithme doit réaliser les calculs modulo le ℓ-ième polynôme de division f_ℓ de E et le degré élevé des f_ℓ rend la méthode impraticable dès que $\ell > 31$.

Notons une combinaison intéressante [6] des pas de bébés et des pas de géants et de la méthode de Schoof qui consiste à calculer $t \bmod \ell_1, \ldots, t \bmod \ell_r$ par Schoof et permet de diminuer d'un facteur de $1/\prod \ell_i$ l'amplitude de l'intervalle de Hasse.

[1] $\lceil x \rceil$ est le plus petit entier $\geq x$ et $\lfloor x \rfloor$ est le plus grand entier $\leq x$

taille des p	qui	date
30		1985
65	A.O.L Atkin	02.91
75	A.O.L Atkin	02.92
100	A.O.L Atkin	02.92
200	A.O.L Atkin	02.92
250	F. Morain	12.93
276	A.O.L Atkin	03.94
350	F. Morain	04.94
376	V. Müller	05.94
400	F. Morain	10.94
425	V. Müller	12.94
500	F. Morain	01.95

Dans cette thèse nous concentrons notre étude sur l'algorithme SEA. Le travail que je présente ici a contribué à déterminer le nombre de points sur une courbe elliptique sur un corps fini $\mathbb{F}_p$ de caractéristique un nombre premier record à savoir $p = 10^{499} + 153$ en Janvier 1995.

0.2 De 1985 à aujourd'hui

On se place tout d'abord dans le cas où le corps de base est premier.

Pour les méthodes classiques, on se réfère à [9].

Le problème est le calcul du nombre de points d'une courbe elliptique E sur un corps fini. Sur $\mathbb{F}_2$ et $\mathbb{F}_3$ le problème est trivial, on supposera donc que $p \geq 5$. Par suite, la courbe E sera donnée par une équation de Weierstrass affine

$$Y^2 = X^3 + AX + B$$

avec A et B dans $\mathbb{F}_p$ tels que $4A^3 + 27B^2 \neq 0$. L'ensemble des $\mathbb{F}_p$-points de E, noté $E(\mathbb{F}_p)$, est un groupe abelien fini. On veut déterminer $m = \#E(\mathbb{F}_p)$.

0.2.1 Méthode élémentaire

Notons, tout de suite, l'algorithme naïf utilisant le symbole de Legendre. La courbe a un point à l'infini $[0 : 1 : 0]$ et donc pour tout $x \in \mathbb{F}_p$, il y a $1 + (\frac{x^3+Ax+B}{p})$ valeurs de y. On a donc

$$m = p + 1 + \sum_{x \in \mathbb{F}_p} (\frac{x^3 + Ax + B}{p}) .$$

0.2.4 Les travaux d'Elkies et d'Atkin

L'algorithme a subi une importante amélioration en 1991 par Elkies [17] dont l'idée consiste à travailler sur un sous-groupe G de $E[\ell]$. Cette idée est née suite à la transformation par Elkies et Miller des résultats de Vélu [41], qui a permis d'atteindre les valeurs des $p_k = \sum_{g \in G} x^k(g)$ et donc des fonctions symétriques d'un facteur h_ℓ de f_ℓ avec la formule de Newton. Ainsi, travailler dans G devint possible par des congruences modulo h_ℓ. Explicitement, les coefficients du polynôme h_ℓ peuvent être calculés si l'on connaît les coefficients $\tilde{A}$, $\tilde{B}$ d'une courbe ℓ-isogène $\tilde{E}$ à E et la valeur de p_1, c'est la méthode de Elkies, ou à partir des valeurs (p_1, p_2, p_3), c'est la méthode de Charlap, Coley et Robbins [8]. On s'intéresse plus particulièrement à la méthode la plus rapide à savoir celle de Elkies.

L'idée de Elkies est utilisable lorsque $t^2 - 4q$ est un carré modulo ℓ donc pour disons la moitié des ℓ, appelés nombres premiers d'Elkies. Néanmoins la méthode a un double avantage : elle ne calcule qu'une valeur propre de π modulo ℓ et ceci en réalisant des congruences modulo h_ℓ de degré $d = (\ell - 1)/2$. Toutefois, il faut au préalable calculer h_ℓ, ce qui nécessite la détermination d'une courbe ℓ-isogène à E. Pour cela, Elkies utilise une équation $\Phi_\ell(X, Y)$ de la courbe modulaire $X_0(\ell)$ (ou la courbe $X_0(\ell)/W_\ell$ avec W_ℓ l'involution d'Atkin-Lehner) ayant des coefficients convenables. Ces équations sont construites en utilisant des fonctions particulières de $\Gamma_0(\ell)$. Des équations "utilisables" sont déterminées disons pour $\ell \leq 71$.

Atkin avait en premier apporté une contribution au problème dès 1986 pour donner la méthode *sort and match* en 1988 [2]. Cette méthode reste utilisée pour les nombres premiers qui ne sont pas d'Elkies et qu'on appelle dorénavant nombres premiers d'Atkin. Atkin a dans le même temps signalé que le type de décomposition de $\Phi_\ell(X, j(E))$ donne l'ordre multiplicatif du quotient des valeurs propres dans $\mathbb{F}_{\ell^2}$. Il a ensuite uniformisé et simplifié la méthode de Elkies en, d'une part, mettant au point une méthode de génération de fonctions pour $\Gamma_0(\ell)$ et, d'autre part, en simplifiant le passage de cette équation à $\tilde{A}, \tilde{B}, p_1$.

0.2.5 Les résultats récents

Notons, finalement, les derniers développements dans ce domaine. Couveignes-Morain [13] ont introduit la notion de cycles d'isogénies qui consiste à réutiliser la courbe isogène obtenue de la même manière que la courbe initiale et ainsi de suite. Cela permet d'atteindre un facteur de f_{ℓ^n}. Ce facteur est utilisé pour la détermination de $t \bmod \ell^n$. Müller [33] a accéléré la recherche de valeurs propres en utilisant un "funny baby-step and giant-step". Terminons avec les résultats de Couveignes [10] qui traite le cas où $p < \ell$ en considérant les groupes formels. Cela permet de travailler sur des corps de petites caractéristiques. Lercier et Morain [28] ont implanté cet algorithme pour $q = 2^r$ avec r de l'ordre de 1000. Noter que Lercier [27] a donné un algorithme différent pour $p = 2$. Plus récemment encore, Couveignes [12] a donné un autre algorithme pour tout p qui évite l'utilisation des groupes formels.

On résume les grands axes de SEA (cas où la caractéristique p du corps est telle que $p \gg \ell$, sinon il faut utiliser l'algorithme de Couveignes) avec le tableau suivant :

Méthode	Ensemble des ℓ	Groupe	Équation	Polynôme	Degré	Résultat
Schoof	$\forall \ell$	$E[\ell]$	$\pi_\ell^2 + k = r\pi_\ell$	f_ℓ	$(\ell^2-1)/2$	$t \bmod \ell$
Elkies (good case de SEA)	"good" ℓ	$E[\ell]_\lambda$	$\pi_\ell = \lambda$ *(original)* $i\pi_\ell = j$ *(Müller)*	h_ℓ	$(\ell-1)/2$	$t \bmod \ell$
Atkin (bad case de SEA)	"bad" ℓ		*Sort and Match*	Φ_ℓ	$\ell+1$	$t_i \bmod \ell$

0.3 Présentation du travail effectué

Cette thèse est présentée dans trois chapitres. Le premier chapitre concerne essentiellement le type de décomposition sur $\mathbb{F}_q$ des polynômes intervenant dans l'algorithme SEA, et plus généralement associés à E, à savoir : les polynômes de division, les polynômes de division exacte, les polynômes de semi-division et les équations polynomiales de $X_0(\ell)$. Dans le deuxième chapitre, je décris quelques innovations dans SEA, qui ont permis d'atteindre un record dans ce domaine [32]. Finalement dans le dernier chapitre, je montre quelques utilisations efficaces des cycles d'isogénies rationnelles.

Chacun de ces chapitres fait ou fera l'objet d'une publication. Le chapitre I est un article en préparation qui s'intitule : "Polynômes 'associés' à une courbe elliptique E sur un corps fini." Le chapitre II : "Remarks on the Schoof-Elkies-Atkin algorithm" va paraître dans la revue *Mathematics of Computation*. Quant au chapitre III, il fait l'objet d'un article commun avec François Morain et Jean-Marc Couveignes : "Isogeny cycles and the Schoof-Elkies-Atkin algorithm"

Voici un résumé bref de chaque chapitre.

Au **chapitre I**, j'introduis d'abord la notion de semi-ordre (noté $s(x)$ pour un élément x d'un anneau) utile pour transcrire le type de décomposition des polynômes cités.

Je décris ensuite quelques propriétés des polynômes de division f_n. Puis, je donne la forme de la décomposition en facteurs irréductibles dans $\mathbb{F}_q[X]$ des f_ℓ (Je montre au chapitre II comment expliciter certains facteurs même dans le cas Atkin).

Je montre comment définir des polynômes, que j'appelle de division exacte et notés $\mathbf{f}_n$, dont la propriété principale est de s'annuler exactement aux points d'ordre n.

Je démontre le résultat suivant :

Proposition 3 *f_ℓ est un polynôme irréductible sur $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$ où les a_i sont les coefficients d'une équation de E.*

Cela permet d'introduire les polynômes U_ℓ, dit de semi-division, de manière plus rigoureuse que dans [8]. Je décris également leur type de décomposition sur $\mathbb{F}_q$.

Finalement, en ce qui concerne les polynômes modulaires, j'obtiens principalement :

Proposition 4 *Avec $k \equiv \bmod \ell$, on a :*

1) Si k est une racine primitive modulo ℓ, alors

Φ_ℓ est irréductible sur $\mathbb{F}_q$ si et seulement si f_ℓ est irréductible sur $\mathbb{F}_q$.

2) Si k n'est pas une racine primitive modulo ℓ et si Φ_ℓ est irréductible sur $\mathbb{F}_q$, alors f_ℓ se décompose en $\frac{\ell-1}{2s(k)}$ facteurs irréductibles de degré $(\ell+1)s(k)$.

Au **Chapitre II**, je présente l'algorithme de Schoof-Elkies-Atkin. Dans un premier temps, je calcule la complexité des différentes méthodes de détermination d'une valeur propre. Je décris un nouvel algorithme de calcul d'une valeur propre du Frobenius modulo ℓ basée sur une idée de Atkin. Ce qui nous donne une méthode de complexité equivalente à la meilleure méthode connue jusqu'alors, celle de Müller, si cette dernière est réalisée en utilisant des compositions. Toutefois, je montre comment on peut éviter ces compositions . J'améliore ensuite la phase finale de détermination d'une valeur propre dans certains cas que l'on précisera.

Puis je propose une alternative à la méthode de Atkin en montrant comment on peut expliciter un facteur du polynôme de division f_ℓ même dans le cas d'un nombre premier d'Atkin. J'explique, ensuite, comment utiliser ce facteur dans la procédure de Schoof que l'on réalise, de plus, en ne calculant que les abscisses des points.

Méthode	Ensemble des ℓ	Groupe	Équation	Polynôme	Degré
Dewaghe	*"bad"* ℓ	$\cup_{i=1}^{e} G_i$	$i\pi_\ell^2 + i = j\pi_\ell$	g_ℓ	ed

Où e est l'ordre entier modulo ℓ [4] de la suite dont le polynôme caractéristique est celui de π modulo ℓ.

Au **Chapitre III**, on s'intéresse aux cycles d'isogénies rationnelles introduit par Couveignes et Morain en 1994.

J'ai remarqué que l'approche d'Elkies pouvait se résumer en une procédure de construction d'un facteur de f_ℓ à partir des quantités (A, B, p_1). Je décris dans un premier temps l'action de l'involution d'Atkin-Lehner W_ℓ sur les quantités (A, B, p_1) ce qui me donne le moyen de changer de directions dans un cycle rationnel d'isogénies en appliquant la procédure $W_\ell(A, B, p_1)$. Cela permet d'accélérer le calcul de $t \bmod \ell^n$ en, d'une part, calculant $t \bmod \ell^2$ avec un seul calcul de pgcd et, d'autre part, en optimisant l'utilisation d'un facteur de h_ℓ (h_ℓ étant un facteur de f_ℓ).

0.4 Travaux constituants la thèse

[A] J.M COUVEIGNES, L. DEWAGHE AND F. MORAIN : *Isogeny cycles and the Schoof-Elkies-Atkin algorithm.* Rapport de Recherches LIX/RR/96/03, Ecole polytechnique - LIX, Août 1996.

[B] L. DEWAGHE : *Polynômes 'associés' à une courbe elliptique sur* $\mathbb{F}_q$. En préparation Juin 1995.

[C] L. DEWAGHE : *Remarks on Schoof-Elkies-Atkin algorithm.* Soumis à Math. of Comp.

[D] L. DEWAGHE : *Un corollaire aux formules de Vélu.* En préparation, Décembre 1995.

Avant-propos

0.5 Equations modulaires

0.5.1 Le groupe modulaire et l'invariant modulaire

On se réfère à [37]. Un élément $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ agit sur $\mathcal{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ par

$$g.z = \frac{az+b}{cz+d} .$$

Le groupe modulaire est $\Gamma = SL_2(\mathbb{Z})/\{\pm 1\}$. On introduit également $\Gamma_0(\ell)$ qui est le sous-groupe d'indice $\ell + 1$ de Γ défini par :

$$\Gamma_0(\ell) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \bmod \ell\}.$$

Une forme modulaire f de poids $2k$[2] (k est un entier) est une fonction holomorphe sur $\mathcal{H}$ et à l'infini, satisfaisant à :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \forall z \in \mathcal{H}, f(z) = (cz+d)^{-2k} f(\frac{az+b}{cz+d}) .$$

La fonction f vérifie en particulier $f(z+1) = f(z)$ et admet donc un développement en série de Fourier : $f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$ avec $q = e^{2i\pi z}$.

Soit $L(1,z) = \mathbb{Z} \oplus z\mathbb{Z}$ un réseau de $\mathbb{C}$ ($z \in \mathcal{H}$). Posons

$$G_{2k}(z) = \sum_{z \in L - \{0\}} 1/z^{2k} = \sum_{(m,n) \neq (0,0)} 1/(mz+n)^{2k}$$

pour $k > 1$. La fonction G_{2k} est une forme modulaire de poids $2k$. On pose $g_2(L) = 60G_4(L)$, $g_3(L) = 140G_6(L)$ et $\Delta = g_2^3 - 27g_3^2$. Ce sont des formes modulaires de poids 4,6 et 12 respectivement. Les coefficients de la q-série de G_{2k} sont donnés par : $\sigma_k(n) = \sum_{d/n} d^k$. On a plus précisement :

$$G_{2k} = 2\zeta(2k)(1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n)$$

avec $q = e^{2i\pi z}$ et B_k les nombres de Bernouilli.

[2] Certains auteurs disent que f est de poids k

Nous utiliserons plus précisement les séries d'Einsenstein normalisées, notée $E_{2k}(z)$. On a

$$E_{2k}(z) = 1/2\zeta(2k)G_{2k}(z).$$

En particulier , on a

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \quad \text{et} \quad E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Remarque 1 *Les séries d'Eisenstein E_4 et E_6 sont des formes modulaires pour $SL_2(\mathbb{Z})$ de poids 4 et 6 respectivement. Par contre, E_2 n'est pas une forme modulaire pour $SL_2(\mathbb{Z})$. On a [21],*

$$\frac{1}{z^2}E_2(-1/z) = E_2(z) + \frac{12}{2\pi iz}.$$

Toutefois, la fonction $\mathcal{E}_2(z) = \ell E_2(\ell z) - E_2(z)$ est une forme modulaire de poids 2 pour $SL_2(\mathbb{Z})$.

L'invariant modulaire est $j = 12^3\frac{g_2^3}{\Delta}$. On peut montrer que la q-série de j est

$$j(q) = \frac{1}{q} + 744 + \sum_{n\geq 1} d_n q^n.$$

Remarque 2 *La notation standard pour les coefficients de j est c_k et non d_k, mais nous allons utiliser c_k pour les coefficients de la fonction de Weierstrass.*

0.5.2 La fonction de Weierstrass

Pour tout réseau L de $\mathbb{C}$, on considère la fonction de Weierstraß

$$\wp(z) = \frac{1}{z^2} + \sum_{w\in L'}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right).$$

On a

Proposition 5 *Pour tout complexe z dans $\mathbb{C} - L$, on a*

$$\wp_L(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n}(L)z^{2n},$$

et

$$\wp_L'(z)^2 = 4\wp_L^3(z) - g_2(L)\wp_L(z) - g_3(L).$$

Ainsi, le point de coordonnées $(\wp_L(z), \wp'_L(z))$ est un point de la courbe

$$Y^2 = 4X^3 - g_2X - g_3.$$

D'autre part, on pose $c_k = (2k+1)G_{2k}(z)$ et on vérifie facilement que $c_k \in \mathbb{Q}[A,B]$. Les coefficients c_k sont entièrement déterminés par A, B. En effet, on a $c_1 = -A/5$ et $c_2 = -B/7$ puis

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

0.5.3 La fonction de Dedekind

Soit z un nombre complexe dans $\mathcal{H}$ et posons $q = e^{2i\pi z}$. La fonction η de Dedekind est défini par

$$\eta(z) = q^{1/24} \prod_{m \geq 1} (1 - q^m) .$$

On peut exprimer η de la manière suivante

$$\eta(z) = q^{1/24}(1 + \sum_{n \geq 1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2})) .$$

0.5.4 La courbe $X_0(\ell)$

Soit ℓ un entier premier et $X_0(\ell)$ la $\ell^{ième}$ courbe modulaire. On s'intéresse à une équation de $X_0(\ell)$, c'est à dire une équation polynomiale du type $\Phi_\ell(f(q), j(q)) = 0$ où f est une fonction sur $\Gamma_0(\ell)$. On pourrait se contenter d'utiliser le fait que $j(\ell z)$ est une fonction sur $X_0(\ell)$ mais l'équation reliant ces invariants modulaires, notée encore $\Phi_\ell(F, J)$, a des coefficients énormes. Par exemple :

$\Phi_2(X,Y) = X^3 - X^2Y^2 + Y^3 + 1488(X^2Y + Y^2X) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000$, et
$\Phi_3(X,Y) = X^4 - X^3Y^3 + Y^4 + 2232(X^2 + Y^2) - 1069956(X^3Y + Y^3X) + 36864000(X^3 + Y^3) + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) + 2^{31}5^622973XY + 2^{45}3^35^9(X + Y)$.

Lorsque $X_0(\ell)$ est de genre 0 (i.e ℓ=2,3,5,7,13), on connaît une paramétrisation de cette courbe, autre que la paramétrisation classique par les invariants de courbes elliptiques ℓ isogène, par

$$x_\ell(z) = \left(\frac{\eta(z)}{\eta(\ell z)}\right)^{24/(\ell-1)} ,$$

et l'invariant modulaire j est relié à x_ℓ par les formules suivantes :

$$j = \frac{(x_2+16)^3}{x_2} = \frac{(x_3+27)(x_3+3)^3}{x_3} = \frac{(x_5^2+10x_5+3)^3}{x_5}$$

$$= \frac{(x_7^2+13x_7+49)(x_7^2+5x_7+1)^3}{x_7} = \frac{(x_{13}^2+5x_{13}+13)(x_{13}^4+7x_{13}^3+20x_{13}^2+19x_{13}+1)^3}{x_{13}}.$$

On constate que l'on a une équation beaucoup plus simple que celle reliant les invariants modulaires. Pour les autres valeurs de ℓ, on peut se référer aux travaux de Atkin et Morain pour avoir une équation simple de $X_0(\ell)$.

0.6 Courbes elliptiques

0.6.1 Courbes elliptiques sur K

Soit K un corps de caractéristique quelconque. Soit $\mathbb{P}_2(K)$ le plan projectif sur K dont les points sont notés $[X : Y : Z]$.

Une courbe elliptique est une courbe régulière donnée par une équation générale en coordonnées projectives $\mathcal{F}(X,Y,Z) = 0$ définie par

$$\mathcal{F}(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

avec les a_i dans K.

Le discriminant Δ défini par

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

où

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

est non nul dans K.

On définit également l'invariant modulaire de la courbe

$$j(E) = \frac{((a_1^2+4a_2)^2 - 24(a_1a_3+2a_4))^3}{\Delta}.$$

En caractéristique différente de 2 et 3, on peut considérer une équation plus simple pour la courbe E, à savoir, une équation sous forme de Weierstrass :

$$Y^2 = X^3 + AX + B$$

et la formule du discriminant se réduit à $\Delta = -16(4A^3 + 27B^2)$ et celle de l'invariant modulaire à $j(E) = 1728\frac{4A^3}{\Delta}$.

L'ensemble des points de E défini sur K est :

$$E(K) = \{[X : Y : Z] \in \mathbb{P}_2(K) \mid \mathcal{F}(X,Y,Z) = 0\}.$$

Il y a un unique point de E avec $Z = 0$, à savoir $[0 : 1 : 0]$ appelé point à l'infini de E, noté O_E. On a :

$$E(K) = \{(X,Y) \in K \times K \mid \mathcal{F}(X,Y,1) = 0\} \cup \{O_E\}.$$

L'ensemble $E(K)$ est un groupe abelien pour la loi *chord and tangent*, noté $\oplus$. Plus précisément, on a :

Théorème 1 *Soit E une courbe elliptique sur K d'équation affine $\mathcal{F}(X,Y,1)=0$.*

1. *Soit $P_0=(x_0,y_0)\in E$. Alors $-P_0=(x_0,-y_0-a_1x_0-a_3)$.*
2. *Soit $P_1\oplus P_2=P_3$ avec $P_i=(x_i,y_i)\in E$.*
   Si $x_1=x_2$ et $y_1+y_2+a_1x_2+a_3=0$ alors $P_1\oplus P_2=O_E$.
   Sinon, soit

$$\begin{cases} \lambda=\frac{y_1-y_2}{x_1-x_2} \quad \text{et} \quad \mu=\frac{y_1x_2-y_2x_1}{x_2-x_1} & \text{si } x_1\neq x_2 \\ \lambda=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} \quad \text{et} \quad \mu=\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3} & \text{si } x_1=x_2 \end{cases}$$

alors $x_3=-a_2-x_1-x_2+\lambda^2+a_1\lambda$ et $y_3=-\mu-a_3-(\lambda+a_1)x_3$.

0.6.2 En caractéristique zéro

Dans ce cas la courbe elliptique peut-être vue comme le quotient de $\mathbb{C}$ par un réseau $L=L(1,z)=\mathbb{Z}\oplus\mathbb{Z}z$, avec $z\in\mathcal{H}$. La courbe $E=\mathbb{C}/L$ est paramétrée par la fonction de Weierstrass $\wp$. Plus précisément, on a

Théorème 2 *Il existe une correspondance analytique biunivoque entre $\mathbb{C}/L$ et la courbe*

$$y^2=4x^3-g_2(L)x-g_3(L)$$

donnée par

$$\Upsilon : z\mapsto (z^3\wp(z),z^3\wp'(z),z^3)\ .$$

0.6.3 En caractéristique p

La courbe elliptique est donnée par une équation $\mathcal{F}(X,Y,Z)=0$ à coefficients dans $\mathbb{F}_q$. On s'intéresse au sous-groupe fini $E(\mathbb{F}_q)$ de $E(\bar{\mathbb{F}}_q)$ et plus particulièment à l'ordre de ce sous-groupe.

Une classe de courbes particulières va nous être donnée par la définition suivante :

Définition 1 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$ telle que $\sharp E(\mathbb{F}_q)=q+1-t$. On dira que E est une courbe supersingulière si p divise t.*

On supposera, dans tout ce qui suit, que la courbe elliptique E n'est pas supersingulière.

La multiplication par un entier n est un morphisme, noté $[n]$, dont le noyau est l'ensemble $E[n]$ des points de n-torsion. La structure de groupe sur $\bar{\mathbb{F}}_q$ est décrite par la proposition suivante :

Proposition 6 *Soient p un nombre premier et $\mathbb{F}_q$ un corps fini de caractéristique p. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On a :*

(i) Le groupe $E(\bar{\mathbb{F}}_q)$ est un groupe de torsion,
(ii) Si $p \not| \ell$ alors $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$,
(iii) Si n est une puissance de p alors $E[n] \simeq \mathbb{Z}/n\mathbb{Z}$ si E n'est pas supersingulière.

On note π l'endomorphisme de Frobenius de E, défini par $\pi : (x, y) \mapsto (x^q, y^q)$ pour $(x, y) \in E(\bar{\mathbb{F}}_q)$.

Proposition 7 *Soit E une courbe elliptique sur $\mathbb{F}_q$ et soit π son endomorphisme de Frobenius. On a*
(i) Dans $End_{\mathbb{F}_q}(E)$, π vérifie la relation : $\pi^2 - [t]\pi + [q] = 0$,
(ii) $|t| \leq 2\sqrt{q}$,
(iii) $\sharp E(\mathbb{F}_q) = q + 1 - t$.

Chapitre 1

Polynômes "associés" à une courbe elliptique E sur $\mathbf{F}_q$

1.1 Introduction

Soient p un nombre premier et ℓ un nombre premier impair tel que $\ell < p$. On considère une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. La courbe E est donnée par une équation générale $\mathcal{F}(X,Y,Z) = 0$ définie par

$$\mathcal{F}(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

avec les a_i dans $\mathbb{F}_q$ et le discriminant Δ défini par

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

où

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

est non nul dans $\mathbb{F}_q$. L'ensemble

$$E(\bar{\mathbb{F}}_q) = \{(X,Y) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q \mid \mathcal{F}(X,Y,1) = 0\} \cup \{O_E\},$$

où $\bar{\mathbb{F}}_q$ est une clôture algébrique de $\mathbb{F}_q$, possède une structure de groupe abélien dont l'élement neutre est O_E.

On s'intéresse dans ce chapitre aux propriétés de polynômes de $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X, Y]$ que l'on dira associés à la courbe elliptique E. Plus particulièrement, on étudie leurs décompositions en facteurs irréductibles sur $\mathbb{F}_q$. On considère les polynômes suivants :

1. Le n-ième polynôme de division de E, notés f_n, et dont la propriété principale est de s'annuler exactement aux points de n-torsion $E[n]$ de E.
2. Le ℓ-ième polynôme, disons de semi-division, de E, notés $\mathcal{U}_\ell$ [8] et dont les zéros sont les sommes des abscisses des points des sous-groupes cycliques d'ordre ℓ de $E[\ell]$.
3. Le n-ième polynôme, disons de division exacte, de E, notés $\mathfrak{f}_n$, qui s'annulent exactement aux points d'ordre n.
4. Le ℓ-ième polynôme modulaire $\Phi_\ell(X,J)$, qui représente une équation affine de la ℓ-ième courbe modulaire $X_0(\ell)$, que l'on considère en $J = j(E)$, l'invariant modulaire de la courbe E.

L'introduction générale nous a permis de voir un aperçu des motivations de ce travail sur cet ensemble de polynômes. A savoir, le type de décomposition, dans $\mathbb{F}_q[X]$, nous donne des renseignements sur $\#E(\mathbb{F}_q)$.

Dans ce chapitre, on présente, essentiellement, la forme de la décomposition en facteurs irréductibles dans $\mathbb{F}_q[X]$ des polynômes associés à E : $f_\ell(X)$, $\mathcal{U}_\ell(X)$ et $\Phi_\ell(X, j(E))$. On montrera en particulier le lien entre la décomposition de f_ℓ et Φ_ℓ sur $\mathbb{F}_q$.

Le chapitre s'articule de la manière suivante : dans un premier temps, je généralise les propriétés de l'ordre entier e d'une suite récurrente d'ordre 2. L'ordre entier sera utile

pour la description de la forme de la décomposition en facteurs irréductibles des polynômes énoncés. Au paragraphe suivant, je décris quelques propriétés des polynômes de division et je donne leur type de décomposition sur $\mathbb{F}_q$. Puis, j'introduis les polynômes de division exacte. Finalement, je décris le type de décomposition des polynômes de semi-division et des polynômes modulaires.

Notation : On désigne par le type de décomposition d'un polynôme P sur un corps K la forme de sa décomposition en facteurs irréductibles dans $K[x]$. Plus précisement, on note

$$P = (n_1 * d_1 * *p_1, n_2 * d_2 * *p_2, \ldots)$$

pour signifier que dans cette décomposition P possède n_1 facteurs irréductibles de degré d_1 à la puissance p_1, n_2 facteurs .... De plus, on abrégera $n * d * *1$ en $n * d$ et $1 * d$ en d.

1.2 Suites linéaires récurrentes d'ordre 2

1.2.1 Définitions et propriétés

On considère les suites linéaires récurrentes d'ordre 2 (en abrégé slr2) dans $\mathbb{Z}/\ell^n\mathbb{Z}$ dont le polynôme caractéristique est $P_n(x) = x^2 - \tau_n x + k_n$ avec $\tau_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ et $k_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$. On note $D_n = \tau_n^2 - 4k_n$ le discriminant de P_n modulo ℓ^n. On s'intéresse à l'ordre entier e_n modulo ℓ^n de P_n, c'est à dire, par définition, au plus petit entier r tel que $x^r \equiv$ un entier ω_n modulo $(\ell^n, x^2 - \tau_n x + k_n)$. Dans le cas $n = 1$, on posera $e_1 = e$ et $P_1(x) = x^2 - \tau x + k$.

Notons que la suite $(e_n)_{n\in\mathbb{N}}$ est une suite croissante.

On utilisera deux suites particulières dont le polynôme caractéristique est P_n : la suite U_r de valeurs initiales $(0, 1)$ et la suite V_r de valeurs initiales $(1, 0)$.

Remarque 3 *Si on note α et β les racines de $P_n(x) = 0$ dans un corps quelconque, on a*

$$\text{si } \alpha \neq \beta \text{ alors } \forall r \in \mathbb{N} \quad U_r = \frac{\alpha^r - \beta^r}{\alpha - \beta} \quad \text{et} \quad V_r = \frac{\alpha\beta^r - \beta\alpha^r}{\alpha - \beta}$$

et

$$\text{si } \alpha = \beta = \lambda \text{ alors } \forall r \in \mathbb{N} \quad U_r = r\lambda^{r-1} \quad \text{et} \quad V_r = (1 - r)\lambda^r$$

sur ce corps. De la définition de e_n, on a

$$U_{e_n} \equiv 0 \bmod \ell^n,$$

donc si $\alpha \neq \beta$, alors e_n est l'ordre de α/β modulo ℓ^n.

On généralise les résultats de [4] concernant l'ordre entier d'une slr2.

Lemme 1 *Pour tout n dans $\mathbb{N}_{\geq 2}$, on a e_{n-1} divise e_n.*

Démonstration: On a $U_{e_n} \equiv 0 \bmod \ell^n$ donc $U_{e_n} \equiv 0 \bmod \ell^{n-1}$ ainsi $(\frac{\alpha}{\beta})^{e_n} \equiv 1 \bmod \ell^{n-1}$ et par suite e_{n-1} divise e_n. □

Lemme 2 *Si D_1 est un carré non nul modulo ℓ, alors P_n admet deux racines modulo ℓ^n et si on note α_n et β_n ces racines, alors $e_n = \mathrm{ord}(\frac{\alpha_n}{\beta_n})$. De plus si $\mathrm{ord}(\frac{\alpha_n}{\beta_n}) \neq \mathrm{ord}(\frac{\alpha_{n-1}}{\beta_{n-1}})$, alors $e_n = \ell e_{n-1}$, sinon on a évidemment $e_n = e_{n-1}$.*

Si D_1 n'est pas un carré modulo ℓ, alors P_1 admet deux racines dans $\mathbb{F}_{\ell^2}$ et si on note α_n et β_n ces racines modulo ℓ^n, alors on a le même résultat que précédemment.

Si D_1 est nul modulo ℓ, alors e_n est une puissance de ℓ.

Démonstration: Lorsque D_1 est nul modulo ℓ on a $e_1 = \ell$ puisque $U_r = r\lambda^{r-1}$. On en déduit immédiatement le résultat pour e_n.

Lorsque D_1 n'est pas nul modulo ℓ on a

$$\forall r \in \mathbb{N} \quad x^r \equiv U_r(\alpha_n, \beta_n)x + V_r(\alpha_n, \beta_n) \bmod (\ell^n, P_n(x)).$$

Par suite, si on pose $u = \alpha_{n-1}/\beta_{n-1}$ on a $e_{n-1} = \mathrm{ord}(u) \bmod \ell^{n-1}$. De $u^{e_{n-1}} \equiv 1 \bmod \ell^{n-1}$ on déduit que $u^{\ell e_{n-1}} \equiv 1 \bmod \ell^n$ donc e_n divise ℓe_{n-1}. Du lemme précédent, le résultat suit immédiatement. □

Proposition 8 *Si P_1 est irréductible sur $\mathbb{F}_\ell$ alors e_n est un diviseur de $\ell^{n-1}(\ell+1)$ et $\ell^{n-1}(\ell+1)/e$ est pair (resp. impair) si $(\frac{k}{\ell}) = 1$ (resp. $(\frac{k}{\ell}) = -1$).*

Si P_1 est réductible mais non-carré sur $\mathbb{F}_\ell$ alors e_n est un diviseur de $\ell^{n-1}(\ell-1)$ et $\ell^{n-1}(\ell-1)/e$ est pair (resp. impair) si $(\frac{k}{\ell}) = 1$ (resp. $(\frac{k}{\ell}) = -1$).

Si P_1 est un carré sur $\mathbb{F}_\ell$ alors e_n est un diviseur de ℓ^n.

Démonstration: Le fait que e_n divise $\ell^{n-1}(\ell+1)$ ou $\ell^{n-1}(\ell-1)$ ou ℓ^n provient immédiatement du lemme combiné avec les résultats déjà connu sur l'ordre entier d'une suite récurrente modulo ℓ dans [4]. Pour la parité, une simple récurrence suffit pour démontrer le résultat. □

Définition 2 *Pour $n \in \mathbb{N}^*$, un élément x de $\mathbb{F}_{\ell^n}$ est appelé racine primitive modulo ℓ si x est d'ordre $\ell^n - 1$.*

On utilisera également la notion de polynôme primitif.

Définition 3 *Soit $f(x) \in \mathbb{F}_\ell[x]$ un polynôme, de degré 2, irréductible sur $\mathbb{F}_\ell$. On dit que f est primitif si ses racines (dans $\mathbb{F}_{\ell^2}$) sont des racines primitives modulo ℓ.*

On a une caractérisation des polynômes primitifs:

Proposition 9 *Une cns pour que $x^2 - \tau x + k$ soit un polynôme primitif sur $\mathbb{F}_\ell$ est:*

(i) l'ordre entier de $x^2 - \tau x + k$, modulo ℓ, est $\ell + 1$,

(ii) k est une racine primitive modulo ℓ.

1.2.2 Le semi-ordre

On introduit une nouvelle notion, celle du semi-ordre.

Définition 4 *Soient $(H,+,\times)$ un anneau et 1 l'élément neutre du groupe $(H^*,\times)$. On appelle semi-ordre de $u \in H^*$, noté $s(u)$, l'ordre de u dans le groupe $H^*/(\pm 1)$.*

On note π_ℓ la restriction de π à $E[\ell]$.

Exemples :

1. Pour $u \in \mathbb{F}_{\ell^2}^*$: si $\mathrm{ord}(u)$ est pair, alors $s(u) = \frac{1}{2}\mathrm{ord}(u)$, sinon $s(u) = \mathrm{ord}(u)$.
2. π_ℓ est d'ordre fini dans $\mathrm{End}(E[\ell])$ car $\pi_\ell^2 - \tau\pi_\ell + k = 0$, avec $k \neq 0$, sur $E[\ell]$; $s(\pi_\ell)$ est le plus petit entier n tel que : $\forall P \in E[\ell]\ \pi_\ell^n(P) = \pm P$. A noter que dans $\mathrm{End}(E[\ell])$, il y a des diviseurs de zéro : par exemple si $\pi_{11}^2 = 3\mathrm{Id}$, on a $\pi_{11}^{10} = \mathrm{Id}$ mais $\pi_{11}^5 \neq \pm\mathrm{Id}$.
3. On définit, également, pour $P \in E[\ell]$, $s_P(\pi_\ell)$ comme étant le plus petit entier n tel que $\pi_\ell^n(P) = \pm P$.

On note α et β les racines de $x^2 - \tau x + k = 0$ dans $\mathbb{F}_{\ell^2}$. λ représentera l'une ou l'autre de ces racines.

On considère $E[\ell]$ comme un espace vectoriel de dimension 2 sur $\mathbb{F}_\ell$ et π_ℓ, la restriction de π à $E[\ell]$, comme une transformation linéaire de $\mathbb{F}_\ell^2$. Son équation caractéristique est $\pi_\ell^2 - \tau\pi_\ell + k = 0$ avec $\tau \equiv t \bmod \ell$ et $k \equiv q \bmod \ell$. On note $E[\ell]_\lambda$ le sous-espace propre associé à λ.

Pour α et β dans $\mathbb{F}_\ell$, on pose $s(\alpha,\beta) = \mathrm{ppcm}(s(\alpha), s(\beta))$ si α et β ont des ordres qui contiennent la même puissance non nulle de 2 et $s(\alpha,\beta) = \mathrm{ppcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$ sinon. On rappelle que e représente l'ordre entier modulo ℓ de $x^2 - \tau x + k$ et ω est tel que $x^e \equiv \omega \bmod (\ell, x^2 - \tau x + k)$.

Remarque 4 *Considérons la slr2 u_n dans $\mathbb{F}_\ell[\pi_\ell]$ définie par: $u_0(\pi_\ell) = Id$; $u_1(\pi_\ell) = \pi_\ell$ et $u_{n+2}(\pi_\ell) = \tau u_{n+1}(\pi_\ell) - k u_n(\pi_\ell)$. Son discriminant est $D = \tau^2 - 4k$.*

Si $(\frac{D}{\ell}) \neq 0$ alors $u_n(\pi_\ell) = [(\alpha^n - \beta^n)/(\alpha - \beta)]\pi_\ell + [(\alpha\beta^n - \beta\alpha^n)/(\alpha - \beta)]Id = [U_n]\pi_\ell + [V_n]Id$.

Si $(\frac{D}{\ell}) = 0$ alors $u_n(\pi_\ell) = [n\lambda^{n-1}]\pi_\ell + [(1-n)\lambda^n]Id = [U_n]\pi_\ell + [V_n]Id$.

Lemme 3 *Avec les notations précédentes, on a*

Si $(\frac{D}{\ell}) = 1$, on a $s(\alpha,\beta) = es(w)$.

Si $(\frac{D}{\ell}) = 0$, on a $s(\lambda) = \mathrm{ord}(k)$.

Si $(\frac{D}{\ell}) = -1$, on a $s(\alpha) = s(\beta) = es(w)$.

Démonstration : on a $u_n(x) = x^n$ si $P_1(x) = 0$ donc $u_n(x) \equiv x^n \bmod P_1(x)$.

• Si $(\frac{D}{\ell}) = 1$, on a $u_n(x) = U_n x + V_n \equiv x^n \bmod P_1(x)$ d'où $\alpha^e = \beta^e = w$, ainsi $\alpha^{es(w)} = \beta^{es(w)} = \pm 1$ et l'entier $n = es(w)$ est minimal pour cette double égalité. Si $\alpha^n = \beta^n = 1$, on a $n = \mathrm{ppcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$. Si $\alpha^n = \beta^n = -1$, on a $\alpha^{2n} = \beta^{2n} = 1$

alors $\mathrm{ord}(\alpha)$ et $\mathrm{ord}(\beta)$ sont pairs et $n = s(\alpha)\delta = s(\beta)\tilde{\delta}$ avec δ et $\tilde{\delta}$ impairs. On a $n = \mathrm{ppcm}(s(\alpha), s(\beta))$. De plus, si $s(\alpha) = 2^{\mu}r$ et $s(\beta) = 2^{\tilde{\mu}}s$ avec r et s impairs alors $\mu = \tilde{\mu}$. Ce cas ne survient, donc, que si α et β ont des ordres contenant la même puissance non nulle de 2.

- Si $(\frac{D}{\ell}) = 0$, on a $\lambda^2 = k$ d'où le résultat.
- Si $(\frac{D}{\ell}) = -1$, $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$ dans $\mathbb{F}_{\ell^2}^*$. On en déduit $s(\alpha) = s(\beta) = es(w)$. □

Proposition 10 *Soit π_ℓ la restriction de l'endomorphisme de Frobenius π, d'une courbe elliptique E, au sous-groupe de ℓ-torsion $E[\ell]$ et soit $P \in E[\ell]$.*

Si $(\frac{D}{\ell}) = 1$ et si $P \in E[\ell]_\lambda$, alors $s_P(\pi_\ell) = s(\lambda)$,
si $P \notin E[\ell]_\lambda$, alors $s_P(\pi_\ell) = s(\alpha, \beta)$.
On a, dans ce cas, $s(\pi_\ell) = s(\alpha, \beta)$.
Si $(\frac{D}{\ell}) = 0$ et si $P \in E[\ell]_\lambda$, alors $s_P(\pi_\ell) = \mathrm{ord}(k)$,
si $P \notin E[\ell]_\lambda$, alors $s_P(\pi_\ell) = \mathrm{ord}(k)\ell$.
On a, dans ce cas, $s(\pi_\ell) = \mathrm{ord}(k)\ell$ si $\dim(E[\ell]_\lambda) = 1$ et
$s(\pi_\ell) = \mathrm{ord}(k)$ si $\dim(E[\ell]_\lambda) = 2$.
Si $(\frac{D}{\ell}) = -1$, alors $\forall P \in E[\ell]$ on a $s_P(\pi_\ell) = s(\lambda)$.
On a, dans ce cas, $s(\pi_\ell) = s(\lambda)$.

Démonstration : • Si $(\frac{D}{\ell}) = 1$ et si $P \in E[\ell]_\lambda$, alors $\pi_\ell(P) = [\lambda]P$ donc $\pi_\ell^{s(\lambda)}(P) = \pm P$ ainsi $s_P(\pi_\ell) = s(\lambda)$. Si $P \notin E[\ell]_\lambda$, alors, puisque $\pi_\ell^n(P) = u_n(\pi_\ell(P)) = [U_n]\pi_\ell(P) + [V_n]P$, si $n = s_P(\pi_\ell)$, on a $\alpha^n = \beta^n = \pm 1$ car $P \notin E[\ell]_\lambda$. Du lemme $s_P(\pi_\ell) = s(\alpha, \beta)$.

• Si $(\frac{D}{\ell}) = 0$ et si $P \in E[\ell]_\lambda$, alors $\pi_\ell(P) = [\lambda]P$ d'où $s_P(\pi_\ell) = s(\lambda) = \mathrm{ord}(k)$. Si $P \notin E[\ell]_\lambda$, alors, puisque $\pi_\ell^n(P) = [U_n]\pi_\ell(P) + [V_n]P$, si $n = s_P(\pi_\ell)$, alors on a immédiatement $n = \mathrm{ord}(k)\ell$.

• Si $(\frac{D}{\ell}) = -1$ on a, $\forall P \in E[\ell]$, $\pi_\ell^n(P) = [U_n]\pi_\ell(P) + [V_n]P$, donc $s_P(\pi_\ell) = s(\lambda)$. □

Remarque 5 $\forall P \in E[\ell]$, $s_P(\pi_\ell) \mid s(\pi_\ell)$.

1.3 Polynômes de division f_n de E

1.3.1 Définition et propriétés

Soit n un entier quelconque, alors [40]

$$[n](X, Y) = (X_n, Y_n) = \left(\frac{\phi_n(X, Y)}{\psi_n^2(X, Y)}, \frac{w_n(X, Y)}{\psi_n^3(X, Y)}\right)$$

où $\phi_n(X, Y)$, $\psi_n(X, Y)$, $w_n(X, Y)$ sont des polynômes dans $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X, Y]$. Les polynômes $\psi_n(X, Y)$, appelés polynômes de Weber, sont définis par les relations suivantes :

$\psi_{-1}(X, Y) = -1$; $\psi_0(X, Y) = 0$; $\psi_1(X, Y) = 1$; $\psi_2(X, Y) = 2Y + a_1X + a_3$;

$\psi_3(X, Y) = 3X^4 + b_2X^3 + 4b_4X^2 + 3b_6X + b_8$;

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

et

$\psi_2\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$; $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$.

Les polynômes w_n et ϕ_n satisfont $\phi_n = X\psi_n^2 - \psi_{n-1}\psi_{n+1}$ et si $p \neq 2$ on a $w_n = \frac{\psi_{2n}}{2\psi_n} - \frac{1}{2}\psi_n(a_1\phi_n + a_3\psi_n^2)$.

Soit $\psi_n'(X)$ représentant $\psi_n(X,Y)$ dans $\mathbb{F}_q[X,Y]/(\mathcal{F}(X,Y,1))$. Quand n est pair on pose $f_n = \psi_n'/(2Y + a_1X + a_3)$ qui est un polynôme de degré $\frac{n^2-4}{2}$ et lorsque n est impair on pose $f_n = \psi_n'$ qui est de degré $\frac{n^2-1}{2}$. Les polynômes f_n sont les polynômes de division de E.

Proposition 11 *Soit $P = (x,y) \in E(\bar{\mathbb{F}}_q)$.*

$$P \in E[n] \Leftrightarrow \psi_n(x,y) = 0.$$

Démonstration : On démontre par récurrence sur r l'équivalence suivante

$$p \mid \psi_r(x,y) \Leftrightarrow p \mid x_r \quad \text{et} \quad p \nmid y_r.$$

• Pour $r = 2$, si $p \mid 2y + a_1x + a_3$ alors $y \equiv -y - a_1x - a_3 \bmod p$ ainsi $[2]P = (x,y) \oplus (x, -y - a_1x - a_3) = O_E$. Réciproquement, si $p \mid x_2$ et $p \nmid y_2$ alors $[2]P = O_E$ donc $P = -P$ ainsi $2y + a_1x + a_3 \equiv 0 \bmod p$.

• Pour $r = 2n$ pair, on utilise égalité $\psi_{2n} = \psi_n^4(2y_n + a_1x_n + a_3)$. Si $p \mid \psi_{2n}(x)$ alors si $p \mid \psi_n$ alors $p \mid x_n$ et $p \nmid y_n$ donc $[n]P = O_E$ et $[2n]P = O_E$. Si $p \nmid \psi_n$ alors $p \mid 2y_n + a_1x_n + a_3$ donc $y_n \equiv -y_n - a_1x_n - a_3$. Réciproquement, si $p \mid x_n$ et $p \nmid y_n$ alors $[2n]P = O_E$ d'où $2y_n + a_1x_n + a_3 \equiv 0 \bmod p$ donc $p \mid \psi_{2n}$.

• Pour $r = 2n + 1$ impair, on utilise l'égalité $\psi_n^2\psi_{n+1}^2(x_n - x_{n+1}) = \psi_{2n+1}$. Si $p \mid \psi_n^2\psi_{n+1}^2(x_n - x_{n+1})$ alors si $p \mid \psi_n$ alors $p \mid \psi_{n+1}$ ou $p \mid \psi_{n-1}$ ce qui conduit à $P = O_E$. De même si $p \mid \psi_{n+1}$ donc $p \mid x_n - x_{n+1}$. Ainsi $p \mid y_{n+1}^2 - y_n^2$ mais le cas $p \mid y_{n+1} - y_n$ entraine $[n+1]P = [n]P$ donc $p \mid y_{n+1} + y_n$ d'où $[n+1]P = -[n]P$. Réciproquement, si $p \mid x_{2n+1}$ et $p \nmid y_{2n+1}$, on a $[n+1]P = -[n]P$ ainsi $x_{n+1} - x_n \equiv 0 \bmod p$ d'où $p \mid f_{2n+1}$. □

Remarque 6 *Si E est une courbe elliptique dont une équation est $Y^2 = X^3 + AX + B$, avec A et B dans $\mathbb{Z}$, alors pour $n > 2$, les polynômes de division f_n de E ont des racines simples.*

Plus précisement, on a :

Théorème 3 *Avec les notations de la remarque précédente, le discriminant du n-ième polynôme de division f_n est donné par:*

$$\mathrm{Disc}(f_n) = C_n(4A^3 + 27B^2)^{\upsilon(\upsilon-1)/6}$$

avec $\upsilon = \deg(f_n)$ et C_n une constante entière non nulle ne dépendant que de n.

Démonstration: On peut poser $f_n(X) = s_0X^v - s_1X^{v-1} + \cdots + (-1)^v s_v$ avec

$$s_i = s_i(A,B) = \sum_{2u+3v=i} c_{uv}A^uB^v.$$

Si on attribue le poids 2 à x, 4 à A et 6 à B, alors le polynôme f_n est homogène de poids $2(v-i)+2i = 2v$. Ainsi $\mathrm{Res}(f_n, f_n')$ est un polynôme homogène dont on peut calculer le poids en considérant le produit des éléments diagonaux du déterminant. Ce terme est égal à $s_0^{v-1}((-1)^{v-1}s_{v-1})^v$, donc le poids de $\mathrm{Res}(f_n, f_n')$ est $2v(v-1) = h$. Si n est impair, on a $v = (n^2-1)/2$ et $h = (n^2-1)(n^2-3)/2$. On en déduit facilement que $h \equiv 0 \bmod 12$. De même lorsque n est pair.

D'autre part, sur $\mathbb{C}$, il existe z tel que $A = -3E_4(z)$ et $B = -2E_6(z)$. De plus $(E_4^3 - E_6^2)/1728$ est une forme parabolique de poids 12 pour $SL_2(\mathbb{Z})$, égale à $q\prod_{n=1}^{\infty}(1-q^n)$ et qui ne s'annule pas au point z puisque les coefficients A et B sont donnés tels que $4A^3 + 27B^2 \neq 0$ (en d'autres termes, z ne peut être à l'infini). Or les formes modulaires de poids zéro pour $SL_2(\mathbb{Z})$ sont les constantes, par conséquent, on a

$$\mathrm{Disc}(f_n(z)) = D_n\left(\frac{E_4^3(z) - E_6^2(z)}{1728}\right)^{h/12},$$

pour $z \in \mathcal{H}$, avec D_n une constante entière ne dépendant que de n.

On obtient alors $\mathrm{Disc}(f_n) = -D_n((4A^3+27B^2)/2^83^6)^{(h/12)}$, mais puisque $f_n \in \mathbb{Z}[A,B,X]$, on a $\mathrm{Disc}(f_n) = C_n(4A^3+27B^2)^{(h/12)}$ avec C_n une constante rationnelle non nulle dont le dénominateur doit diviser 2 et 3 comme on peut le constater en considérant le premier et dernier terme du développement de $(4A^3+27B^2)^{(h/12)}$, C_n est donc une constante entière non nulle. □

Remarque 7 *Le résultat précédent reste valable pour les courbes elliptiques définies sur $\mathbb{F}_q$ de caractéristique p pour $p \neq 2,3$, à condition de supposer $n > 2$ et n non multiple de p. En effet, puisque $f_{\mu p}' \equiv 0 \bmod p$, on a $C_{\mu p} \equiv 0 \bmod p$.*

1.3.2 Décomposition des polynômes f_ℓ

La remarque suivante nous montre l'utilité de la notion du semi-ordre.

Remarque 8 *S'il existe $P = (x_0, y_0) \in E[\ell]^*$ tel que $s_P(\pi_\ell) = s < (\ell^2-1)/2$, alors, par définition de s_P, on a $\pi_\ell^s(x_0,y_0) = \pm(x_0,y_0)$, ainsi $x_0^{q^s} = x_0$, donc $x_0 \in \mathbb{F}_{q^s}$ et $\notin \mathbb{F}_{q^{s'}}$, avec s' un diviseur de s, car s est minimal pour la relation précédente. On en déduit que le polynôme minimal, $Irred_{\mathbb{F}_q}(x_0) = \prod_{i=0}^{s-1}(x - x_0^{q^i})$, de x_0 sur $\mathbb{F}_q$, est un facteur irréductible, sur $\mathbb{F}_q$, du polynôme de division f_ℓ.*

Proposition 12 *Avec les notations du chapitre, on a:*

f_ℓ est irréductible sur $\mathbb{F}_q$ si et seulement si $P_1(x) = x^2 - \tau x + k$ est un polynôme primitif de $\mathbb{F}_\ell[x]$.

Démonstration : Si f_ℓ est irréductible sur $\mathbb{F}_q$, on a $(\frac{D}{\ell}) = -1$. $P_1(x)$ est donc irréductible sur $\mathbb{F}_\ell$. D'autre part, on a $s(\pi_\ell) = (\ell^2 - 1)/2 = s(\lambda)$.

Si $x^2 - \tau x + k$ est primitif, alors $(\frac{D}{\ell}) = -1$ et $\forall P \in E[\ell]$, $s_P(\pi_\ell) = s(\lambda) = (\ell^2 - 1)/2$ donc f_ℓ est irréductible, car sinon les points P, dont les abscisses seraient racines d'un facteur de degré d de f_ℓ, vérifieraient $s_P(\pi_\ell) \leq d \leq \frac{\ell^2-1}{2}$. □

Corollaire 2 *Si k n'est pas une racine primitive modulo ℓ alors le polynôme de division f_ℓ est réductible sur $\mathbb{F}_q$.*

Démonstration : On utilise la condition nécessaire et suffisante pour avoir un polynôme primitif. □

On décrit, maintenant, la forme de la décomposition en facteurs irréductibles des f_ℓ. Pour cela, on pose, si α et $\beta \in \mathbb{F}_\ell$, $s(\alpha)n = \frac{\ell-1}{2}$ et $s(\beta)m = \frac{\ell-1}{2}$, et si $\lambda \in \mathbb{F}_{\ell^2}$, $s(\lambda)n = \frac{\ell^2-1}{2}$. Puis, $\tilde{n}e = \ell - 1$ ou $\tilde{n}e = \ell + 1$ suivant les cas, et $s(w)\delta = \frac{\ell-1}{2}$.

Proposition 13 *Avec les notations introduites, on a :*

Si $(\frac{D}{\ell}) = 1$, *alors* $f_\ell = (n * s(\alpha), m * s(\beta), \tilde{n}\delta * s(\alpha, \beta))$.

Si $(\frac{D}{\ell}) = 0$ *et si* $\dim(E[\ell]_\lambda) = 2$, *alors* $f_\ell = ((\ell + 1)n * \mathrm{ord}(k))$,

et si $\dim(E[\ell]_\lambda) = 1$, *alors* $f_\ell = (n * \mathrm{ord}(k)\ell, n * \mathrm{ord}(k))$.

Si $(\frac{D}{\ell}) = -1$, *alors* $f_\ell = (n * s(\lambda)) = (\tilde{n}\delta * s(\lambda))$.

Démonstration : • Si $(\frac{D}{\ell}) = 1$, alors π_ℓ a deux valeurs propres α et β dans $\mathbb{F}_\ell$ et $E[\ell] = E[\ell]_\alpha \oplus E[\ell]_\beta = \langle P \rangle \oplus \langle Q \rangle$. Soit $R \in E[\ell]$.

Si $R \in E[\ell]_\lambda$, alors $s_R(\pi_\ell) = s(\lambda)$. On a donc n (resp.m) facteurs de degré $s(\alpha)$ (resp.$s(\beta)$) dont les racines sont les abscisses des points de $E[\ell]_\alpha$ (resp.$E[\ell]_\beta$).

Si $R \notin E[\ell]_\lambda$, alors $s_R(\pi_\ell) = s(\alpha, \beta) = es(w)$ et $es(w)\tilde{n}\delta = \frac{\ell^2-1}{2} - (\ell - 1)$. On obtient $\tilde{n}\delta$ facteurs de degré $s(\alpha, \beta)$ dont les racines sont les abscisses des points $R = [\eta]P + [\mu]Q$ avec $\eta\mu \neq 0$.

• Si $(\frac{D}{\ell}) = 0$, alors on a une valeur propre double $\alpha = \beta = \lambda$. Soit $R \in E[\ell]$.

Si $\dim E[\ell]_\lambda = 2$, alors $E[\ell] = E[\ell]_\lambda \ni R$ donc $s_R(\pi_\ell) = s(\lambda) = \mathrm{ord}(k)$ et $s(\lambda)n = (\ell - 1)/2$. On a donc $(\ell + 1)n$ facteurs de degré $\mathrm{ord}(k)$ dont les racines sont les abscisses des points $R, [\lambda]R, [\lambda^2]R, \ldots, [\lambda^{s(\lambda-1)}]R$.

Si $\dim E[\ell]_\lambda = 1$, alors $E[\ell] = E[\ell]_\lambda \oplus K$ avec $\dim(K) = 1$.

Si $R \in E[\ell]_\lambda$, on a $s_R(\pi_\ell) = \mathrm{ord}(k)$ d'où f_ℓ possède n facteurs irréductibles de degré $\mathrm{ord}(k)$ de f_ℓ.

Si $R \notin E[\ell]_\lambda$, alors $s_R(\pi_\ell) = \mathrm{ord}(k)\ell$ et les abscisses de ces points sont racines de n facteurs irréductibles de degré $\mathrm{ord}(k)\ell$. (On obtient bien n facteurs puisque $((\frac{\ell^2-1}{2} - \frac{\ell-1}{2})/(\mathrm{ord}(k)\ell) = n)$.

• Si $(\frac{D}{\ell}) = -1$, on sait que $\forall R \in E[\ell]$ $s_R(\pi_\ell) = s(\lambda)$, alors f_ℓ se décompose en n facteurs de degré $s(\lambda)$. □

Exemples :

1. La courbe elliptique d'équation $y^2 = x^3 + 102x + 14$ dans $\mathbb{F}_{233}$ a un endomorphisme de Frobenius dont la trace t vérifie $t \bmod 5 \equiv 1$, on a donc $\pi_5^2 - \pi_5 + 3 = (\pi_5 - 2)(\pi_5 - 3)$, d'où $\alpha = 2$ et $\beta = 4$ et $s(2) = 2$, $s(4) = 1$, $s(2,4) = 4$, ainsi $f_5 = (1, 1, 2, 4, 4)$.

2. La courbe elliptique d'équation $y^2 = x^3 + 42x + 68$ dans $\mathbb{F}_{223}$ est telle que $t \bmod 7 \equiv 4$. On a $\pi_7^2 - 4\pi_7 + 6 = 0$ donc $\pi_7^8 = 0$, d'où $f_7 = (8, 8, 8)$.

3. La courbe elliptique d'équation $y^2 = x^3 + 14x + 5$ dans $\mathbb{F}_{131}$ est telle que $t \bmod 5 \equiv 3$. On a $\pi_5^2 - 3\pi_5 + 1 = 0$ donc $(\pi_5 - 4)^2 = 0$, d'où $f_5 = (1, 1, 5, 5)$.

Le résultat qui suit nous sera utile pour introduire les polynômes de semi-division $\mathcal{U}_\ell$.

Proposition 14 *Le polynôme de division $f_\ell(X)$ est irréductible dans $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$.*

Démonstration :

• Si $k \equiv q \bmod \ell$ est une racine primitive modulo ℓ, alors on peut trouver un $a \in \mathbb{F}_\ell$ tel que le polynôme $x^2 - ax + k$ soit primitif dans $\mathbb{F}_\ell[X]$. Or il existe une courbe elliptique E tel que $\mathrm{tr}(\pi_\ell) = a$ et le polynôme f_ℓ de E est irréductible sur $\mathbb{F}_q$.

• Si k n'est pas une racine primitive modulo ℓ.

(a) Supposons $(\frac{k}{\ell}) = -1$. On peut trouver τ_1 dans $\mathbb{F}_\ell$ tel que $x^2 - \tau_1 x + k$ soit irréductible sur $\mathbb{F}_\ell$ et d'ordre entier $\ell + 1$ modulo ℓ (il en existe $\varphi(\ell + 1)$ [4]). D'autre part, il existe une courbe elliptique E_1 telle que $\mathrm{tr}(\pi_\ell) = \tau_1$. Le polynôme de division f_ℓ de E_1 se décompose en $(\ell - 1)/(2s(k))$ facteurs de degré $s(k)(\ell + 1)$. On peut trouver τ_2 dans $\mathbb{F}_\ell$ tel que $x^2 - \tau_2 x + k$ soit réductible sur $\mathbb{F}_\ell$ mais non-carré parfait et dont l'ordre entier modulo ℓ est $\ell - 1$ (il en existe $\varphi(\ell - 1)$ [4]). Parmi ces valeurs, on choisit τ_2 tel que les racines de $x^2 - \tau_2 x + k = 0$, notées α et β, vérifient $\mathrm{ord}(\alpha) = \ell - 1$ et $\mathrm{ord}(\beta) = (\ell - 1)/2$. Pour une courbe elliptique E_2 dont la trace du Frobenius est τ_2 le polynôme de division f_ℓ se décompose sur $\mathbb{F}_q$ comme suit : si $\ell \equiv 3 \bmod 4$ on a

$$f_\ell = ((\ell - 1)/2, (\ell - 1)/2, (\ell - 1)/2 * (\ell - 1))$$

et si $\ell \equiv 1 \bmod 4$ on a

$$f_\ell = ((\ell - 1)/2, 2 * (\ell - 1)/4, (\ell - 1)/2 * (\ell - 1)).$$

Si l'on veut trouver une décomposition sur $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$ contenant les décompositions de $f_\ell^{E_1}$ et $f_\ell^{E_2}$, il faut prendre une décomposition contenant un facteur de degré $\mathrm{ppcm}(\ell - 1, \ell + 1) = (\ell^2 - 1)/2 = \deg(f_\ell)$, d'où le résultat.

(b) Supposons $(\frac{k}{\ell}) = 1$. On doit ici décomposer en deux sous-cas.

(i) Si $\ell \equiv 3 \bmod 4$ alors pour $k = 1$ on considère les décompositions, sur $\mathbb{F}_q$, de f_ℓ suivantes :

$$((\ell - 1)/2 * \ell, (\ell - 1)/2 * 1) \text{ et } ((\ell + 1) * (\ell - 1)/2).$$

Cela donne une décomposition

$$(\ell((\ell - 1)/2), (\ell - 1)/2)$$

et en considérant la décomposition $(2, 2, \ldots, 2)$ obtenue pour une courbe supersingulière, on en déduit le résultat pour ce cas. Pour les autres valeurs de k on considère les décompositions suivantes :

$$(n_1 * (\ell \mathrm{ord}(k)), n_1 * \mathrm{ord}(k)) \text{ si } (\frac{D}{\ell}) = 0, \text{ et } (n * s(\lambda)) \text{ si } (\frac{D}{\ell}) = -1$$

avec $n = 2n_1$. Cela donne une décomposition possible de f_ℓ de la forme

$$(n_1 * \mathrm{ord}(k)(\ell + 1)).$$

En considérant la décomposition possible suivante $((\ell+1)*((\ell-1)/2))$ (utile si $\mathrm{ord}(k) \neq d$) dans le cas $(\frac{D}{\ell}) = 1$, on obtient le résultat escompté puisque $\mathrm{ppcm}((\frac{\ell-1}{2}), \mathrm{ord}(k)(\ell+1)) = \deg(f_\ell)$ si $\ell \equiv 3 \bmod 4$.

(ii) Si $\ell \equiv 1 \bmod 4$, alors le ppcm précédent est égal à $\deg(f_\ell)/2$ et donc on obtient une décomposition possible de f_ℓ sur $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$ en 2 facteurs irréductibles. Mais, la décomposition $(n_1*(\ell \mathrm{ord}(k)), n_1*\mathrm{ord}(k))$ dans le cas où le discriminant est nul modulo ℓ et le fait que l'action du Frobenius permute les points de la droite rationnelle et change de droite les autres points montre que la réductibilité de $f_\ell(a_1, \ldots, a_6)$ en deux facteurs est impossible. □

1.3.3 Polynômes de division exacte de E

On peut définir des polynômes $\mathtt{f}_n$ dont les zéros sont les abscisses des points d'ordre égal à n. On définit au préalable l'ensemble D_k des i tels que :

1. si k est pair alors $i \mid k$, $i \neq k$, $i \nmid (k/2)$
   (a) et si $k/2 \equiv 1, 3 \bmod 4$ alors $i \neq 2$,
   (b) et si $k/2 \equiv 2 \bmod 4$ alors $i \neq 4$,
2. si k est impair $i \mid k$, $i \neq k$ et si $(k-1)/2 \equiv 1 \bmod 3$, alors $i \neq 3$.

On considère la récurrence suivante :
$\mathtt{f}_1 = 1$; $\mathtt{f}_2 = 2Y + a_1X + a_3$; $\mathtt{f}_3 = 3X^4 + b_2X^3 + 4b_4X^2 + 3b_6X + b_8$,
$\mathtt{f}_4 = (2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)$,
et
$\mathtt{f}_{2n} = (\prod_{i|n+2} \mathtt{f}_i \prod_{i|n-1} \mathtt{f}_i^2 - \prod_{i|n-2} \mathtt{f}_i \prod_{i|n+1} \mathtt{f}_i^2)_{i \nmid 2n} / \prod_{i \in D_{2n}} \mathtt{f}_i$,
$\mathtt{f}_{2n+1} = (\prod_{i|n+2} \mathtt{f}_i \prod_{i|n} \mathtt{f}_i^3 - \prod_{i|n-1} \mathtt{f}_i \prod_{i|n+1} \mathtt{f}_i^3)_{i \nmid 2n+1} / \prod_{i \in D_{2n+1}} \mathtt{f}_i$.
Où $(.)_{i \nmid n}$ signifie que tous les produits à l'intérieur de la parenthèse s'étendent sur les indices i ne divisant pas n.
On a, par exemple, $\mathtt{f}_{14} = \mathtt{f}_3\mathtt{f}_9\mathtt{f}_3^2\mathtt{f}_6^2 - \mathtt{f}_5\mathtt{f}_4^2\mathtt{f}_8^2$.
On pose $s_n = \prod_{i|n+2} \mathtt{f}_i \prod_{i|n-1} \mathtt{f}_i^2 - \prod_{i|n-2} \mathtt{f}_i \prod_{i|n+1} \mathtt{f}_i^2$
et $r_n = \prod_{i|n+2} \mathtt{f}_i \prod_{i|n} \mathtt{f}_i^3 - \prod_{i|n-1} \mathtt{f}_i \prod_{i|n+1} \mathtt{f}_i^3$.

Proposition 15 $\psi_n = \prod_{i|n} \mathtt{f}_i$.

Démonstration : On démontre ce résultat par récurrence en supposant la relation vraie jusqu'à l'ordre $n+2$.

• à l'ordre $2n$: on a $\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n-1}^2)/(2y + a_1x + a_3)$ donc par hypothèse $\psi_{2n} = \prod_{i|n} \mathtt{f}_i s_n/\mathtt{f}_2$. Si n est impair, on a $s_n = (s_n)_{i\nmid 2n}\mathtt{f}_2^2$ (avec $(s_n)_{i\nmid 2n}$ signifiant que les produits apparaissant dans la définition de s_n s'étendent sur les indices i ne divisant pas $2n$) ; si n est pair et $\not\equiv 2 \bmod 4$, on a $s_n = (s_n)_{i\nmid 2n}\mathtt{f}_2$ et si $n \equiv 2 \bmod 4$, on a $s_n = (s_n)_{i\nmid 2n}\mathtt{f}_2\mathtt{f}_4$. On en déduit immédiatement que $\psi_{2n} = \prod_{i|2n} \mathtt{f}_i$.

• à l'ordre $2n+1$: Si $n \equiv 1 \bmod 3$, alors $r_n = (r_n)_{i\nmid 2n+1}\mathtt{f}_3$ (avec $(r_n)_{i\nmid 2n+1}$ signifiant que les produits apparaissant dans la définition de r_n s'étendent sur les indices i ne divisant pas $2n+1$), sinon $r_n = (r_n)_{i\nmid 2n+1}$, d'où la conclusion. □

Proposition 16 *Pour $n > 2$ on a $\mathtt{f}_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X]$.*

Démonstration : On a $\mathtt{f}_{2n+1} = (r_n)_{i\nmid 2n+1}/\prod_{i\in D_{2n+1}} \mathtt{f}_i$. Supposons que l'on ait $j \in D_{2n+1}$ tel que $\mathtt{f}_j = 0$, alors $\psi_j = 0$ donc $\psi_{2n+1} = 0 = r_n$. Si $n \not\equiv 1 \bmod 3$, alors $r_n = (r_n)_{i\nmid 2n+1} = 0$ donc $\mathtt{f}_j$ divise le numérateur de $\mathtt{f}_{2n+1}$. Si $n \equiv 1 \bmod 3$, alors $r_n = (r_n)_{i\nmid 2n+1}\mathtt{f}_3 = 0$ et si $\mathtt{f}_3 = 0$, alors $\psi_3 = 0$ et comme j n'est pas un multiple de 3 car sinon ψ_j aurait une racine double on a $(j,3) = 1$ et $\psi_3 = 0 = \psi_j$ ce qui est impossible.

On a $\mathtt{f}_{2n} = (s_n)_{i\nmid 2n}/\prod_{i\in D_{2n}} \mathtt{f}_i$. Supposons que l'on ait $j \in D_{2n}$ tel que $\mathtt{f}_j = 0$, alors $\psi_j = 0$ donc $\psi_{2n} = (\prod_{i|n} \mathtt{f}_i)s_n/\mathtt{f}_2 = 0$. Si n est impair, alors $(\prod_{i|n} \mathtt{f}_i)(s_n)_{i\nmid 2n}\mathtt{f}_2 = 0$. Or $\mathtt{f}_2 \neq 0$ car $\psi_j = \mathtt{f}_2\mathtt{f}_j \prod \mathtt{f}_k$ et les $\mathtt{f}_i$ dans le produit exprimant ψ_{2n} sont tous non nuls car $\mathtt{f}_i = \mathtt{f}_j = 0$ entraine que ψ_{2n} admet une racine double. Les autres cas se résolvent de la même manière. □

Exemple : On a $\mathtt{f}_{15} = \frac{\mathtt{f}_9\mathtt{f}_7^3 - \mathtt{f}_2^4\mathtt{f}_4^3\mathtt{f}_6^3\mathtt{f}_6}{\mathtt{f}_5}$ et $\mathtt{f}_6 = \mathtt{f}_5 - \mathtt{f}_4^2 \equiv -\mathtt{f}_4^2 \bmod \mathtt{f}_5$, $\mathtt{f}_9 = \mathtt{f}_2^4\mathtt{f}_4^3\mathtt{f}_6 - \mathtt{f}_5^3 \equiv \mathtt{f}_2^4\mathtt{f}_4^5 \bmod \mathtt{f}_5$, $\mathtt{f}_8 = \mathtt{f}_3^3\mathtt{f}_6 - \mathtt{f}_5^2 \equiv -\mathtt{f}_3^3\mathtt{f}_4^2 \bmod \mathtt{f}_5$ d'où $\mathtt{f}_9\mathtt{f}_7^3 - \mathtt{f}_2^4\mathtt{f}_4^3\mathtt{f}_8^3\mathtt{f}_6 \equiv \mathtt{f}_2^4\mathtt{f}_4^{11}(\mathtt{f}_2^{12}\mathtt{f}_4^3 - \mathtt{f}_3^9) \bmod \mathtt{f}_5 \equiv 0 \bmod \mathtt{f}_5$. Ces formules permettent de donner une relation polynomiale pour $\mathtt{f}_{15}$ mais ce n'est pas aussi simple dans le cas général, par exemple déjà pour $\mathtt{f}_{21}$ d'où la nécéssité d'un algorithme de simplification du dénominateur, quand il y en a un, de $\mathtt{f}_n$.

Proposition 17 *Le polynôme $\mathtt{f}_n$ est de degré $(\varpi(n)^2-1)/2$ avec $\varpi(n)$ le nombre d'entiers $< n$ et qui ne divisent pas n.*

Démonstration : Il suffit de dénombrer le nombre de points de $E[n]$ qui ne sont pas dans $E[n']$ pour $n' \mid n$. □

Proposition 18 *Le point (x,y) d'une courbe elliptique E est un point d'ordre égal à n si et seulement si $\mathtt{f}_n(x,y) = 0$.*

Démonstration : Soit $P = (x,y)$ un point d'ordre égal à n. Au point (x,y) on a $\psi_n = \prod_{i|n} \mathtt{f}_i = 0$. S'il existe d, diviseur de n, tel que $d \neq n$ et $\mathtt{f}_d(x,y) = 0$, alors $\psi_d(x,y) = 0$ d'où $[d]P = 0_E$ et la contradiction.

Supposons que l'on ait $\mathtt{f}_n(x,y) = 0$ alors $\psi_n(x,y) = 0$ et par conséquent $[n]P = O_E$ avec $P = (x,y)$. Si $[d]P = O_E$ où d est un diviseur de n, alors $\psi_d(x,y) = \prod_{i|d} \mathtt{f}_i(x,y) = 0$ et donc on aurait $\mathtt{f}_j(x,y) = 0$ avec j un diviseur de d. Mais $\mathtt{f}_n(x,y)\mathtt{f}_j(x,y)$ divise $\psi_n(x,y)$ donc ψ_n aurait une racine double (x,y) ce qui est impossible. □

1.4 Polynômes de semi-division et polynômes modulaires

1.4.1 Les polynômes $\mathcal{U}_\ell$ de E

On se réfère à [8] en y apportant des précisions.

On définit dans ce paragraphe d'autres polynômes, notés $\mathcal{U}_\ell$, de la manière suivante: on note $d = (\ell - 1)/2$ et considère les $\ell + 1$ sous-groupes cycliques $G_i = \langle P_i \rangle$ d'ordre ℓ de $E[\ell]$, $i = 0, \ldots, \ell$, et on pose $p_{1,i} = x(P_i) + \ldots + x([d]P_i)$. Les polynômes $\mathcal{U}_\ell$ sont les polynômes de degré $\ell + 1$ qui ont pour racines les $p_{1,i}$ pour $i = 0, \ldots, \ell$.

Plus précisement, soit P un point de ℓ-torsion de E, pour i premier à ℓ, on note $[i]P = (x_i, y_i)$. On a $x_{-i} = x_{i+\ell} = x_i$. D'autre part, on sait maintenant que f_ℓ est irréductible sur $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$, par suite l'extension

$$\mathcal{K} \hookrightarrow \mathcal{K}(x_1),$$

avec $\mathcal{K} = \mathbb{F}_q(a_1, a_2, a_3, a_4, a_6)$, est une extension algébrique de degré $\deg(f_\ell) = (\ell^2 - 1)/2$. Et puisque

$$x_i = x_1 - \frac{\psi_{i-1}(x_1)\psi_{i+1}(x_1)}{\psi_i(x_1)} ,$$

les x_i sont des éléments de $\mathcal{K}(x_1)$.

Considérons, maintenant, pour chaque i premier à ℓ, l'automorphisme v_i de $\mathcal{K}(x_1)$ fixant $\mathcal{K}$ défini comme suit:

$$\begin{aligned} v_i : \mathcal{K}(x_1) &\to \mathcal{K}(x_1) \\ x_1 &\mapsto v_i(x_1) = x_i , \end{aligned}$$

et considérons le sous-groupe engendré par v, noté $\langle v \rangle$, dans $\mathrm{Aut}(\mathcal{K}(x_1))$. On a $v_i \circ v_j = v_{ij}$, ainsi

$$\begin{aligned} \Upsilon : \mathbb{F}_\ell^* &\to \langle v \rangle \\ i &\mapsto v_i \end{aligned}$$

est un homomorphisme de groupe. Le noyau de cet homomorphisme est $\mathrm{Ker}(\Upsilon) = \{\pm 1\}$, donc $\#\langle v \rangle = d$ puisque $\mathbb{F}_\ell^*/\mathrm{Ker}(\Upsilon) \cong \langle v \rangle$. On note L le corps fixe de ce groupe d'automorphismes. L est un sous-corps de $\mathbb{F}_q(x_1)$ d'indice $d = (\ell - 1)/2$ donc une extension de degré $\ell + 1$ de $\mathbb{F}_q$, ainsi

$$L \cong \mathbb{F}_{q^{\ell+1}} .$$

On peut facilement construire des éléments de L. En effet, toute fonction symétrique en $x_1, x_2, \ldots, x_d$ est un élément de L. En particulier, $p_1 = x_1 + x_2 + \cdots + x_d$ et plus généralement $p_k = x_1^k + x_2^k + \cdots + x_d^k$ sont des éléments de L. On note $\mathcal{U}_\ell$ le polynôme minimal de p_1 sur $\mathbb{F}_q$.

On peut consulter [8] pour plus de détails, en particulier il y est démontré que $\mathcal{U}_\ell \in \mathbb{F}_q[X]$ et il y est donné un procédé de construction de ces polynômes dans le cas où la caractéristique du corps est $\neq 2, 3$. On a, par exemple:

$\mathcal{U}_3(X) = X^4 + 2AX^2 + 4BX - A^2/3$;
$\mathcal{U}_5(X) = X^6 + 20AX^4 + 160BX^3 - 80A^2X^2 - 128ABX - 80B^2$;
$\mathcal{U}_7(X) = X^8 + 84AX^6 + 1512BX^5 - 1890A^2X^4 - 9072ABX^3 + 644A^3X^2$
$-21168B^2X^2 + 5832A^2BX - 567A^4$.

On donne, maintenant, la décomposition en facteurs irréductibles sur $\mathbb{F}_q$ des polynômes de semi-division $\mathcal{U}_\ell$.

Proposition 19 *Avec les notations du chapitre, on a:*
Si $(\frac{D}{\ell}) = 1$, *alors* $\mathcal{U}_\ell = (1, 1, \tilde{n} * e)$.
Si $(\frac{D}{\ell}) = 0$ *et si* $\dim E[\ell]_\lambda = 2$, *alors* $\mathcal{U}_\ell = ((\ell+1)n * 1)$,
et si $\dim E[\ell]_\lambda = 1$, *alors* $\mathcal{U}_\ell = (1, \ell)$ $(e = \ell)$.
Si $(\frac{D}{\ell}) = -1$, *alors* $\mathcal{U}_\ell = (\tilde{n} * e)$.

Démonstration : • Si $(\frac{D}{\ell}) = 1$, alors $E[\ell] = E[\ell]_\alpha \oplus E[\ell]_\beta = \langle P \rangle \oplus \langle Q \rangle$.

Considérons la droite $\langle P \rangle$. π_ℓ permute les points de $\langle P \rangle$ car $\pi_\ell(P) = [\alpha]P$. Par suite $p_1 = x(P) + x([2]P) + \ldots + x([d]P)$ est une racine de $\mathcal{U}_\ell$ dans $\mathbb{F}_q$.

De même pour $\langle Q \rangle$, $x(Q) + x([2]Q) + \ldots + x([d]Q)$ est une racine de $\mathcal{U}_\ell$ dans $\mathbb{F}_q$.

Parmi les $\ell - 1$ droites restantes, considérons $\langle [\eta]P + [\mu]Q \rangle$ avec $\eta\mu \neq 0$. On pose $R = [\eta]P + [\mu]Q$. Puisque $\pi_\ell^e(R) = [\alpha^e]R$, π_ℓ^e permute les points de $\langle R \rangle$ et $x_i^{q^e} = x_{i\alpha^e}$, donc $p_1(R)^{q^e} = p_1(R)$ et $p_1(R)$ est une racine d'un facteur irréductible de degré e de $\mathcal{U}_\ell$. Et puisque $\ell - 1 = \tilde{n}e$, $\mathcal{U}_\ell$ possède $\tilde{n}$ facteurs irréductibles de degré e.

• Si $(\frac{D}{\ell}) = 1$, alors on a une valeur propre double λ.

Si $\dim(E[\ell]_\lambda) = 2$, alors $\forall P \in E[\ell]$ on a $\pi_\ell(P) = [\lambda]P$. Chaque droite $\langle P \rangle$ est stable par π_ℓ, ainsi $\mathcal{U}_\ell$ se décompose totalement sur $\mathbb{F}_q$.

Si $\dim(E[\ell]_\lambda) = 1$, $E[\ell] = E[\ell]_\alpha \oplus K = \langle P \rangle \oplus \langle Q \rangle$. $E[\ell]_\lambda = \langle P \rangle$ fournit un facteur linéaire de $\mathcal{U}_\ell$ dont la racine est $p_1(P)$. On considère $R_\mu = [\eta]P + [\mu]Q$ avec $\mu \neq 0$ et comme $e = \ell$ est le plus petit entier n tel que $\pi_\ell^n(R_\mu) \in \langle R_\mu \rangle$, les $p_1(R_\mu)$, pour $\mu = 1, \ldots, \ell$, sont les racines conjuguées d'un facteur irréductible de degré ℓ de $\mathcal{U}_\ell$ sur $\mathbb{F}_q$.

• Si $(\frac{D}{\ell}) = -1$, alors on n'a pas de valeur propre dans $\mathbb{F}_\ell$.

Pour tout $R \in E[\ell]^*$, e est le plus petit entier n tel que $\pi_\ell^n(R) \in \langle R \rangle$ et $\pi_\ell^e(R) = [\alpha^e]R$. On a donc, $\tilde{n}$, où $\tilde{n}e = \ell + 1$, facteurs irréductibles de degré e, dont les racines conjuguées sont $p_1(R), p_1(\pi_\ell(R)), \ldots, p_1(\pi_\ell^{e-1}(R))$, du polynôme $\mathcal{U}_\ell$ sur $\mathbb{F}_q$. □

Exemples :

1. La courbe d'équation $y^2 = x^3 + 41x + 13$ dans $\mathbb{F}_{191}$ est telle que $\mathrm{tr}(\pi) \bmod 7 \equiv 3$, on a donc $\pi_7^2 - 3\pi_7 + 2 = (\pi_7 - 1)(\pi_7 - 2)$ et $\pi_7^3 = \mathrm{Id}$, ainsi $\mathcal{U}_7 = (1, 1, 3, 3)$.
2. La courbe d'équation $y^2 = x^3 + 42x + 68$ dans $\mathbb{F}_{239}$ est telle que $\mathrm{tr}(\pi) \bmod 5 \equiv 4$. On a $\pi_5^2 + \pi_5 + 4 = 0$ $(\pi_5 - 2)^2 = 0$ et $\pi_5^5 = \mathrm{Id}$, d'où $\mathcal{U}_7 = (1, 5)$.
3. La courbe d'équation $y^2 = x^3 + 14x + 5$ dans $\mathbb{F}_{271}$ est telle que $\mathrm{tr}(\pi) \bmod 5 \equiv 4$. On a $\pi_5^2 + \pi_5 + 1 = 0$ et $\pi_5^3 = \mathrm{Id}$, d'où $\mathcal{U}_5 = (3, 3)$.

Proposition 20 *Si* $\mathcal{U}_\ell$ *est réductible sur* $\mathbb{F}_q$, *alors* f_ℓ *est réductible sur* $\mathbb{F}_q$.

Remarque 9 *La réciproque est fausse comme le montre l'exemple de la courbe* $y^2 = x^3 + 32x + 44$ *dans* $\mathbb{F}_{83}$. *On a* $\pi_7^2 + \pi_7 - 1 = 0$, *donc* $\pi_7^8 = -\mathrm{Id}$ *et* $\mathcal{U}_7 = (8)$ *est irréductible, mais* $f_7 = (8,8,8)$ *est réductible.*

Démonstration : Supposons que $\mathcal{U}_\ell$ soit réductible sur $\mathbb{F}_q$. Si $(\frac{D}{\ell}) \neq -1$, alors π_ℓ admet au moins une valeur propre dans $\mathbb{F}_\ell$, donc f_ℓ est réductible sur $\mathbb{F}_q$.

Si $(\frac{D}{\ell}) = -1$, alors $e \neq \ell + 1$ et $P_1(x) = x^2 - \tau x + k$, dont l'ordre entier est e, n'est pas primitif sur $\mathbb{F}_\ell$. Ainsi, f_ℓ est réductible. □

Proposition 21 *Le polynôme* $\mathcal{U}_\ell$ *est irréductible sur* $\mathbb{F}_q[a_1, a_2, a_3, a_4, a_6, X]$.

Démonstration :

Le résultat est immédiat si $k \equiv q \bmod \ell$ est une racine primitive modulo ℓ. Supposons le contraire.

Si $(\frac{k}{\ell}) = 1$, alors on peut choisir une trace de Frobenius de manière à avoir un discriminant nul. Ce qui donne une décomposition de type $\mathcal{U}_\ell = (1, \ell)$. Prenons maintenant une courbe supersingulière on aura $\mathcal{U}_\ell = (2, 2, \ldots, 2)$. D'où la conclusion.

Si $(\frac{k}{\ell}) = -1$, alors on considère une courbe elliptique tel que le Frobenius ait un polynôme caractéristique dont l'ordre entier modulo ℓ soit $\ell + 1$. □

1.4.2 Les polynômes $\Phi_\ell(X, j(E))$

Pour les $j \in \mathbb{F}_q$ la forme de la décomposition des polynômes $\Phi_\ell(X, j(E))$ est donnée par le théorème (6.2) de [36]. On propose une démonstration utilisant l'ordre entier e de la suite de polynôme caractéristique $x^2 - \tau x + k$.

Proposition 22 *Si la courbe elliptique* E *n'est pas supersingulière et si* $J(E) \neq 0$ *et* $J(E) \neq 1728$, *alors le type de décomposition du polynôme modulaire* $\Phi_\ell(X, j(E))$ *est:*

Si $(\frac{D}{\ell}) = 1$, *alors* $\Phi_\ell = (1, 1, \tilde{n} * e)$.

Si $(\frac{D}{\ell}) = 0$ *et si* $\dim(E[\ell]_\lambda) = 2$, *alors* $\Phi_\ell = ((\ell + 1) * 1)$,
et si $\dim(E[\ell]_\lambda) = 1$, *alors* $\Phi_\ell = (1, \ell); (e = \ell)$.

Si $(\frac{D}{\ell}) = -1$, *alors* $\Phi_\ell = (\tilde{n} * e)$.

Démonstration : Si $(\frac{D}{\ell}) = 1$, alors on a deux courbes elliptiques ℓ-isogènes à E définies sur $\mathbb{F}_q$ et $\tilde{n}$ courbes sur $\mathbb{F}_{q^e}$ puisque les noyaux des isogénies correspondantes sont $\mathbb{F}_{q^e}$-rationnels de part la définition de e.

Si $(\frac{D}{\ell}) = 0$, alors ou bien toutes les courbes ℓ-isogènes à E sont définies sur $\mathbb{F}_q$ ou bien une seule.

Si $(\frac{D}{\ell}) = -1$, alors le résultat est immédiat. □

On décrit, maintenant, le lien entre la réductibilité de $\Phi_\ell(j, F)$ et celle de f_ℓ.

Remarque 10 *Si* $\Phi_\ell(j, F)$ *est réductible sur* $\mathbb{F}_q$, *alors* f_ℓ *est réductible sur* $\mathbb{F}_q$.

La réciproque est fausse comme le montre l'exemple de la courbe $y^2 = x^3+32x+44$ *dans* $\mathbb{F}_{83}$. *On a* $\phi_7^2 + \phi_7 - 1 = 0$, *donc* $\phi_7^8 = -\mathrm{Id}$ *et* $\Phi_7 = (8)$ *est irréductible, mais* $f_7 = (8,8,8)$ *est réductible.*

Supposons que $\Phi_\ell(j,F)$ *soit réductible sur* $\mathbb{F}_q$. *Si* $(\frac{D}{\ell}) \neq -1$, *alors* π_ℓ *admet au moins une valeur propre dans* $\mathbb{F}_\ell$, *donc* f_ℓ *est réductible sur* $\mathbb{F}_q$.

Si $(\frac{D}{\ell}) = -1$, *alors* $e \neq \ell+1$ *et* $P_1(x) = x^2 - \tau x + k$, *dont l'ordre entier est* e, *n'est pas primitif sur* $\mathbb{F}_\ell$. *Ainsi,* f_ℓ *est réductible.* □

Remarque 11 *Si* ω *est une racine primitive modulo* ℓ *alors on a l'équivalence suivante :*

Φ_ℓ *est réductible sur* $\mathbb{F}_q$ *si et seulement si* f_ℓ *est réductible sur* $\mathbb{F}_q$.

En effet, supposons que Φ_ℓ *soit irréductible sur* $\mathbb{F}_q$, *alors* $(\frac{D}{\ell}) = -1$ *et* $e = \ell+1$. *De* $e = \ell+1$, *on a* $\omega = k$ *donc* $n = 1$ *et de* ω *primitive, on a* $\delta = 1$.

On en déduit la proposition suivante :

Proposition 23 *Avec* $k \equiv q \bmod \ell$, *on a*

1. *Si* k *est une racine primitive modulo* ℓ, *alors*

   Φ_ℓ *est irréductible sur* $\mathbb{F}_q$ *si et seulement si* f_ℓ *est irréductible sur* $\mathbb{F}_q$.

2. *Si* k *n'est pas une racine primitive modulo* ℓ, *alors*

   si $\Phi_\ell(j(E),X)$ *est irréductible sur* $\mathbb{F}_q$, *alors* f_ℓ *se décompose en* $\frac{\ell-1}{2s(k)}$ *facteurs irréductibles de degré* $(\ell+1)s(k)$.

Chapitre 2

Remarques sur l'algorithme de Schoof-Elkies-Atkin

2.1 Introduction

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de grande caractéristique p. On sait que l'ensemble des points de E, noté $E(\bar{\mathbb{F}}_q)$, est un groupe abelien fini. Pour tout sous-corps K de $\bar{\mathbb{F}}_q$, $E(K)$ est un sous-groupe de $E(\bar{\mathbb{F}}_q)$.

On s'intéresse dans ce chapitre à la détermination de l'ordre du sous-groupe fini $E(\mathbb{F}_q)$. Plus précisement, on aborde quelques aspects essentiels du meilleur algorithme connu de calcul de $\#E(\mathbb{F}_q)$, avec $q = p^r$ où p est très grand, à savoir l'algorithme de Schoof-Elkies-Atkin.

En 1985, René Schoof [35] décrivit un algorithme déterministe du calcul de $\sharp E(\mathbb{F}_q)$. La méthode utilise les propriétés de l'endomorphisme de Frobenius π de E. L'endomorphisme π satisfait l'équation $\pi^2 - t\pi + q = 0$ où t est un entier vérifiant $\#E(\mathbb{F}_q) = q + 1 - t$. En utilisant le fait que $| \#E(\mathbb{F}_q) - (q+1) | \leq 2\sqrt{q}$, on calcule $\#E(\mathbb{F}_q)$ modulo ℓ pour de petits nombres premiers ℓ. Pour réussir, la méthode détermine l'équation caractéristique de π agissant sur les points de ℓ-torsion $E[\ell]$ de E, vu comme un espace vectoriel de dimension 2 sur $\mathbb{F}_\ell$. En travaillant sur $E[\ell]$ l'algorithme nécessite de nombreux calculs de congruences modulo les polynômes de divisions f_ℓ de la courbe elliptique E. Cela donne un algorithme polynomial mais le degré élevé, $(\ell^2 - 1)/2$, des f_ℓ rend l'algorithme inefficace lorsque p est très grand.

En 1991, Elkies [17] a apporté une amélioration conséquente qui consiste à travailler dans le noyau d'une isogénie de degré ℓ. Ces noyaux sont les sous-espaces de dimension 1 de $E[\ell]$. Cette idée marche lorsque l'on a une isogénie définie sur le corps de base, c'est à dire, pour à peu prés la moitié des ℓ, appelé nombres *premiers d'Elkies*. Pour un tel ℓ Elkies travaille dans un sous-espace propre lineaire de $E[\ell]$ en calculant un facteur de degré $d = (\ell - 1)/2$ de f_ℓ. Ce facteur est utilisé à la place de f_ℓ dans les congruences polynomiales avec un gain de temps considérable. Cela nous permet de calculer la valeur propre correspondante et donc t mod ℓ.

Atkin [2] quant à lui a donné dès 1986 les premières modifications à l'algorithme de Schoof et a mis au point la méthode *sort and match* utilisée, depuis Elkies, dans le cas où π_ℓ n'admet pas de valeurs propres dans $\mathbb{F}_\ell$ (bad case). Puis, en 1992, il a uniformisé et simplifié la méthode de Elkies (good case) en exhibant une méthode de génération d'une équation Φ_ℓ pour la ℓ-ième courbe modulaire $X_0(\ell)$ (et $X_0(\ell)/W_\ell$) nécessaire à la détermination d'une courbe ℓ-isogène à E. L'algorithme devient, alors, efficace pour des p très grand [3]. L'algorithme ainsi amélioré s'appelle S.E.A pour Schoof-Elkies-Atkin.

Les améliorations apportées récemment ont été décrites dans l'introduction générale.

On commence par décrire l'algorithme SEA. Puis on étudie les différentes méthodes de détermination d'une valeur propre de π_ℓ et on en calcule les temps d'exécution. On accélère la méthode, asymptotiquement la meilleure, du funny baby-step giant-step de Müller, dans certains cas que l'on précise. D'autre part, on présente une extension de la méthode de Elkies aux nombres premiers ℓ restants : ceux qui ne sont pas d'Elkies. On peut alors déterminer explicitement un facteur du polynôme de division f_ℓ même dans le cas où π_ℓ n'a pas de valeurs propres dans $\mathbb{F}_\ell$. On montre ensuite comment réaliser la procédure de Schoof sur les abscisses des points seulement.

Ces résultats ont permis à Francois Morain [8] d'utiliser sa propre implantation de

S.E.A pour le calcul du nombre de points sur $y^2 = x^3 + 4589x + 91228$ modulo un nombre premier record $p = 10^{499} + 153$. Le nombre de points de E modulo p est $p + 1 - t$ avec

$$t = 553171250536065691629765302031848745987239740325468656806599631$$
$$701127413799294574444261156061625865014222379729340531550358993888$$
$$032237207379679849162325347608624510817409606791818935212167258043$$
$$610673320683043495396594922651059440690814986469417896 9.$$

2.2 Algorithme S.E.A

On présente dans ce paragraphe l'algorithme S.E.A [7]. On commence par rappeler brièvement les notions nécessaires concernant les courbes elliptiques [40].

2.2.1 Courbes elliptiques sur un corps fini

Une courbe elliptique E dans $\mathbb{P}^2(\mathbb{F}_q)$ est donnée par une équation générale en coordonnées projectives $[X : Y : Z]$

$$\mathcal{F}(X, Y, Z) := Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) = 0$$

où les a_i sont dans $\mathbb{F}_q$ et de discriminant Δ non nul dans $\mathbb{F}_q$.

L'ensemble $(E(\mathbb{F}_q), \oplus)$ a une structure de groupe abelien et a pour élément neutre $O_E = [0 : 1 : 0]$.

Le sous-groupe de n-torsion, $E[n] = \{P \in E(\bar{\mathbb{F}}_q) \mid [n]P = O_E\}$, peut être représenter par

$$\mathbb{F}_q[X, Y]/(f_n(X), \mathcal{F}(X, Y, 1)).$$

L'endomorphisme de Frobenius π de la courbe E vérifie l'équation

$$\pi^2 - t\pi + q = 0$$

sur $E(\bar{\mathbb{F}}_q)$ avec $t \in \mathbb{Z}$ la trace de π satisfaisant $\mid t \mid < 2\sqrt{q}$. Le cardinal de $E(\mathbb{F}_q)$ est relié à t par la relation $\#E(\mathbb{F}_q) = q + 1 - t$. Quand ℓ est un nombre premier, la restriction π_ℓ de π au groupe $E[\ell]$ vérifie l'équation

$$\pi_\ell^2 - \tau\pi_\ell + k = 0$$

sur $E[\ell]$ avec $t \equiv \tau \bmod \ell$ et $q \equiv k \bmod \ell$. On note α et β les racines dans $\mathbb{F}_{\ell^2}$ de $f(x) = x^2 - \tau x + k = 0$ et $D = \tau^2 - 4k$ le discriminant de f. Maintenant supposons que $\ell \neq p$. Dans ce cas

$$E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

et donc on peut considérer $E[\ell]$ comme un espace vectoriel de dimension 2 sur $\mathbb{F}_\ell$. Le polynôme f est le polynôme caractéristique de π_ℓ et α, β sont les valeurs propres π_ℓ. Lorsque l'on a une valeur propre λ dans $\mathbb{F}_\ell$, on note $E[\ell]_\lambda$ le sous-espace propre correspondant

de π_ℓ. Remarquons que dans ce cas $E[\ell]_\lambda$ est $\mathbb{F}_q$-rationnel. D'autre part, il y a $\ell+1$ sous-groupes cycliques de $E(\bar{\mathbb{F}}_q)$ d'ordre ℓ, que l'on note $G_1, G_2, \ldots, G_{\ell+1}$. Ce sont les sous-espace linéaire du $\mathbb{F}_\ell$-espace $E[\ell]$.

Le cas $\ell = 2$ est un cas pathologique (voir [14]) et donc, dans la suite, on supposera que ℓ est un nombre premier impair.

La courbe E est dites supersingulière si et seulement si $t \equiv 0 \bmod p$. On connaît beaucoup de résultats concernant les courbes elliptiques supersingulières [40] et on suppose que E n'est pas supersingulière.

2.2.2 Isogénie entre courbes elliptiques

Soient E_1 et E_2 deux courbes elliptiques définies sur le même corps K. Une isogénie de E_1 vers E_2 est un morphisme $\varrho : E_1 \to E_2$ défini sur K et qui préserve la structure de groupe. L'ensemble des isogénies $Hom(E_1, E_2)$ possède une structure de groupe abelien. Il existe une dualité naturelle entre $Hom(E_1, E_2)$ et $Hom(E_2, E_1)$ associant à une isogénie $\varrho : E_1 \to E_2$ une isogénie duale $\hat{\varrho} : E_2 \to E_1$ de même degré (disons n) que ϱ avec les propriétés : $\hat{\hat{\varrho}} = \varrho$, $\hat{\varrho} \circ \varrho = [n]_{E_1}$ et $\varrho \circ \hat{\varrho} = [n]_{E_2}$.

On relie les isogénies au groupe de torsion.

Le noyau $\mathrm{Ker}(\varrho)$ d'une isogénie séparable $\varrho : E_1 \to E_2$ est l'ensemble

$$\mathrm{Ker}(\varrho) = \{P \in E_1(K) \mid \varrho(P) = O_{E_2}\}.$$

C'est un sous-groupe de $E_1(\bar{K})$ d'ordre $\deg(\varrho)$ qui est rationnel sur K.

Inversement, tout sous-groupe fini G de $E_1(\bar{K})$ rationnel sur K est le noyau d'une isogénie séparable de degré $\mid G \mid$ de E_1 vers une autre courbe elliptique $E_2 = E_1/G$ définie sur K.

En effet, le noyau donne une bijection entre les classes d'isomorphismes d'isogénies séparable sur K de E_1 vers une autre courbe et les sous-groupes K-rationnels finis de E_1.

Remarque 12 *Si on se place sur le corps fini $\mathbb{F}_q$ alors en utilisant le théorème de Deuring [36] on peut remonter l'isogénie*

$$E(Y^2 = X^3 + AX + B) \to E/G(Y^2 = X^3 + \tilde{A}X + \tilde{B})$$

en caractéristique zéro. Plus précisement, il existe $q = exp(2i\pi z) \in \mathbb{C}$ tel que $E_4(z)$ et $E_6(z)$ soient des entiers dans un corps de nombres et il y a un idéal premier $\mathcal{P}$ de corps résiduel $\mathbb{F}_q$ de l'anneau des entiers de ce corps de nombres et telle que la réduction modulo $\mathcal{P}$ de l'isogénie

$$0 \to \mu_\ell \to \mathbb{C}^*/q^{\mathbb{Z}} \to \mathbb{C}^*/q^{\ell\mathbb{Z}} \to 0$$

donne l'isogénie

$$0 \to G \to E \to E/G \to 0$$

sur $\mathbb{F}_q$. La courbe $\mathbb{C}^*/q^{\mathbb{Z}}$ admet une équation de Weierstrass de la forme

$$Y^2 = X^3 - 3E_4(z)X - 2E_6(z)$$

avec $A \equiv -3E_4(z) \bmod \mathcal{P}$ *et* $B \equiv -2E_6(z) \bmod \mathcal{P}$. *De même* $\mathbb{C}^*/q^{\ell\mathbb{Z}}$ *admet une équation*

$$Y^2 = X^3 - 3\tilde{E}_4(z)X - 2\tilde{E}_6(z)$$

avec $\tilde{A} \equiv -3\tilde{E}_4(z) \bmod \mathcal{P}$ *et* $\tilde{B} \equiv -2\tilde{E}_6(z) \bmod \mathcal{P}$

2.2.3 Calcul d'un facteur h_ℓ de f_ℓ

Depuis le chapitre 1, on sait que l'on dispose d'équations modulaires $\Phi_\ell(J, F)$, de degré $\ell+1$, qui relie l'invariant j d'une courbe elliptique et une fonction F de $\Gamma_0(\ell)$. Le polynôme modulaire Φ_ℓ nous donne une équation de la ℓ^{ieme} courbe modulaire $X_0(\ell)$. Le choix de "bons" polynômes Φ_ℓ est décrit dans [2] et [31]. En fait, il a deux cas: celui où on utilise $X_0(\ell)$ et celui avec $X_0(\ell)/W_\ell$. D'autre part, le calcul de h_ℓ diffère suivant le cas p grand ou p petit.

Atkin [2] a montré comment obtenir, pour un "bon" nombre premier ℓ, un facteur $h_\ell(X) = \prod_{i=1}^{d}(X - x_i)$ de f_ℓ où les x_i sont les abscisses des points du sous-groupe $G = E[\ell]_\lambda$, à partir d'une racine F de $\Phi_\ell(X, J(E)) \equiv 0$ dans $\mathbb{F}_q$ via une courbe ℓ-isogène à E, disons

$$Y^2 = X^3 + \tilde{A}X + \tilde{B},$$

défini sur $\mathbb{F}_q$. En effet, le formulaire de Atkin [2], [31] donne, à partir d'une racine F, les valeurs de $p_1 = \sum_{i=1}^{d} x_i$; $\tilde{A}$; $\tilde{B}$ et nous permet, avec la méthode de Elkies, de calculer les valeurs $p_k = \sum_{i=1}^{d} x_i^k$ pour $1 \leq k \leq d$ et donc un facteur h_ℓ de f_ℓ à l'aide des formules de Newton.

Lorsque $E[\ell]$ possède un sous-groupe $\mathbb{F}_q$-rationnel d'ordre ℓ, noté G, on peut expliciter l'isogénie séparable $\varrho : E \to E/G$ de degré ℓ à l'aide du polynôme h_ℓ de degré $(\ell-1)/2$ dont les racines sont les abscisses des points du noyau $G = \mathrm{Ker}\varrho$. On dira que $\tilde{E}$ est dans la direction λ si l'isogénie entre E et $\tilde{E}$ a pour noyau $E[\ell]_\lambda$.

2.2.4 L'algorithme SEA

L'algorithme original de Schoof détermine $\sharp E(\mathbb{F}_q)$ à partir de la relation $\sharp E(\mathbb{F}_q) = q + 1 - t$, où t est la trace de l'endomorphisme de Frobenius de E, en calculant $t \bmod \ell$ pour les nombres premiers $\ell = 2, 3, \ldots, L$. Puisque $|t| \leq 2\sqrt{q}$, il suffit de prendre L tel que $\prod_{\ell<L} \ell > 4\sqrt{q}$ et le théorème chinois donne la valeur exacte de t. Schoof détermine $t \bmod \ell$ en étudiant l'action de π en tant qu'élément de $GL_2(\mathbb{F}_\ell)$ sur les points de ℓ-torsion.

Pour cela, on détermine quelle relation du type

$$(x^{q^2}, y^{q^2}) \oplus [k](x, y) = [\tilde{\tau}](x^q, y^q) \ , \ 0 \leq \tilde{\tau} \leq \ell - 1 \ .$$

pour $\tilde{\tau} \in \mathbb{F}_\ell$ est vérifiée sur $E[\ell]$. Explicitement, on compare les abscisses des $d = (\ell-1)/2$ premières équations puis les ordonnées pour déterminer le signe de τ lorsque l'on a égalité des abscisses en utilisant les formules d'addition sur une courbe elliptique [9]. A noter que l'on ne peut utiliser les formules de multiplication sur E puisqu'elles nécessitent la connaissance des polynômes de division de E.

• L'idée de Elkies est de considérer un ensemble plus petit que $E[\ell]$, à savoir le noyau de l'une des $\ell+1$ isogénies connues de degré ℓ

$$E \xrightarrow{\varrho_i} E_i, 1 \leq i \leq \ell+1$$

qui sont les espaces linéaires de $E[\ell]$. Cela est possible lorsque D est un carré modulo ℓ. Dans ce cas les valeurs propres α et β sont dans $\mathbb{F}_\ell$ et ℓ est appelé un nombre *premier d'Elkies*. Les sous-espaces propres correspondants sont rationnels sur $\mathbb{F}_q$. Par conséquent, lorsque l'on a deux valeurs propres dans $\mathbb{F}_\ell$ on a deux espaces propres $\mathbb{F}_q$-rationnel et ainsi deux isogènies définies sur $\mathbb{F}_q$. En fait, chaque isogénie correspond à un facteur h_ℓ de degré $d=(\ell-1)/2$, du polynôme de division f_ℓ dans $\mathbb{F}_q[x]$. Soit $E[\ell]_\lambda$ le sous-espace correspondant à la valeur propre λ et P_λ un générateur de $E[\ell]_\lambda$. On a

$$E[\ell]_\lambda = \langle P_\lambda \rangle = \mathbb{F}_q[X,Y]/(h_\ell(X), \mathcal{F}(X,Y,1))$$

avec $h_\ell(X) = \prod_{i=1}^{d}(X - x([i]P_\lambda))$ de degré $d=(\ell-1)/2$.

Soit $X_0(\ell)$ la courbe modulaire et $\Phi_\ell(X,Y)$ son équation canonique. L'existence d'une valeur propre rationnelle λ pour le Frobenius de E entraine l'existence d'un point rationnel sur $X_0(\ell)$ et réciproquement. Ainsi $\Phi_\ell(X, j(E)) = 0$ a une racine dans $\mathbb{F}_q$ si et seulement si ℓ est un nombre *premier d'Elkies*.

On doit calculer h_ℓ à partir de Φ_ℓ. Il y a deux cas.

Si $p \neq 2,3$ et ℓ un nombre premier d'Elkies tel que $\ell \ll p$ on se réfère à Atkin [3]. Atkin montre comment déterminer la courbe ℓ-isogène et l'isogénie et ensuite déduit h_ℓ. Explicitement, on obtient h_ℓ comme il est décrit dans le paragraphe précédent.

Si $p=2$ ou 3 ou $\ell \approx p$, alors on peut consulter les travaux de Couveignes [10] et l'implantation dans [28].

Une fois h_ℓ connu, on doit déterminer quelle relation du type

$$\pi_\ell = \tilde{\lambda}$$

pour $\tilde{\lambda}$ in $\mathbb{F}_\ell$ est satisfaite sur $E[\ell]_\lambda = \mathbb{F}_q[X,Y]/(h_\ell(X), \mathcal{F}(X,Y))$. Explicitement, on cherche une égalité parmi les $\ell-1$ équations

$$(x^q, y^q) = [\tilde{\lambda}](x,y)\ ,\ 1 \leq \tilde{\lambda} \leq \ell-1\ .$$

• Si D n'est pas un carré modulo ℓ alors ℓ est appelé un nombre *premier d'Atkin*. Dans ce cas, les G_i sont $\mathbb{F}_{p^e}$-rationnel où e est le plus petit entier n pour lequel π_ℓ^n est dans $\mathbb{F}_\ell$. L'automorphisme π_ℓ agit sur les G_i également et l'on verra ultérieurement comment obtenir un facteur de f_ℓ dans ce cas à partir de G_i "conjugués".

Atkin détermine, dans ce cas, l'ordre entier e de π_ℓ. La valeur de e est calculée via le type de la décomposition de Φ_ℓ sur $\mathbb{F}_q$. Les valeurs de τ correspondantes vérifient l'équation polynomiales $T_n(v+1/2\tau, -v+1/2\tau)$ de degré $\varphi(e)$ avec $v^2 = (\tau^2-4k)/4 = D/4$ et T_n l'homogénisation du polynôme cyclotomique d'indice n [4]. D'autre part, le résultat $(\frac{k}{\ell}) = (-1)^e$ de la proposition (6.3) de [36] est dejà contenu dans les théorèmes 3 de [4].

Le type de décomposition est la base de la méthode *sort and match* de Atkin [2]. Plutôt que de réaliser les calculs modulo les polynômes de division f_ℓ de degré $(\ell^2-1)/2$,

Atkin travaille avec les polynômes modulaires de degré $\ell + 1$. Cela est beaucoup plus efficace mais on obtient moins d'informations : plutôt que d'avoir $t \bmod \ell$ Atkin obtient certaines informations sur la valeur de $t \bmod \ell$ en calculant le type de décomposition de Φ_ℓ c'est à dire la valeur de e. Ensuite, il utilise un baby-step et giant-step sophistiqué parmi les possibles classes résiduelles. Mais l'algorithme résultant n'est pas un algorithme polynomial.

Schématiquement l'algorithme S.E.A se déroule de la manière suivante :
On calcule le $\text{pgcd}(X^q - X, \Phi_\ell(X, j(E)))$ dans $\mathbb{F}_q[X]$.

- Si deg(pgcd) = 1 ou 2, ℓ est un nombre premier d'Elkies.
  1. On calcule une racine F_λ de ce pgcd.
  2. On détermine les coefficients $\tilde{A}$ et $\tilde{B}$ de la courbe ℓ-isogène à E dans la direction λ et la valeur de p_1 en utilisant le formulaire de [7] (voir annexe).
  3. On calcule un facteur h_ℓ de f_ℓ à partir de la récurrence (R_1) suivante :
$$A - \tilde{A} = 5(6p_2 + 2Ap_0),$$
$$B - \tilde{B} = 7(10p_3 + 6Ap_1 + 4Bp_0)...$$
  4. On détermine une valeur propre de π_ℓ en travaillant modulo le polynôme h_ℓ, ce qui nous donne $t \bmod \ell$.
- Si deg(pgcd) = 0, ℓ est un nombre premier d'Atkin.
  1. On utilise la méthode de Atkin [2].

Pour résumer, on peut décrire les diverses étapes de S.E.A, dans le cas d'un nombre premier ℓ d'Elkies, par la suite

$$\Phi_\ell(X, j(E)) \to F_\lambda \to \{\tilde{A}, \tilde{B}, p_1\} \to p_k \to s_k \to h_l \to \lambda \bmod \ell \to t \bmod \ell.$$

Exemple : On considère la courbe elliptique E d'équation $y^2 = x^3 + 24x + 51$ sur le corps fini $\mathbb{F}_{53}$. Son invariant modulaire est $j = 37$. Le nombre premier $\ell = 7$ est un nombre d'Elkies puisque

$$\Phi_7(F, j(E)) = (32 + F)(41 + F)(27 + 51F + F^2 + F^3)(21 + 11F + 7F^2 + F^3)$$

sur $\mathbb{F}_{53}$. On choisit la racine $F_1 = 12$. Le formulaire d'Atkin nous donne $\tilde{A} = 32$, $\tilde{B} = 51$ et $p_1 = 4$. Ainsi, la courbe d'équation $y^2 = x^3 + 32x + 51$ est 7-isogène à E. Avec les formules d'Elkies, on obtient $p_2 = 4$ et $p_3 = 19$. Ainsi, le polynôme

$$44 + 6x + 49x^2 + x^3$$

est un facteur du polynôme de division f_7^E. Le calcul

$$x^{53} \bmod h_\ell(x) \equiv x$$

nous montre que 1 est une valeur propre du Frobenius de E modulo 7. Cela signifie que le facteur précédent se décompose totalement sur $\mathbb{F}_{53}$:

$$44 + 6x + 49x^2 + x^3 = (x + 12)(x + 40)(x + 50).$$

Puisque $k = 4$, l'autre valeur propre est 4 on en déduit, donc, que $t \bmod 7 \equiv 5$.

On peut obtenir le facteur de degré 3 de f_7^E correspondant à la valeur propre 4 en considérant l'autre racine de Φ_7, à savoir $F_2 = 21$. La courbe 7-isogène obtenue a pour équation $y^2 = x^3 + 46x + 4$ et a un invariant égal a $\tilde{j} = 44$. On trouve

$$26 + 21x + 28x^2 + x^3$$

comme facteur de f_7^E.

Dans le cas d'un nombre premiers d'Elkies, Morain et Couveignes utilisent le schéma précédent avec la courbe isogène obtenue et itèrent le procédé, introduisant, ainsi, une nouvelle notion : celle de cycles d'isogénies rationnelles. Cela permet d'attraper un facteur du polynôme de division f_{ℓ^n} et de l'utiliser pour le calcul de $t \bmod \ell^n$ comme on le verra au chapitre III.

2.3 Recherche d'une valeur propre

Nous sommes ici dans la seconde étape de la méthode de Elkies, à savoir, le polynôme h_ℓ est déjà calculé. Il s'agit maintenant de déterminer une valeur propre de l'automorphisme π_ℓ.

On rappelle les diverses méthodes de détermination d'une valeur propre pour π_ℓ et on les compare en calculant leur complexité.

2.3.1 Complexité

L'opération élémentaire sera ici considérée comme étant la multiplication de deux éléments de $\mathbb{F}_q$.

Arithmétique des polynômes. Soit $M(d)$ le nombre d'opérations nécessaires pour déterminer le produit de deux polynômes de degré d dans $\mathbb{F}_q[x]$. On a $M(d) = O(d^2)$ pour la méthode classique, $M(d) = O(d^{\log_2 3}) = O(d^{1.585})$ avec l'algorithme de Karatsuba et l'utilisation d'une FFT nécessite $M(d) = O(d \log d)$ opérations (voir [20]).

Calcul de $\pi_\ell(x, y)$. Le temps nécessaire pour calculer $x^q \bmod h_\ell(x)$ est $O(M(d) \log q)$ en utilisant la décomposition binaire gauche-droite de q. Pour la détermination de $y^q \bmod h_\ell(x)$ on réalise $O(M(d) \log q)$ opérations également. En effet, si $p > 2$, alors $y^q \equiv \mathcal{G}^{(\frac{q-1}{2})}(x) \bmod h_\ell$ avec $y^2 = \mathcal{G}(x) := x^3 + a_2x^2 + a_4x + a_6$ l'équation de E et si la caractéristique est $p = 2$ on calcule y^q à partir de l'équation de E à savoir $\mathcal{F}(x, y) = 0$.

Comparer les coordonnées de points. Pour calculer une valeur propre il faudra comparer les coordonnées de points de $E[\ell]_\lambda$ ce qui signifie la comparaison de fonctions

rationnelles $\frac{A(x)}{B(x)}$ avec une liste $\frac{C_n(x)}{D_n(x)}$ modulo $h_\ell(x)$ dans $\mathbb{F}_q[x]$. On évite les divisions en testant $A(x)D_n(x) \equiv B(x)C_n(x) \bmod h_\ell(x)$. Ensuite, on utilise une idée de Shoup [33] qui consiste à tester $L(AD_n) = L(BC_n)$ où L est une application linéaire aléatoire. Cela a l'avantage de nous permettre de réaliser les calculs dans $\mathbb{F}_q$ en utilisant la matrice de multiplication par A et B modulo h_ℓ. Cette stratégie coute $O(2d)$ opérations. Lorsque une égalité est trouvée on vérifie que $A(x)D_n(x) \equiv B(x)C_n(x) \bmod h_\ell(x)$. Pour cette stratégie on utilise $O(M(d)) + O(nd)$ opérations.

Calcul de $f \circ g$ mod h. On utilise ici la composition de Brent, Kung [5]. Explicitement, on calcule $f \circ g \bmod h$ en écrivant le polynôme f comme $\sum_{j=0}^{d/T} f_j(x)x^{Tj}$ avec $f_j(x) = \sum_{i=0}^{T} a_{i+Tj}x^i$ où T est un paramétre (voir [39]). Ainsi, on calcule et on stocke $g, g^2, \ldots, g^T$ et on a $f \circ g = f_0(g) + g^T(f_1(g) + g^T(f_2(g) + \cdots))$. La composition modulaire nécessite $O((T + d/T)M(d)) + O(d^2)$ opérations [39].

Recherche de δ tel que $\pi_\ell^\delta = \pm Id$. L'égalité $\pi_\ell^\delta = \pm Id$ sur $E[\ell]_\lambda$ implique $x^{q^\delta} \equiv x \bmod h_\ell(x)$. Soit $r = \lceil\sqrt{d}\rceil$. On peut écrire $\delta = jr - i$ avec i, j deux entiers tels que $0 \leq i, j <\approx r$. On calcule et on stocke $x^q, x^{q^2} = x^q \circ x^q, \ldots, x^{q^r} = x^{q^{r-1}} \circ x^q$ qui a l'avantage de nécessiter que du précalcul de x^{q^i} pour $2 \leq i \leq T$. Ensuite on cherche une égalité avec une puissance $x^{q^{jr}}$ que l'on calcule par composition de x^{q^r} [39]. Quand une égalité est détectée on a $\delta = jr - i$. Ainsi cet algorithme nécessite $O((T + rd/T)M(d)) + O(rd^2)$ opérations. On optimise la valeur de T en prenant $T = \sqrt{rd}$ ce qui donne $O(\sqrt{rd}M(d)) + O(rd^2)$ opérations.

On peut utiliser le fait que δ est un diviseur de d. Ainsi on peut prendre $r = \lceil\sqrt{\overline{d}}\rceil$ avec $\overline{d}$ le plus grand diviseur de d différent de d. De plus, lorsque $\ell \equiv 1 \bmod 4$, on utilise le fait que le nombre $w = (\ell - 1)/(2\delta)$ de facteurs de h_ℓ doit satisfaire $(\frac{\mathcal{D}}{p}) = (-1)^{d-w}$ où $\mathcal{D} = \mathrm{disc}(h_\ell)$ et donc parfois on peut prendre un r encore plus petit et ainsi diminuer le nombre de test.

Remarquons que cette idée peut être utiliser pour la détermination du type de décom-position du polynôme modulaire Φ_ℓ dans le cas où ℓ est un nombre premier d'Atkin.

Calcul de $[n](x, y)$. On peut utiliser les formules d'addition classiques $R = P \oplus Q$ sur E où l'on réalise des multiplications et une division. Les multiplications sont réalisées en $O(M(d))$ opérations et la division, qui est essentiellement un pgcd, en $O(G(d))$ opérations avec $G(d) = d^3$ en utilisant la méthode classique ou $G(d) = M(d)\log^2 d$ si on utilise l'algorithme HGCD de Aho [1]. Ainsi le calcul de $[n]P$ nécessite $O((\log n)M(d)) + O((\log n)G(d))$ opérations et le calculs des $[i]P$ pour $i = 1, \ldots, n$ nécessite $O(nM(d)) + O(nG(d))$ opérations.

Remarquons que l'on a la possibilité d'utiliser la formule de multiplication $x([n]P) = x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}(x, y)$ en calculant les polynômes ψ_i modulo h_ℓ ce qui est réalisable en $O(nM(d))$ opérations. Mais pour se faire on doit réaliser une division ce qui donne asymp-totiquement le même temps que celui obtenu avec les formules d'addition. Néanmoins on peut calculer les $[i]P$ pour $i = 1, \ldots, n$ sous forme de fractions rationnelles en $O(nM(d))$ opérations.

On rappelle briévement maintenant les diverses procédures de calcul d'une valeur

propre du Frobenius. Les écritures en italiques dans les algorithmes renvoient à ce paragraphe sur la complexité.

2.3.2 Méthodes élémentaires

Elkies utilise l'équation

$$(X^q, Y^q) = [\tilde{\lambda}](X, Y)$$

pour $1 \leq \tilde{\lambda} \leq d$ et il compare les abscisses des points puis, lorsque une égalité est obtenu, il teste l'égalité des ordonnées pour déterminer le signe de la valeur propre.

La méthode de Elkies :

1. *Calculer* $x^q \bmod h_\ell(x)$.
2. Pour $\tilde{\lambda} = 1, \ldots$
   (a) *comparer* les abscisses de $\pi_\ell(x, y)$ et $[\tilde{\lambda}](x, y)$,
   (b) si égalité alors $\lambda \equiv \pm\tilde{\lambda} \bmod \ell$.
3. Recherche du signe : *Calculer* $y^q \bmod h_\ell(x)$ et *comparer* avec y_λ.

Ainsi, cette méthode classique de recherche de valeur propre nécessite $O(M(d)\log q) + O(dG(d))$ opérations.

Par la suite Atkin proposa une autre version qui permit d'éviter le calcul de $x^q \bmod h_\ell(x)$. Il considère la même équation mais compare seulement les ordonnées des points et utilise le résultat suivant :

Théorème 4 *(Atkin) On suppose que l'on a trouvé* $\tilde{\lambda}$ *tel que* $Y^q = Y_{\tilde{\lambda}}$. *Alors* $\tilde{\lambda}$ *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* $h_\ell(x)$ *est non nul.*

La méthode de Atkin :

1. *Calculer* $y^q \bmod h_\ell(x)$.
2. Pour $\tilde{\lambda} = 1, \ldots,$
   (a) *comparer* les ordonnées de $\pi_\ell(x, y)$ et $[\tilde{\lambda}](x, y)$,
   (b) si égalité alors $\lambda \equiv \tilde{\lambda} \bmod \ell$.

Cette stratégie permet de gagner un facteur 2 dans la complexité.

On peut gagner encore un peu de temps sur le calcul de la multiplication sur E en utilisant les pas de bébés et les pas de géants de Shanks [38]. Soit $r = \lceil\sqrt{d}\rceil$ alors pour $\tilde{\lambda} \in \mathbb{F}_\ell^*$ on peut écrire $\tilde{\lambda} = i + jr$ avec $0 \leq i, j < r$. On utilise alors l'équation sous la forme

$$(X^p, Y^p) - [i](X, Y) = [j][r](X, Y)$$

et l'avantage de cette stratégie est que les entiers i et j sont petits comparés à ℓ. La méthode compare les ordonnées des points [33].

La méthode de Shanks :

1. Pour $j = 0, \ldots, m$,
   (a) *calculer* $[j][m](x, y)$,
   (b) stocker dans une table $\{j, y_{jm}\}$.
2. Pour $i = 0, \ldots, m-1$,
   (a) *calculer* l'ordonnées de $(x^q, y^q) - i.(x, y)$,
   (b) *chercher* une égalité avec la table,
   (c) si égalité alors $\lambda \equiv i + jm \bmod \ell$.

La méthode nécessite $O(M(d)\log q) + O(\sqrt{d}M(d)) + O(\sqrt{d}G(d))$ opérations.

2.3.3 Vers de meilleures stratégies

La méthode de Atkin :
Atkin a suggéré d'utiliser l'équation $\pi_\ell^i = [j]$ en calculant au préalable le semi-ordre de la valeur propre. On rend l'algorithme plus rapide que celui proposé par Atkin en exhibant un algorithme complexe à partir de cette idée.

Proposition 24 *Soit δ le plus petit entier n tel que $\pi_\ell^n = \pm Id$. Alors, pour un entier j tel que $s(j) = \delta$, il existe un unique entier i tel que*

$$\pi_\ell^i = [j]$$

sur $E[\ell]_\lambda$ avec $(i, \delta) = 1$.

Démonstration : L'entier δ est le semi-ordre de λ puisque

$$(X^{q^\delta}, Y^{q^\delta}) = \lambda^\delta(X, Y) = \pm(X, Y) = (X, \pm Y).$$

D'autre part,l'ensemble S des éléments de même ordre δ que λ est de la forme $S = \{\lambda^i \mid (i, \delta) = 1\}$. Ainsi, pour un j de semi-ordre δ il existe un unique i tel que $\lambda^i \equiv \pm j \bmod \ell$ et $(i, \delta) = 1$. □

On calcule le semi-ordre δ de la valeur propre comme indiqué précédemment avec r un paramétre que l'on fixera par la suite. Puis on détermine le plus petit $j \in \mathbb{F}_\ell^*$ de semi-ordre égal à δ. Maintenant on cherche i tel que $(X^{q^i}, X^{q^i}) = [j](X, Y) = (X_j, X_j)$ modulo $h_\ell(X)$. Ainsi on doit comparer X^{q^i} avec X_j tel que $(i, \delta) = 1$. Puisqu'on n'a seulement que quelques puissances de X^q et X^{q^r} on choisit de procéder de la manière suivante. Si $i \leq r$ alors X^{q^i} est connu. Si $i > r$, soit ξ le plus petit entier tel que $i + \xi r > \delta$. On peut écrire $i + \xi r = \delta + \mu$ avec $\mu < r$. Ainsi, si $X^{q^i} \equiv X_j$ alors $X^{q^{i+\xi r}} \equiv X_j \circ X^{q^{\xi r}}$ et donc $X^{q^\mu} \equiv X_j \circ X^{q^{\xi r}}$. Les X^{q^μ} et $X^{q^{\xi r}}$ sont déjà calculés puisque $\mu < r$ et $\xi r < \delta$.

On doit comparer π_ℓ^μ et $[j] \circ \pi_\ell^{\xi r}$ pour tout μ tel que $0 \leq \mu < r$ et $1 \leq \xi < \delta/r$. Utilisant le fait que

$$X_j = X - \frac{\psi_{j+1}\psi_{j-1}}{\psi_j^2}(X, Y)$$

cela équivaut à tester

$$X^{q^\mu}(H_j \circ X^{q^{\xi r}}) \equiv K_j \circ X^{q^{\xi r}} \bmod h_\ell(X)$$

avec

$$H_j \equiv \psi_j^2 \bmod (h_\ell, \mathcal{F}) \text{ et } K_j \equiv XH_j - \psi_{j+1}\psi_{j-1} \bmod (h_\ell, \mathcal{F}).$$

Cela est réalisé, pour le calcul, en utilisant les formules de récurrences des polynômes de division et, pour la comparaison, en utilisant une application linéaire aléatoire L comme décrit dans la section 3.1.

Plus précisement, on pose $H(X) \equiv X^{q^{\xi r}} \bmod h_\ell(X)$ puis on calcule modulo $h_\ell(X)$ (pour avoir une écriture plus simple, on suppose que $p \neq 2, 3$) :

$P_0(X) = 0$, $P_1(X) = 1$, $P_2(X) = 2$,
$P_3(X) = 3H^4(X) + 6AH^2(X) + 12BH(X) - A^2$,
$P_4(X) = 4(H^6(X) + 5AH^4(X) + 20BH^3(X) - 5A^2H^2(X) - 4ABH(X) - 8B^2 - A^3)$ et
$W(X) = H^3(X) + AH(X) + B$.

On pose alors

$$P_{2n}(X) = P_n(X)(P_{n+2}(X)P_{n-1}^2(X) - P_{n-2}(X)P_{n+1}^2(X))$$

et

$$P_{2n+1}(X) = \begin{cases} W^2(X)P_{n+2}(X)P_n^3(X) - P_{n-1}(X)P_{n+1}^3(X) & \text{si } n \text{ est pair,} \\ P_{n+2}(X)P_n^3(X) - W^2(X)P_{n-1}(X)P_{n+1}^3(X) & \text{sinon.} \end{cases}$$

Cette récurrence est réalisée jusqu'à l'indice j et pour les δ/r valeurs de ξ.

En ce qui concerne le choix du paramétre r, il faut pouvoir écrire $i + \xi r = \delta + \mu$ pour les valeurs de $i > r$ à balayer et on veut que les $x^{q^{\xi r}}$ soient déjà calculés. Pour cela, on prend r solution de l'équation $r^2 + r - \delta = 0$. Dans ce cas, on a $\xi r < \delta - \sqrt{d} < d - \sqrt{d}$.

Remarque 13 *Si on calcule $j(x, y)$ et $j^{-1}(x, y)$ alors on peut restreindre l'ensemble des valeurs i à tester à un ensemble à $\delta/2$ éléments. Dans ce cas, on peut tester seulement les $i \geq d/2$, ce qui donne $\xi r < d - d/2$ mais il faut alors calculer aussi $j^{-1}(x, y)$.*

On résume l'algorithme dans ce qui suit :

1. *Calculer* $x^q \bmod h_\ell(x)$.
2. *Calculer* et stocker $x^{q^i} \equiv x^{q^{(i-1)}} \circ x^q \bmod h_\ell$ pour $2 \leq i \leq r$.
3. (a) Pour $j = 1, 2, \ldots, r$,
   (b) *calculer* $x^{q^{rj}} \equiv x^{q^{r(j-1)}} \circ x^{q^r} \bmod h_\ell$,

(c) *comparer* avec x^{q^j} et si une égalité est trouvée on a δ,

(d) stocker $x^{q^{rj}}$.

4. Calculer le plus petit j dans $\mathbb{F}_\ell^*$ tel que $s(j)$ soit un multiple de δ,

   (a) *Comparer* $K_j(x)$ avec les $x^{q^i} H_j(x)$ pour $1 \leq i \leq r$ et $(i, \delta) = 1$ en utilisant L,

   (b) si une égalité est trouvée on a λ.

5. Pour $\xi = 1, 2, \ldots$

   (a) *Calculer* $H_j(x^{q^{\xi r}})$ et en déduire $K_j(x^{q^{\xi r}})$,

   (b) *tester* $x^{q^\mu} H_j^2(x^{q^{\xi r}}) \equiv K_j(x^{q^{\xi r}}) \bmod h_\ell$ pour les valeurs de μ tels que $0 \leq \mu < r$ et $i + \xi r = \delta + \mu$ avec $(i, \delta) = 1$,

   (c) Si une égalité est détectée, vérifier avec les polynômes et calculer λ ,

   (d) sinon, continuer.

On a :

Proposition 25 *La méthode de Atkin nécessite* $O(M(d)\log q) + O(\sqrt{rd}M(d)) + O(rd^2) + O(d^2)$ *opérations et* $O((2r + R)d)$ *espace mémoire avec* r *racine de* $x^2 + x - d = 0$ *et* $R = \deg(K_j)$.

Démonstration : La méthode réalise $O(M(d)\log q)$ opérations pour le calcul de x^q mod h_ℓ et $O(\sqrt{rd}M(d)) + O(rd^2)$ opérations pour le calcul de δ et $O(M(d)) + O(d^2)$ pour le calcul de i. Pour la place mémoire, on a $2r + R$ polynômes de degré d à stocker. □

Remarque 14 *Le calcul "dominant" dans l'algorithme d'Atkin dépend de la méthode de multiplications de deux polynômes c'est à dire de la taille de* $M(d)$.

Mais l'algorithme ne donne que la valeur propre modulo le signe. Il existe encore une autre méthode qui est, actuellement, la plus rapide asymptotiquement.

La méthode de Müller :

La méthode de Müller [33] consiste en un funny baby-step et giant-step. Explicitement, il existe un entier $k_{opt} \approx \lceil\sqrt{d}\rceil$ tel que pour tout λ dans $\mathbb{F}_\ell^*$ il y ait des entiers i, j avec $1 \leq i, j \leq k_{opt}$ tels que $\lambda \equiv \pm i/j \bmod \ell$. Ainsi Müller utilise l'équation

$$[i](X^q, Y^q) = [j](X, Y).$$

Cette idée nous permet d'utiliser les polynômes de divisions puisque i et j sont petits par rapport à ℓ. Explicitement, on doit trouver i et j tels que

$$X - \frac{\psi_{i+1}\psi_{i-1}}{\psi_i^2}(X, Y) \equiv X^q - \frac{\psi_{j+1}\psi_{j-1}}{\psi_j^2}(X^q, Y^q) \bmod (h_\ell(X), \mathcal{F}(X, Y, 1))$$

que l'on peut écrire sous la forme

$$\frac{A_i(X)}{B_i(X)} \equiv \frac{A_j(X^q)}{B_j(X^q)} \bmod h_\ell(X).$$

En utilisant une application linéaire L on détermine i et j. La méthode évite le calcul des ordonnées et donne deux valeurs possibles de $\lambda \equiv \pm i^{-1}j \bmod \ell$. On a :

1. Pour $j = 1, \ldots, k_{opt}$,
   (a) *calculer* $[j](x, y)$,
   (b) stocker dans une table $\{j, x_j\}$.
2. Pour $i = 0, \ldots, m-1$,
   (a) *calculer* x_i^q en utilisant les formules de récurrences donnant les polynômes de divison,
   (b) *chercher* une égalité avec la table,
   (c) si égalité alors $\lambda \equiv \pm i^{-1}j \bmod \ell$.

Proposition 26 *La méthode de Müller nécessite* $O(M(d)\log q) + O(\sqrt{d}M(d)) + O(d^{5/2})$ *opérations et* $O(d\sqrt{d})$ *espace mémoire.*

Démonstration : On utilise $O(\sqrt{d}M(d))$ opérations pour le calcul des polynômes de divisions. Puis $O(d^{3/4}M(d)) + O(d^{5/2})$ pour la composition par x^q puisque ici le paramétre T est optimal pour $T = \sqrt{2}d^{3/4}$ mais si on utilise la récurrence des polynômes de division cela nécessite $O(\sqrt{d}M(d))$ opérations. Finalement, on utilise $O(M(d)) + O(d^2)$ opérations pour la comparaison des coordonnées. □

On connaît, maintenant, une valeur propre du Frobenius de E modulo le signe. Pour déterminer le signe exacte de la valeur propre, la méthode classique consiste à tester l'équivalence suivante : $Y^q \equiv Y_\lambda \bmod h_\ell(X)$. On présente une solution beaucoup plus rapide pour la détermination du signe de la valeur propre.

2.3.4 Le signe de $\lambda \bmod \ell$

On montre dans ce paragraphe comment éviter le calcul des ordonnées des points dans le cas où f_ℓ a un facteur de degré impair. Les résultats sont valables pour les méthodes de Atkin et Müller mais nous ne donnons les détails que pour la méthode de Müller. On a des entiers i, j tels que $[i]\pi_\ell = \pm[j]$ sur $E[\ell]_\lambda$. Posons $\lambda_0 \equiv ij^{-1} \bmod \ell$ on a $\lambda \equiv \pm\lambda_0 \bmod \ell$.

En caractéristique $p \neq 2$.
Dans ce cas E a une équation de la forme

$$Y^2 = G(X) := X^3 + a_2X^2 + a_4X + a_6.$$

On a :

Théorème 5 *Soit ℓ un nombre premier d'Elkies tel que $\ell \equiv 3 \bmod 4$ et h_ℓ un facteur de f_ℓ correspondant à λ. Si $[i]\pi_\ell = [j]$ sur $E[\ell]_\lambda$ alors on a :*

$$\lambda = \left(\frac{\lambda_0}{\ell}\right)\left(\frac{r}{q}\right)\lambda_0 \ ,$$

avec $r = \text{Résultant}(h_\ell, \mathcal{G})$.

Démonstration : Puisque $d = (\ell-1)/2$ est impair, on a $\pi_\ell^d = \pm(\frac{\lambda_0}{\ell})Id$ sur $E[\ell]_\lambda$. Si $\pi_\ell^d = Id$ ce qui signifie $(X^{q^d}, Y^{q^d}) = (X, Y)$ sur $E[\ell]_\lambda$, alors on a $E[\ell]_\lambda \subset E(\mathbb{F}_{q^d})$. Ainsi, pour tout P dans $E[\ell]_\lambda$, $\mathcal{G}(x(P))$ est un carré dans $\mathbb{F}_{q^d}$ et par suite $\prod_{i=1}^{d}(\mathcal{G}(x_i)) = r$ est un carré dans $\mathbb{F}_q$, avec x_i les racines de $h_\ell(X) = 0$, puisque d est impair. Par contre, si $\pi_\ell^d = -Id$ sur $E[\ell]_\lambda$, alors $(\frac{r}{q}) = -1$.

Ainsi, $\lambda = \lambda_0$ si et seulement si $(\frac{\lambda_0}{\ell})$ et $(\frac{r}{q})$ sont de même signe et $\lambda = -\lambda_0$ si et seulement si les deux quantités précédentes sont de signes différents. □

Exemple : Considérons la courbe $y^2 = x^3 + 4312x + 9867$ sur $\mathbb{F}_{17389}$. La factorisation du polynôme Φ_{43} sur $\mathbb{F}_{17389}$ nous montre que π_{43} admet deux valeurs propres dans $\mathbb{F}_{43}$ et donc le polynôme de division f_{43} admet deux facteurs de degré 21 modulo 17389. Explicitement, on a

$$h_{43} = 5304+5095x+9634x^2+9447x^3+10495x^4+2335x^5+16248x^6+454x^7+ 11634x^8+7661x^9+16799x^{10}+2870x^{11}+5586x^{12}+11693x^{13}+1975x^{14}+ 5920x^{15}+14785x^{16}+6873x^{17}+4789x^{18}+13401x^{19}+8275x^{20}+x^{21}.$$

Avec la méthode de Müller on obtient $\lambda_0 = 7$ et donc la valeur propre λ associé à h_{43} satisfait $\lambda = \pm 7$.

Dans la méthode originale, on doit comparer les ordonnées des points pour conclure. On calcule donc $y^p \bmod h_{43}(x)$ et $4y^{p+1}f_7^3 - f_9f_6^2 + f_5f_8^2 \bmod h_{43}$. Avec un sparc1, on obtient $\lambda = 7$ en 7.56 secondes.

Par contre, avec l'amélioration proposée, on doit juste calculer la valeur de $r = \text{Résultant}(x^3 + 4312x + 9867, h_{43})$. On trouve $r = 155551$ et $(\frac{r}{p}) = 1$ en 0.066 seconde et puisque $(\frac{7}{43}) = -1$ on a $\lambda = 7$.

Pour des valeurs de ℓ très grandes, cela donne un moyen évident d'accélérer le "funny" baby-step et giant-step de Müller.

Le tableau suivant transcrit clairement l'avantage du calcul d'un résultant dans la recherche du signe d'une valeur propre pour π_ℓ. Les calculs sont réalisés avec la courbe précédente et les résultats sont donnés en temps CPU.

ℓ	$\deg(h_\ell)$	r	y^p
19	9	0.03	2.2
43	21	0.05	4.72
71	35	0.11	17.55
103	51	0.21	34.06
131	65	0.28	52.63
167	83	0.46	81.33
227	113	0.78	139.92
271	135	1.08	191.30

Dans le théorème précédent on utilise le fait que d, le degré de h_ℓ, est impair. Dans le cas $\ell \equiv 1 \bmod 4$, le polynôme h_ℓ est de degré pair. On peut, alors, calculer λ_0 avec le polynôme h_ℓ comme d'habitude et ensuite déterminer $s(\lambda)$, puisque $s(\lambda_0) = s(\pm\lambda_0)$ et dans le cas où ce semi-ordre est impair on peut utiliser le résultat suivant :

Corollaire 3 *Si $\ell \equiv 1 \bmod 4$ et $s(\lambda_0)$ est impair, alors h_ℓ a un facteur g_ℓ de degré impair $s(\lambda_0)$ et la valeur propre associée à h_ℓ est*

$$\lambda = \lambda_0^{s(\lambda_0)} \left(\frac{r}{q}\right) \lambda_0,$$

avec $r = \text{Résultant}(g_\ell, \mathcal{G})$.

Démonstration : On note que $\pi_\ell^{s(\lambda_0)} = \pm Id$ sur $E[\ell]_\lambda$, lorsque $s(\lambda_0)$ est impair. Si $\pi_\ell^{s(\lambda_0)} = Id$, alors on a $E[\ell]_\lambda \subset E(\mathbb{F}_{q^{s(\lambda_0)}})$. Ainsi, pour tout P dans $E[\ell]_\lambda$, $\mathcal{G}(x(P))$ est un carré dans $\mathbb{F}_{q^{s(\lambda_0)}}$ et par suite $\prod_{i=1}^{s(\lambda_0)}(\mathcal{G}(x_i)) = r$ est un carré dans $\mathbb{F}_q$, avec x_i les racines de $g_\ell(X) = 0$, puisque d est impair. Par contre, si $\pi_\ell^d = -Id$ sur $E[\ell]_\lambda$, alors $(\frac{r}{q}) = -1$. □

Exemple : On considère toujours la courbe $y^2 = x^3 + 4312x + 9867$ sur $\mathbb{F}_{17389}$. Dans le cas $\ell = 29$ on a encore deux valeurs propres et la méthode de Müller donne $\lambda_0 = 4$. On a

$$h_{29} = 14857 + 11597x + 8078x^2 + 12406x^3 + 5018x^4 + 8378x^5 + 6772x^6 + 5809x^7 + 10942x^8 + 13433x^9 + 8919x^{10} + 4597x^{11} + 10848x^{12} + 1290x^{13} + x^{14}$$

et puisque le semi-ordre de 4 est 7 dans $\mathbb{F}_{29}$ on peut calculer un facteur g_{29} de degré 7 de h_{29}. On obtient le polynôme

$$g_{29} = 1028 + 6670x + 12102x^2 + 5117x^3 + 899x^4 + 14793x^5 + 7211x^6 + x^7$$

qui nous permet de trouver le signe de la valeur propre associé à h_{29}. On trouve $r = \text{Résultant}(x^3 + 4312x + 9867, g_{29}) = 2504$ puis $(\frac{2504}{17389}) = -1$ et $\lambda_0^{s(\lambda_0)} = -1$ donc $\lambda = 4$ et $t \bmod 29 = 23$.

En caractéristique 2.

On peut supposer que l'équation de E est de la forme $Y^2 + XY = X^3 + B$ avec B dans $\mathbb{F}_{2^m}$ (voir [29]).

Théorème 6 *Supposons que $\ell \equiv 3 \bmod 4$. En écrivant $h_\ell = x^d - s_1 x^{d-1} + \cdots + (-1)^d s_d$ le polynôme correspondant à λ, on a :*

$$\lambda = \begin{cases} \left(\frac{\lambda_0}{\ell}\right)\lambda_0 & \text{si } \mathrm{Tr}(s_1 + B(s_{d-1}^2 - 2s_d s_{d-2})/s_d^2) = 0, \\ -\left(\frac{\lambda_0}{\ell}\right)\lambda_0 & \text{sinon.} \end{cases}$$

Démonstration : Notons, tout d'abord, que l'équation $X^2 + X = \gamma$ a une racine dans $\mathbb{F}_{2^n}$ si et seulement si $\mathrm{Tr}(\gamma) = 0$. En écrivant l'équation de E sous la forme $(y/x)^2 + (y/x) = x + B/x^2$, les points de $E[\ell]_\lambda = \langle P = (x, y)\rangle$ sont dans $\mathbb{F}_{p^d}$ si et seulement si $\mathrm{Tr}(\gamma_i) = 0$ avec $\gamma_i = x_i + B/x_i^2$ et $x_i = x([i]P)$. De plus, on a

$$r = \sum_{i=1}^{d} \mathrm{Tr}(\gamma_i) = \mathrm{Tr}(\sum_{i=1}^{d}(\gamma_i)) = \mathrm{Tr}(s_1 + B(s_{d-1}^2 - 2s_d s_{d-2})/s_d^2)\ ,$$

où les s_i sont les fonctions symétriques de h_ℓ, ainsi r est facilement calculé. Finalement, si r $= 0$, alors la valeur propre associée au facteur h_ℓ est $\lambda \equiv (\frac{\lambda_0}{\ell})\lambda_0 \bmod \ell$, sinon $\lambda \equiv -(\frac{\lambda_0}{\ell})\lambda_0 \bmod \ell$. □

Proposition 27 *Soit h_ℓ un facteur de f_ℓ correspondant à $\lambda = \pm\lambda_0$. Si h_ℓ a un facteur $g_\ell = x^{s(\lambda_0)} - \tilde{s}_1 x^{s(\lambda_0)-1} + \cdots + (-1)^{s(\lambda_0)}\tilde{s}_{s(\lambda_0)}$ de degré impair $s(\lambda_0)$ alors*

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

2.4 La méthode de Elkies avec les nombres premiers d'Atkin

On montre ici comment utiliser la méthode de Elkies dans le cas où π_ℓ n'a pas de valeurs propres rationnelles ce qui veut dire que D n'est pas un carré modulo ℓ. Plus précisement, on peut calculer un facteur du polynôme de division f_ℓ même dans le cas où l'équation modulaire $\Phi_\ell(X, j(E)) = 0$ n'a pas de racines dans $\mathbb{F}_q$. On montre ensuite comment réaliser la procédure de Schoof sur les abscisses des points uniquement.

2.4.1 Recherche d'un facteur de f_ℓ

On suppose dans ce paragraphe que $q = p$ est premier et $p \neq 2, 3$; ℓ est un nombre premier d'Atkin tel que $\ell \ll p$.

On décrit comment étendre la méthode de Elkies aux nombres premiers ℓ pour lesquels π_ℓ n'admet pas de valeurs propres dans $\mathbb{F}_\ell$. C'est le cas où le polynôme $\Phi_\ell(X, j(E))$ n'admet pas de racines dans $\mathbb{F}_p$, cas qui n'est pas traité par Elkies.

L'automorphisme π_ℓ agit sur les $(\ell+1)$ sous-groupes $G_1, G_2, \ldots, G_{\ell+1}$ de $E[\ell]$. On note $G_i = \langle P_i \rangle$ pour $i = 1, \ldots, \ell+1$. D'autre part, l'ordre entier e modulo ℓ de la suite de polynôme caractéristique $x^2 - \tau x + k$ est, par définition, le plus petit entier n pour lequel $\pi_\ell^n \in \mathbb{F}_\ell$, ainsi les G_i sont $\mathbb{F}_{p^e}$-rationnels et, donc, les $\ell+1$ courbes E_i sont définies sur $\mathbb{F}_{p^e}$. Le polynôme de division f_ℓ a un facteur de degré d sur $\mathbb{F}_{p^e}$ et donc par conjugaison on peut trouver un facteur de degré ed sur $\mathbb{F}_p$.

Explicitement, on procède de la manière suivante :

On détermine un facteur $M_\ell(F)$ unitaire irréductible de degré e du polynôme $\Phi_\ell(F, j(E))$ dans $\mathbb{F}_p[x]$. On sait qu'il existe e isogénies ϱ_i, $i = 1, 2, \ldots, e$, définie sur $\mathbb{F}_{p^e}$ de la courbe elliptique E vers d'autres courbes E_i définie sur $\mathbb{F}_{p^e}$ dont le noyau

$$G_i = \{O_E, P_i, 2P_i, \ldots, (\ell-1)P_i\}$$

est rationnel sur $\mathbb{F}_{p^e}$.

Si on note $F_1, F_2, \ldots, F_e$ les racines conjuguées de $M_\ell(F)$ dans $\mathbb{F}_{p^e}$ alors $\tilde{A}_i = \tilde{A}(F_i)$ et $\tilde{B}_i = \tilde{B}(F_i)$ sont les coefficients de la courbe elliptique E_i. On a également $p_1(F_i) = \sum_{j=1}^{d} x([j]P_i)$. Les formules de récurrence (R_1) permettent de déterminer ed polynômes $p_k(F)$, $k = 1, 2, \ldots, ed$, de degré $e-1$ que l'on note $p_k(F) = \sum_{j=0}^{e-1} a_{j,k} F^j$ avec $a_{j,k} \in \mathbb{F}_p$. Pour k tel que $1 \leq k \leq ed$ on note

$$p_k = \sum_{i=1}^{e} p_k(F_i) = \sum_{i=1}^{e} (\sum_{j=1}^{d} x^k([j]P_i)).$$

Lemme 4 $p_k \in \mathbb{F}_p$.

Démonstration : En effet, $p_k^p = \sum_{i=1}^{e} p_k^p(F_i) = \sum_{i=1}^{e} p_k(F_i^p) = \sum_{j=1}^{e} p_k(F_j) = p_k$, puisque les F_i sont les racines conjuguées du polynôme irréductible $M_\ell(F)$. □

On calcule les p_k pour $k = 1, 2, \ldots, ed$ de la manière suivante :
on a

$$p_k = \sum_{i=1}^{e} p_k(F_i) = \sum_{i=1}^{e} (\sum_{j=0}^{e-1} a_{j,k} F_i^j) = \sum_{j=0}^{e-1} a_{j,k} (\sum_{i=1}^{e} F_i^j)$$

donc $p_k = \sum_{j=0}^{e-1} a_{j,k} \tilde{p}_j$ avec $\tilde{p}_j = \sum_{i=1}^{e} F_i^j$. Mais les F_i sont racines de

$$M_\ell(F) = \tilde{s}_0 F^e - \tilde{s}_1 F^{e-1} + \cdots + (-1)^e \tilde{s}_e$$

, on peut alors calculer les $\tilde{p}_j$ à partir des valeurs connues $\tilde{s}_j$ à l'aide de la relation inverse de Newton :

$$\tilde{p}_0 = e \ , \ \tilde{p}_1 = \tilde{s}_1 \text{ et pour } j > 1 \text{ on a } \tilde{p}_j = (-1)^{j-1}(j\tilde{s}_j + \sum_{k=1}^{j-1} (-1)^k \tilde{p}_k \tilde{s}_{j-k}).$$

On en déduit les ed valeurs p_k à partir des e valeurs $\tilde{p}_j$ et on détermine les s_k à l'aide de la relation de Newton. On obtient ainsi un facteur de degré ed du polynôme de division f_ℓ.

Pour l'algorithme S.E.A, dans le cas où le polynôme $\Phi_\ell(F, j(E))$ n'a pas de racine dans $\mathbb{F}_p$, on peut déterminer un facteur de degré ed du polynôme f_ℓ lorsque e n'est pas trop grand et l'utiliser à la place de f_ℓ dans l'algorithme. On utilise, alors, l'algorithme original de Schoof à la place de la méthode de Atkin. Par exemple pour $\ell = 271$ avec la courbe du record le polynôme $\Phi_\ell(F, j(E))$ se décompose en facteurs de degré 4 et a permis à Morain d'utiliser l'algorithme original de Schoof avec un polynôme de degré 540 [8].

Cette extension permet, également, de déterminer une décomposition partielle des polynômes de division d'indice premier ℓ en itérant la méthode à chaque facteur irréductible de $\Phi_\ell(F, j(E))$.

Exemple : On considère la courbe elliptique E d'équation $y^2 = x^3 + 2x + 41$ dans $\mathbb{F}_{59}$ d'invariant $j = 31$. On calcule les coefficients d'un facteur du polynôme de division f_5 de E. On a :

$$\Phi_\ell(F, 31) \bmod 59 = (32 + 45F + 41F^2 + F^3)(50 + 13F + 48F^2 + F^3).$$

	$M_1 = 32 + 45F + 41F^2 + F^3$	$M_2 = 50 + 13F + 48F^2 + F^3$
$p_0(F)$	2	2
$p_1(F)$	$41 + 31F + 56F^2$	$4 + 10F + 48F^2$
$p_2(F)$	$26 + 22F + 46F^2$	$46 + 54F + 47F^2$
$p_3(F)$	$39 + 20F + 21F^2$	$2 + 24F + F^2$
$p_4(F)$	$6 + 11F + 16F^2$	$33 + 18F + 7F^2$
$p_5(F)$	$17 + 41F + 51F^2$	$16 + 24F + 58F^2$
$p_6(F)$	$41F + 34F^2$	$19 + 27F + 24F^2$
$p_1, \ldots, p_6$	$2, 38, 28, 22, 7, 38, 21$	$2, 21, 5, 11, 18, 40, 38$
g_5	$55, 3, 10, 13, 21, 1$	$29, 28, 2, 41, 38, 1$

On obtient donc

$$f_5 = (55 + 3x + 10x^2 + 13x^3 + 21x^5 + x^6)(29 + 28x + 2x^2 + 41x^4 + 38x^5 + x^6).$$

2.4.2 Calcul de $t \bmod \ell$

Dans ce paragraphe, on accélère la procédure de Schoof (ℓ est toujours un nombre premier d'Atkin). Plus précisement, on teste les équations $\pi_\ell^2 + k = \tilde{\tau}\pi_\ell$ en $\tilde{\tau}$ en n'utilisant que les abscisses des points.

Rappelons tout d'abord que si

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

et

$$(x_1, y_1) - (x_2, y_2) = (x_4, y_4) \ ,$$

alors on a $(x_3 + x_4)(x_1 - x_2)^2 = S(x_1, x_2)$ et $(x_3 x_4)(x_1 - x_2)^2 = P(x_1, x_2)$ avec

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

et

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

Ainsi les valeurs x_3 et x_4 sont solutions de l'équation quadratique $E(X) = NX^2 - SX + P$ avec $N(x_1, x_2) = (x_1 - x_2)^2$. On vérifie facilement que ce sont les seules.

Dans la méthode de Schoof on cherche un $\tilde{\tau}$ telle que l'équation $\pi_\ell^2 + k = \tilde{\tau}\pi_\ell$ soit satisfaite sur $E[\ell]$. On utilise la méthode de Müller avec les entiers i, j et k_{opt} dans l'équation $i\pi_\ell^2 + ik = j\pi_\ell$. Notre stratégie consiste à chercher une valeur j pour laquelle $x([j]\pi_\ell)$ est une racine de l'équation quadratique $E(X)$ donnée par $S_i = S(x_i^{q^2}, x_{ik})$, $P_i = P(x_i^{q^2}, x_{ik})$ et $N_i = N(x_i^{q^2}, x_{ik})$ comme précédemment.

D'autre part, si $x_j^q = x_3$ alors $x(i\pi_\ell^2 + ik) = x(j\pi_\ell)$ et par suite on a deux possibilités : $\pi_\ell^2 + k = \pm\tau_0\pi_\ell$ sur $E[\ell]$. Ainsi, dans ce cas $\tau \equiv \pm\tau_0 \bmod \ell$. Alors que si $x_j^q = x_4$ on a $x(i\pi_\ell^2 - ik) = x(j\pi_\ell)$ ce qui donne $\pi_\ell^2 - k = \pm\tau_0\pi_\ell$ et donc $\pi_\ell = 2k/(\tau \pm \tau_0)$. Mais ce dernier cas n'est pas possible puisque ℓ est un nombre premier d'Atkin.

Pour le calcul de $x_i^{q^2}$, on calcule au préalable $R(x) \equiv x^{q^2} \bmod h_\ell(x)$ puis on utilise la récurrence des polynômes de division en $R(x)$.

On obtient un nouvel algorithme qui évite le calcul de y^{q^2} et y^q et donne deux valeurs possibles pour $t \bmod \ell$. L'algorithme que je propose est le suivant :

1. *Calculer* $x^q \bmod h_\ell(x)$,
2. pour $j = 1, \ldots, k_{opt}$
   (a) *Calculer* $x_j(x) = x([j](x, y))$
   (b) *calculer* $x_j(x^q) = x([j](x^q, y^q))$.
3. *Calculer* $x^{q^2} \equiv x^q \circ x^q \bmod h_\ell(x)$.
4. Pour $i = 1, 2 \ldots$
   (a) *Calculer* $x_i(x^{q^2}) = x([j](x^{q^2}, y^{q^2}))$,
   (b) *calculer* $x_{ik}(x) = x([ik](x, y))$,
   (c) calculer $S_i = S(x_i^{q^2}, x_{ik})$,$P_i = P(x_i^{q^2}, x_{ik})$ et $N_i = N(x_i^{q^2}, x_{ik})$ à partir de la table et poser $E_i(X) = N_i X^2 - S_i X + P_i$,

(d) *chercher* j dans la table tel que $E_i(x_j) = 0$ en utilisant une application linéaire aléatoire. Si on trouve une racine on a $\tau \equiv \pm i^{-1} j \bmod \ell$.

Exemple : Considérons la courbe $y^2 = x^3 + 362x + 34$ sur $\mathbb{F}_{397}$. Avec $\ell = 11$ on a $e = 6$ donc on peut calculer un facteur h_{11} de degré 30 de f_{11} et l'utiliser pour calculer $t \bmod 11$. Mais puisque $\pi_\ell^6 = -1$ on peut réaliser les calculs modulo un facteur g_{11} de degré 6 de h_{11}. On a

$g_{29} = x^6 + 64x^5 + 333x^4 + 394x^3 + 294x^2 + 336x + 184$.

On prend $k_{opt} = 3$ et on stocke $\{j, x_j, x_j^q\}$ pour $j = 1, 2, 3$.

	x_j $(\epsilon = 0)$	x_j^p $(\epsilon = 1)$
$\phi_1(x^{q^\epsilon})$	x	$80 + 344x + 237x^2 + 93x^3 + 155x^4 + 215x^5$
$f_1^2(x^{q^\epsilon})$	1	1
$\phi_2(x^{q^\epsilon})$	$34 + 125x + 70x^2 + x^4$	$219 + 254x + 194x^2 + 146x^3 + 370x^4 + 351x^5$
$f_2^2(x^{q^\epsilon})$	$136 + 257x + 4x^3$	$386 + 239x + 358x^2 + 54x^3 + 94x^4 + 371x^5$
$\phi_3(x^{q^\epsilon})$	$296 + 277x + 258x^2 + 86x^3 + 191x^4 + 119x^5$	$74 + 304x + 255x^2 + 174x^3 + 240x^4 + 33x^5$
$f_3^2(x^{q^\epsilon})$	$138 + 88x + 139x^2 + 280x^3 + 38x^4 + 331x^5$	$138 + 88x + 139x^2 + 280x^3 + 38x^4 + 331x^5$

On a $k = 1$ donc $x_{ik} = x_i$.

	$i = 1$	$i = 2$
$\phi_i(x^{q^2})$	$1 + 316x + 57x^2 + 324x^3 + 203x^4 + 384x^5$	$362 + 376x + 395x^2 + 202x^3 + 339x^4 + 174x^5$
$f_i^2(x^{q^2})$	1	$300 + 143x + 196x^2 + 171x^3 + 245x^4 + 29x^5$
M_i	$79 + 322x + 328x^2 + 112x^3 + 127x^4 + 263x^5$	$258 + 295x + 324x^2 + 195x^3 + 384x^4 + 359x^5$
S_i	$222 + 175x + 186x^2 + 260x^3 + 88x^4 + 199x^5$	$160 + 32x + 216x^2 + 354x^3 + 171x^4 + 346x^5$
P_i	$43 + 226x + 23x^2 + 396x^3 + 51x^4 + 313x^5$	$57 + 242x + 298x^2 + 5x^3 + 135x^4 + 281x^5$
$E_i(x_1^q)$	$394 + 298x + 59x^2 + 154x^3 + 267x^4 + 25x^5$	0
$E_i(x_2^q)$	$234 + 268x + 49x^2 + 183x^3 + 171x^4 + 371x^5$	- - -
$E_i(x_3^q)$	$77 + 229x + 142x^2 + 163x^3 + 226x^4 + 47x^5$	- - -

Finalement, on obtient $(i, j) = (2, 1)$ et $t \bmod 11 \equiv \pm 5$.

2.4.3 Le signe de $t \bmod \ell$

On peut encore utiliser l'idée du paragraphe §3 pour déterminer le signe dans $\tau_0 \equiv \pm t \bmod \ell$ et donc éviter le calcul des ordonnées modulo h_ℓ en calculant un résultant. Mais, ici, on doit avoir de plus e impair. En effet, puisque π_ℓ satisfait l'équation $x^2 - \tau x + k = 0$, on a $\pi_\ell^n = [U_n]\pi_\ell + [V_n]$ avec U_n et V_n des polynômes en τ et k. On a immédiatement $V_n = -kU_{n-1}$ et de plus le polynôme U_n contient uniquement des puissances paires de τ si n est impair et des puissances impaires sinon [4]. D'autre part, $\pi_\ell^e = V_e$ puisque e est le plus petit entier n pour lequel π_ℓ^n est dans $\mathbb{F}_\ell$. Noter également que la valeur de e ne dépend pas du signe de τ. Ainsi, lorsque e est impair, on a $V_e(\pm\tau, k) = \pm V_e(\tau, k)$ donc dans ce cas $\pi_\ell^e = \pm V_e(\tau_0, k)$. On pose $\omega_0 = V_e(\tau_0, k)$.

En caractéristique $p \neq 2$.

Proposition 28 *On suppose que e est impair. Soit h_ℓ un facteur de degré ed de f_ℓ.*
Lorsque $\ell \equiv 3 \bmod 4$ on a

$$t \equiv \left(\frac{r}{q}\right)\left(\frac{\omega_0}{\ell}\right)\tau_0 \bmod \ell$$

avec $r = \text{Résultant}(h_\ell, \mathcal{G})$.
Lorsque $s(\omega_0)$ est impair on a

$$t \equiv \left(\frac{r}{q}\right)\omega_0^{s(\omega_0)}\tau_0 \bmod \ell$$

avec $r = \text{Résultant}(g_\ell, \mathcal{G})$ *où g_ℓ est un facteur de degré $s(\omega_0)$ de h_ℓ.*

Démonstration : On a $\pi_\ell^e = \pm\omega_0$ sur $E[\ell]$, ainsi $\pi_\ell^{ed} = \pm\omega_0^d = \pm(\frac{\omega_0}{\ell})Id$ sur $E[\ell]$ si d est impair et $\pi_\ell^{es(\omega_0)} = \pm\omega_0^{s(\omega_0)} = \pm(\frac{\omega_0}{\ell})Id$ sur $E[\ell]$ si $s(\omega_0)$ est impair. □

La quantité $\omega = V_e(\tau_0, k)$ est la valeur de $\pi_\ell^e \in \mathbb{F}_\ell$ et est donc facilement calculée à partir de $\pi_\ell^2 = \tau_0\pi_\ell + k$. Le type de décomposition de h_ℓ est déterminé en calculant $s(\omega_0)$.

Exemple : Considérons la courbe $y^2 = x^3 + 4312x + 9167$ sur $\mathbb{F}_{12853}$. On considère tout d'abord le cas $\ell \equiv 3 \bmod 4$ avec $\ell = 19$. On a $e = 5$ et un facteur h_{19} de degré 45 de f_{19} et avec la nouvelle procédure de Schoof on obtient $t \bmod 19 \equiv \pm 7$. On détermine le signe de τ en calculant $r = \text{Résultant}(x^3 + 4312x + 9167, h_{19}) = 11226$ et puisque $(\frac{r}{p}) = 1$ et $P_5(7, 9) = 4$ on a $t \bmod 19 = 7$.

Considérons maintenant le cas $\ell = 13$, on a $e = 7$ impair et $t \equiv \pm 5 \bmod 13$. Mais $\ell \equiv 1 \bmod 4$ donc on ne peut utiliser directement le facteur h_{13} de degré 42 de f_{13} dans un résultant. Toutefois, puisque $\pi_{13}^7 = \pm 10$ a un semi-ordre égal à $s(10) = 3$ le polynôme h_{13} a un facteur irréductible g_{13} de degré 21 que l'on peut utiliser dans un résultant On obtient $r = \text{Résultant}(x^3 + 4312x + 9167, g_{13}) = 9515$ et $(\frac{r}{p}) = -1$ ainsi on a $t \bmod 13 = 5$.

En caracteristique 2.

Proposition 29 *On suppose que e est impair. Soit h_ℓ un facteur de degré ed de f_ℓ.*
Lorsque $\ell \equiv 3 \bmod 4$ on a

$$\tau = \begin{cases} \left(\frac{\omega_0}{\ell}\right)\tau_0 & \text{si } \operatorname{Tr}(s_1 + B(s_{ed-1}^2 - 2s_{ed}s_{ed-2})/s_{ed}^2) = 0, \\ -\left(\frac{\omega_0}{\ell}\right)\tau_0 & \text{sinon,} \end{cases}$$

avec s_i les fonctions symétriques de h_ℓ.
Lorsque $s(\omega)$ iest impair on a

$$\tau = \begin{cases} \omega_0^{s(\omega_0)}\tau_0 & \text{si } \operatorname{Tr}(\tilde{s}_1 + B(\tilde{s}_{es(\omega_0)-1}^2 - 2\tilde{s}_{es(\omega_0)}\tilde{s}_{es(\omega_0)-2})/\tilde{s}_{es(\omega_0)}^2) = 0, \\ -\omega_0^{s(\omega_0)}\tau_0 & \text{sinon,} \end{cases}$$

avec $\tilde{s}_i$ les fonctions symétriques d'un facteur g_ℓ de degré $es(\omega_0)$ de h_ℓ.

Chapitre 3

Cycles d'isogénies rationnelles

3.1 Introduction

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ de caractéristique p. La courbe est donnée par une équation $\mathcal{F}(X,Y,Z) = 0$ sous la forme générale

$$\mathcal{F}(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) .$$

Ainsi, un point générique sur la courbe est donnée par (X,Y) mod $\mathcal{F}$. Soit m le nombre de points sur E. On sait que $m = p + 1 - t$, avec t un entier satisfaisant $\mid t \mid < 2\sqrt{q}$. On se place dans ce chapitre dans le cas où la caractéristique du corps p est un très grand nombre premier, disons p superieur à 10^{200}. Pour déterminer le nombre de points de E on sait que l'on doit utiliser l'algorithme de Schoof-Elkies-Atkin décrit dans le chapitre précédent.

On sait que l'algorithme de Schoof détermine t mod ℓ pour suffisamment de petits nombres premiers ℓ en travaillant modulo des polynômes de degré $(\ell^2 - 1)/2$. La méthode s'étend également aux puissances de nombres premiers ℓ^n. Avec l'amélioration de Elkies, un nombre premiers peut-être bon ou mauvais. Comme nous l'avons vu au chapitre II, lorsque ℓ est un bon nombre premier, la méthode de Elkies permet de calculer t mod ℓ beaucoup plus rapidement que dans l'algorithme de Schoof en travaillant modulo des polynômes de degré $(\ell - 1)/2$. De plus, dans ce cas, on peut calculer t mod ℓ^n plus rapidement que dans l'algorithme de Schoof. Dans ce chapitre, on explique, en étudiant une nouvelle notion introduite par Morain et Couveignes en 1994, celle de cycles d'isogénies rationnelles [13], comment déterminer t mod ℓ^n avec la même compléxité que pour t mod ℓ dans le cas de bons nombres premiers ℓ. Pour cela, on précise le rôle des isogénies dans l'amélioration apportée par Elkies et Atkin. On approfondit l'étude de cette notion et on donne quelques utilisations efficaces de ces cycles pour la détermination de t mod ℓ^n.

Ce chapitre se décompose de la manière suivante : Dans un premier temps, on revoit brièvement l'algorithme SEA en mettant l'accent sur le calcul de t mod ℓ^n et sur le rôle des isogénies. On introduit pour cela le module de Tate $T_\ell(E)$ de la courbe elliptique E. Puis, on présente les cycles rationnels de courbes isogènes sur $\mathbb{F}_q$ en itérant la méthode de Elkies. Cela permet d'attraper un facteur de f_{ℓ^n} et de l'utiliser dans SEA. Ensuite, j'introduis le changement de directions en utilisant l'action de l'involution d'Atkin-Lehner et on en tire un double avantage pour la détermination de t mod ℓ^n :

D'une part, on peut ramener le calcul de t mod ℓ^n à celui de t mod $\ell^{n/2}$ et, d'autre part, cela permet d'optimiser l'utilisation d'un facteur de h_ℓ (h_ℓ étant lui même un facteur de f_ℓ).

3.2 La méthode de Schoof-Elkies-Atkin

3.2.1 Le module de Tate

Soit E/K une courbe elliptique. Le module de Tate de E est le groupe

$$T_\ell(E) = \lim_{\leftarrow} E[\ell^n],$$

la limite inverse étant prise suivant l'application naturelle $E[l^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$. Puisque chaque $E[\ell^n]$ est un $\mathbb{Z}/\ell^n\mathbb{Z}$-module, on en déduit que le module de Tate a une structure naturelle de $\mathbb{Z}_\ell$-module. On a la proposition suivante :

Proposition 30 *En tant que $\mathbb{Z}_\ell$-module, le module de Tate a la structure suivante :*
$-T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *si* $\ell \neq car(K)$,
$-T_p(E) \cong 0$ *ou* $\mathbb{Z}_p$ *si* $p = car(K) > 0$.

3.2.2 L'idée initiale

On considère ℓ un petit nombre premier avec $\ell < p$. L'endomorphisme de Frobenius π de E induit un automorphisme π_ℓ de l'espace des points de ℓ-torsion $E[\ell]$ que l'on peut étendre au module de Tate $T_\ell(E)$.

L'idée de Schoof dans son algorithme est de considérer π en tant qu'element de $GL_2(\mathbb{F}_\ell)$ avec l'équation $\pi_\ell^2 - \tau\pi_\ell + k = 0$ sur $E[\ell]$ où $\tau \equiv t \bmod \ell$ et $k \equiv q \bmod \ell$. Comme nous l'avons vu au chapitre précédent, Schoof obtient ainsi la valeur de $t \bmod \ell$ en utilisant les polynômes de division f_ℓ de E.

On peut aller encore plus loin en considérant π en tant qu'élément de $GL_2(\mathbb{Z}_\ell)$. On a l'équation

$$\pi_\ell^2 - \bar{t}\pi_\ell + \bar{q} = 0$$

sur $T_\ell(E)$ avec $\bar{t} \in \mathbb{Z}_\ell$ et $\bar{q} \in \mathbb{Z}_\ell^*$.

Explicitement, on peut écrire $\bar{t} = \sum_{n=0} \tau_n \ell^n$ avec $\tau_0 = \tau$ et $\bar{q} = \sum_{n=0} k_n \ell^n$ avec $k_0 = k$.

On peut ainsi déterminer la décomposition ℓ-adique de la trace du Frobenius de E en utilisant les polynômes de division f_{ℓ^k} de E. Mais comme nous l'avons vu les polynômes de division ont un degré trop élevé.

3.2.3 l'idée d'Elkies

L'idée de Elkies est que si $\mathrm{Disc}(\pi) = t^2 - 4q$ est un carré non nul modulo ℓ (le cas zéro marche également mais de manière un peu différente) alors π a deux valeurs propres rationnelles distinctes α et β dans $\mathbb{F}_\ell$ et même dans $\mathbb{Z}_\ell$. Ainsi, le module de Tate $T_\ell(E)$ se décompose en la somme directe des deux sous-espaces propres correspondants

$$T_\ell(E) = T_\alpha^E \oplus T_\beta^E$$

et de même pour le groupe de ℓ-torsion.

On sait également que le polynôme de division $f_\ell^E(X)$ possède alors deux facteurs h_α et h_β de degré $d = (\ell - 1)/2$ et à chacun correspond une valeur propre. D'autre part, on a deux courbes, E_α et E_β, ℓ-isogène à E, définies sur $\mathbb{F}_q$ dont on écrira une équation sous la forme $\mathcal{F}_\lambda$ avec

$$\mathcal{F}_\lambda(X,Y,Z) = Y^2Z + a_{1\lambda}XYZ + a_{3\lambda}YZ^2 - (X^3 + a_{2\lambda}X^2Z + a_{4\lambda}XZ^2 + a_{6\lambda}Z^3),$$

via deux isogénies ϱ_λ tel que $Ker(\varrho_\lambda) = T_\lambda^E \cap E[\ell]$. Et, pour tout point $P = (X, Y) \bmod \mathcal{F}$ de E on peut écrire

$$\varrho_\lambda(P) = (\frac{k_\lambda(X)}{h_\lambda^2(X)}, \frac{g_\lambda(X)}{Y h_\lambda^3(X)}) \bmod \mathcal{F}_\lambda$$

pour $\lambda = \alpha, \beta$.

L'idée est de remplacer le polynôme $f_\ell^E(X)$ par l'un des facteurs h_α ou h_β.

Ainsi la méthode globale se décompose en deux étapes :

On recherche une racine rationnelle de l'équation modulaire de degré $\ell + 1$. S'il y en a une, on utilise la méthode de Elkies, sinon, on utilise la méthode de Atkin.

Comme signalé au chapitre 2, cet algorithme n'utilise que des polynômes de degré $\ell+1$ et $(\ell - 1)/2$ ce qui est beaucoup plus petit que $(\ell^2 - 1)/2$.

3.3 Cycles rationnels de courbes isogènes

3.3.1 Théorie

On se réfère ici à [13]. On suppose maintenant que $\pi \in GL_2(\mathbb{Z}_\ell)$ a deux valeurs propres rationnelles distinctes α et β. Notons que, puisque les deux isogénies sont rationnelles, elles commutent avec l'endomorphisme de Frobenius π. Cela entraine que, pour la courbe ℓ-isogène, les valeurs propres du Frobenius sont identiques. Puisque les sous-espaces propres T_α et T_β sont indépendant, ϱ_α induit une bijection entre T_α^E et le sous-espace propre correspondant sur E_α et réciproquement ϱ_β induit une bijection entre T_β^E et le sous-espace propre correspondant sur E_β.

L'existence de deux valeurs propres rationnelles a une autre conséquence intérressante, à savoir que E_α a également deux isogénies rationnelles de degré ℓ, chacune associée à une valeur propre. On note $\varrho_{\alpha\alpha}$ (notés en abrégé ϱ_{α^2}) et $\varrho_{\alpha\beta}$ ces deux isogénies et $E_{\alpha\alpha}$ et $E_{\alpha\beta}$ les courbes elliptiques images. D'autre part, on sait que, puisque ϱ_α est rationnelle, l'isogénie duale $\hat{\varrho}_\alpha$ est également rationnelle. Par suite, $\hat{\varrho}_\alpha$ est égale à $\varrho_{\alpha\alpha}$ ou $\varrho_{\alpha\beta}$. En regardant la restriction à T_α^E on voit que

$$\hat{\varrho}_\alpha = \varrho_{\alpha\beta} \ .$$

On peut exprimer cela en disant que les deux directions rationnelles ne sont pas simplement indépendantes mais duales.

Maintenant, si E est une courbe définie sur $\mathbb{F}_q$ tel que $t^2 - 4q$ est un carré modulo ℓ on peut alors construire deux suites périodiques de courbes isogènes sur $\mathbb{F}_q$. Ces suites définissent deux permutations $\mathcal{I}_\alpha$ et $\mathcal{I}_\beta$ sur l'ensemble des courbes elliptiques sur $\mathbb{F}_q$, classifié modulo les $\mathbb{F}_q$-isomorphismes. La permutation $\mathcal{I}_\alpha$ est engendré par le quotient de E par α et les permutations sont inverses l'une de l'autre.

$$E \xrightarrow{\varrho_\alpha} E_\alpha \xrightarrow{\varrho_{\alpha^2}} E_{\alpha^2} \xrightarrow{\varrho_{\alpha^3}} \ldots$$

$$E \xrightarrow{\varrho_\beta} E_\beta \xrightarrow{\varrho_{\beta^2}} E_{\beta^2} \xrightarrow{\varrho_{\beta^3}} \ldots$$

Ces suites sont déterminés de la manière suivante. On utilise l'équation modulaire $\Phi_\ell(X,Y)$. On note j_0 l'invariant modulaire de E et on résoud l'équation polynomiale $\Phi_\ell(X,j_0)=0$ sur $\mathbb{F}_q$. Si on se trouve dans le cas d'Elkies, cette équation possède deux racines rationnelles simples distinctes F_α et F_β, à partir desquelles on détermine les courbes rationnelles, E_α et E_β, ℓ-isogènes à E d'invariants respectifs j_α et j_β. Ensuite on résoud l'équation $\Phi_\ell(X,j_\alpha)=0$ sur $\mathbb{F}_q$. On trouve deux racines distinctes rationnelles simples, l'une d'entre elle est $W_\ell(F_\alpha)=F_{\alpha\beta}$ et correspond à l'isogénie duale. On choisit l'autre racine que l'on note F_{α^2} donnant E_{α^2}. On poursuit le procédé en résolvant sur $\mathbb{F}_q$ l'équation $\Phi_\ell(X,j_{\alpha^2})=0$ et ainsi de suite.

3.3.2 Exemple

On considère la courbe elliptique E d'équation $y^2=x^3+13x+12$ dans $\mathbb{F}_{97}$. On donne dans le tableau suivant la liste des courbes 5-isogènes du cycle commençant par la courbe E.

E	$j(E)$	$F(E)$
[13, 12]	90	62
[35, 86]	35	18
[87, 83]	29	91
[33, 77]	4	50
[27, 40]	95	88
[34, 29]	17	27
[78, 8]	90	

Dans l'autre direction, on obtient le cycle inverse :

E	$j(E)$	$F(E)$
[13, 12]	90	23
[82, 57]	17	28
[27, 57]	95	26
[61, 63]	4	42
[37, 23]	29	83
[9, 6]	35	46
[80, 27]	90	

3.3.3 Calcul d'un facteur de f_{ℓ^n}

Le facteur de $f_\ell^E(x)$ correspondant à $T_\alpha^E \cap E[\ell]$ est h_α, le dénominateur de ϱ_α. Maintenant, si l'on veut le facteur de $f_{\ell^2}^E$, on procède de la manière suivante. Considérons les isogénies

$$(x,y) \stackrel{\varrho_\alpha}{\to} (X=\frac{k_\alpha(x)}{h_\alpha(x)^2},-) \stackrel{\varrho_{\alpha\alpha}}{\to} (\frac{k_{\alpha\alpha}(X)}{h_{\alpha\alpha}(X)^2},-).$$

On calcule au préalable le polynôme $h_{\alpha\alpha}$ qui est le dénominateur de $\varrho_{\alpha\alpha}$, de la même manière que pour h_α sauf que l'on remplace E par E_α en faisant attention de ne pas prendre $\hat{\varrho}_\alpha = \varrho_{\alpha\beta}$. En effet, on considère l'isogénie à partir de E_α associé à la valeur propre α. On remarque que $\varrho_\alpha(T_\alpha^E \cap E[\ell^2]) = (T_\alpha^{E_\alpha} \cap E_\alpha[\ell])$ par conséquent on a $\varrho_{\alpha\alpha} \circ \varrho_\alpha(T_\alpha^E \cap E[\ell^2]) = O_{E_{\alpha\alpha}}$ ainsi $\mathrm{Ker}(\varrho_{\alpha\alpha} \circ \varrho_\alpha) \subset E[\ell^2]$ et donc le facteur de $f_{\ell^2}^E$ que l'on recherche est obtenue en déterminant le numérateur de $h_{\alpha\alpha} \circ \varrho_\alpha$. En itérant le procédé on peut calculer un facteur de degré $\ell^{n-1}d$ si ℓ est impair (la cas $\ell = 2$ est un peu différent et est un cas pathologique [14] puisque le type de décomposition du polynôme $\Phi_2(X, j(E))$ sur $\mathbb{F}_q[X]$ est (1) ou $(1,1,1)$) du polynôme f_{ℓ^n} en explicitant le numérateur de

$$h_{\alpha^n} \circ \varrho_{\alpha^{n-1}} \circ \cdots \circ \varrho_\alpha.$$

De cette manière on peut calculer un facteur de degré $\ell^{n-1}(\ell-1)/2$ du polynôme $f_{\ell^n}^E$ et ensuite utiliser l'idée de Schoof pour calculer l'ordre du groupe modulo ℓ^n plutôt que modulo ℓ. Cela nous permet de tirer plus d'avantages des bons petits nombres premiers ℓ.

3.4 Algorithme

On décrit dans ce paragraphe comment implanter de manière efficace cette idée. Le problème est la détermination itératives d'une racine rationnelle des équations modulaires. On introduira une idée originale de changement de directions qui aura ici une double application.

3.4.1 Calculs de h_α et ϱ_α

On utilise la démarche de Atkin, à savoir on résoud l'équation $\Phi_\ell(X, j_0) \equiv 0$ dans $\mathbb{F}_q$. À partir d'une racine F_α on détermine j_α racine de

$$\Phi_\ell(W_\ell(F_\alpha), Y) \equiv 0$$

dans $\mathbb{F}_q$ (lorsque $q = p$ est très grand, on peut faire mieux dans le cas "canonique"). Chaque solution y nous permet de construire un facteur h_y de $f_\ell^E(X)$ et on connaît ainsi explicitement l'isogénie ϱ_α puisque

$$\varrho_\alpha(x,y) = \left(\frac{k_\alpha(x)}{h_\alpha^2(x)}, \frac{g_\alpha(x,y)}{h_\alpha^3(x)}\right)$$

avec k_α un polynôme de degré ℓ à coefficients dans $\mathbb{F}_q$ et qui est donné explicitement en fonction de h_α.

En effet, connaissant l'équation d'une courbe elliptique E sur un corps K et les coordonnées des points d'un sous-groupe fini G de E, Vélu [41] donne les équations de la courbe isogène E/G et d'une isogénie $\mathcal{I} : E \longrightarrow E/G$. On donne ces équations en fonction du polynôme dont les racines sont les abscisses des points de G c'est à dire h.

On suppose que G ne possède pas de points d'ordre 2 et donc on peut écrire $G^* = S \cup (-S)$ avec $S \cap (-S) = \emptyset$. L'isogénie $\mathcal{I}$, de degré impair, admet les équations

$$\begin{cases} X_P = x_P + \sum_{Q \in S} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x-x_Q)^2} \right), \\ \\ Y_P = y_P - \sum_{Q \in S} \left(u_Q \frac{2y + a_1 x + a_3}{(x-x_Q)^3} + t_Q \frac{a_1(x-x_Q) + y - y_Q}{(x-x_Q)^2} + \frac{a_1 u_Q - \mathcal{F}_Q^x \mathcal{F}_Q^y}{(x-x_Q)^2} \right), \end{cases}$$

avec les notations

$$\begin{cases} Q = (x_Q, y_Q), \\ \mathcal{F}_Q^x = 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q, \ \mathcal{F}_Q^y = -2y_Q - a_1 x_Q - a_3, \\ u_Q = 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6, \ t_Q = 6x_Q^2 + b_2 x_Q + b_4. \end{cases}$$

On introduit de plus les notations suivantes :
$u = 4x^3 + b_2 x^2 + 2b_4 x + b_6, w = a_1 x + a_3, r = x^3 + a_2 x^2 + a_4 x + a_6$.
On obtient :

Proposition 31 *Soit G un sous-groupe d'ordre impair n de E . Soit $h = x^d - s_1 x^{d-1} + \ldots + (-1)^d s_d$ le polynôme dont les racines sont les abscisses des points de G. L'isogénie $\mathcal{I}$ est donnée par les relations :*

$$\begin{cases} X = nx - u(\frac{h'}{h})' - t\frac{h'}{h} - 2s_1, \\ \\ Y = y\frac{dX}{dx} - a_1(X - x) - \frac{1}{2}w(u\frac{h'}{h})'' + w'(r\frac{h'}{h})' - w(r'\frac{h'}{h}) + \\ (w + a_1 x)\frac{n-1}{2} - a_1 s_1. \end{cases}$$

L'équation de E/G est $Y^2 + A_1 XY + A_3 Y = X^3 + a_2 X^2 + a_4 X + A_6$ avec

$A_1 = a_1$, $A_2 = a_2$, $A_3 = a_3$, $A_4 = a_4 - 5(6s_1^2 - 12s_2 + b_2 s_1 + b_4)$,
$A_6 = a_6 - (70s_1^3 - 210 s_2 s_1 + 210 s_3 + 20 b_2 s_1^2 - 40 b_2 s_2 + (21 b_4 + b_2^2) s_1 + 7 b_6 + b_2 b_4)$.

Démonstration : On transforme chaque somme $\sum_{Q \in S} \frac{T(x_Q)}{(x-x_Q)^k}$ pour un polynôme T de degré au plus 3 et un entier $k = 1, 2, 3$ en écrivant S en puissances de $(x - x_Q)$ avec Taylor et en remarquant que $\sum_{Q \in S} \frac{1}{(x-x_Q)^k} = \frac{(-1)^{k-1}}{(k-1)!}(\frac{h'}{h})^{(k-1)}$.

On a, par exemple,

$$\frac{t_Q}{x - x_Q} = \frac{t}{x - x_Q} - (12x + b_2) + 6(x - x_Q)$$

et

$$\frac{u_Q}{(x - x_Q)^2} = \frac{u}{(x - x_Q)^2} - 2\frac{t}{x - x_Q} + (12x + b_2) - 4(x - x_Q),$$

ce qui donne

$$X = x + \sum_{Q \in S} \frac{u}{(x - x_Q)^2} - \frac{t}{x - x_Q} + 2(x - x_Q)$$

d'où le résultat.

Notons que la formule de Taylor n'a pas de sens en caractéristique 2 et 3. On peut néanmoins lui donner un sens puisque l'on peut simplifier T'' par 2! et T''' par 3!. □

Ces formules donnent donc explicitement les polynômes k_α et g_α en fonction du facteur h_α du polynôme de division f_ℓ.

3.4.2 Algorithme

On présente un algorithme de calcul de $t \bmod \ell^n$ lorsque ℓ est un nombre premier d'Elkies. Pour cela on détermine progressivement la décomposition ℓ-adique d'une valeur propre en avancant dans le cycle. L'algorithme s'exécute de la manière suivante [13] :

1. Trouver les racines de $\Phi_\ell(X, j(E)) = 0$ dans $\mathbb{F}_q$,
2. si Φ_ℓ a deux racines rationnelles distinctes alors
   (a) calculer l'équation $\mathcal{F}_\lambda$ de la courbe isogène E_λ. En déduire un facteur h_λ de f_ℓ^E et l'isogénie ϱ_λ,
   (b) déterminer la valeur propre λ en utilisant Müller,
   (c) pour $n = 2$ à $nmax$ faire :
      i. (Trouver la courbe suivante dans la direction λ.) Déterminer la racine F_{λ^n} de $\Phi_\ell(X, j(E_{\lambda^{n-1}})/(X - W_\ell(F_{\lambda^{n-1}})) = 0$. En déduire l'équation $\mathcal{F}_{\lambda^n}$ de E_{λ^n},
      ii. déterminer l'isogénie ϱ_{λ^n} entre $E_{\lambda^{n-1}}$ et E_{λ^n} et le facteur h_{α^n} de $f_\ell^{E_{\alpha^n}}$,
      iii. (Calcul du nouveau facteur de $f_{\ell^n}^E$.) On note h le numérateur de $h_{\lambda^n} \circ \varrho_{\lambda^{n-1}} \circ \ldots \circ \varrho_\lambda$,
      iv. (Trouver la valeur propre modulo ℓ^n.) trouver $\bar{\lambda}$, $0 \leq \bar{\lambda} < \ell$ tel que $\lambda_n = \lambda_{n-1} + \bar{\lambda}\ell^{n-1}$ satisfait à l'égalité $(X^q, Y^q) = [\lambda_{n-1}](X, Y) \oplus [\bar{\lambda}](\ell^{n-1}(X, Y))$ dans $\mathbb{F}_q[X, Y]/(\mathcal{F}_\lambda(X, Y), h(X))$.

3.4.3 Exemple

On considère la courbe elliptique E d'équation $y^2 = x^3 + 2x + 5$ sur $\mathbb{F}_{37}$. L'invariant modulaire de la courbe est $j(E) = 23$. On explicite un facteur du polynôme de division f_{49} de E. On a

$$\Phi_7(F, j(E)) = (4 + F)(25 + F)(27 + 28F + 3F^2 + F^3)(25 + 13F + 33F^2 + F^3)$$

sur $\mathbb{F}_{37}$. On choisit la racine $F_1 = 33$ et on trouve j_1 comme racine de $\Phi_7(7^2, x) \equiv 0 \bmod 37$. On obtient $j_1 = 27$. d'où E_1 a pour équation $y^2 = x^3 + 4x + 20$ et

$$h_1(x) = x^3 + 10x^2 + 35x + 35.$$

On en déduit

$$k_1(x) = x^7 + 20x^6 + 29x^5 + 4x^4 + 4x^3 + 22x^2 + 13x + 19.$$

On continue le procédé dans la même direction en considérant une racine de

$$\Phi_7(j_1, F) = (3+F)(28+F)(3+17F+13F^2+F^3)(30+4F+21F^2+F^3)$$

sur $\mathbb{F}_{37}$ et en écartant la racine $W_7(F_1) = 7^2/F_1 = 34$ car sinon on retournerait vers E. Ainsi, on prend $F_{11} = 9$ ce qui donne le facteur

$$h_{11} = 10 + 7x + 34x^2 + x^3$$

de $f_7^{E_1}$. Un facteur de f_{25}^E est alors le numérateur de $h_{11}(\varrho_1(X))$ c'est à dire

$$x^{21} + 20x^{20} + 4x^{19} + 16x^{18} + 33x^{17} + 3x^{16} + 15x^{15} + 5x^{14} + 6x^{13} + 25x^{12} + 27x^{11} + 2x^{10} + 2x^9 + 8x^8 + 23x^7 + 3x^6 + 6x^5 + 18x^4 + x^3 + 12x + 4$$

3.5 Améliorations

On voit facilement que l'algorithme marche si l'on remplace h_α par l'un de ces facteurs. Si on s'autorise la factorisation, on peut alors penser à passer, dans les cas favorables, d'un facteur h_ℓ^α irréductible à l'autre facteur h_ℓ^β de f_ℓ qui peut-être réductible. On sait depuis le chapitre I que le polynôme h_α se décompose en $d/s(\alpha)$ facteurs de degré $s(\alpha)$ où $s(\alpha)$ est le semi-ordre de la valeur propre α. En remplacant h_α par l'un de ces facteurs on peut calculer un facteur de degré $s(\alpha)\ell^{n-1}$ de f_{ℓ^n} en remontant un facteur de degré $s(\alpha)$ de f_ℓ^E. Cette approche nous suggère de prendre la direction de la valeur propre qui a le semi-ordre le plus petit. Mais cela nécessite la factorisation à chaque étape du polynôme h_α obtenu. Pour pallier cet inconvenient on utilise le changement de directions que l'on décrit maintenant. On verra ensuite que l'on peut en tirer un autre avantage.

3.5.1 Changer de directions

On considère dans ce paragraphe ℓ un nombre premier d'Elkies. On présente dans ce paragraphe une méthode qui va nous permettre de changer de facteur de f_ℓ^E (pour être plus précis on change de courbe donc de polynôme de division et par la même de facteur). Pour cela on utilise l'action de l'involution d'Atkin-Lehner W_ℓ qui permet de passer de ϱ à $\hat{\varrho}$ et donc de α à l'autre valeur propre β. Mais cette action nous fait passer sur la courbe isogène $\tilde{E}$. Or deux courbes isogènes ont le même nombre de points et par conséquent leur endomorphisme de Frobenius ont les mêmes valeurs propres. Pour être plus explicite, on détermine l'action de W_ℓ sur les formes modulaires (pour $SL_2(\mathbb{Z})$) $\mathcal{E}_2(z) = \ell E_2(\ell z) - E_2(z)$, $E_4(z)$ et $E_6(z)$ de poids 2, 4 et 6 respectivement. On a le schéma suivant :

$$
\begin{array}{lcll}
E & & \tilde{E} = E/G & \hat{E} \\
A = -3E_4(z) & \varphi & \tilde{A} = -3\ell^4 E_4(\ell z) & \hat{A} = -3\ell^4 E_4(z) \\
B = -2E_6(z) & \longrightarrow & \tilde{B} = -2\ell^6 E_6(\ell z) & \hat{B} = -2\ell^6 E_6(z) \\
p_1 = \frac{1}{2}\ell\mathcal{E}_2(z) & & \tilde{p}_1 = \frac{1}{2}\ell^3\mathcal{E}_2(\ell z) & \hat{p}_1 = \frac{1}{2}\ell^3\mathcal{E}_2(z) \\
p_2, p_3, \cdots & & \tilde{p}_2, \tilde{p}_3, \cdots & \hat{p}_2, \hat{p}_3, \cdots
\end{array}
$$

avec G un sous-groupe rationnel de $E[\ell]$ et p_1 la somme des abscisses des points de G.

Proposition 32 *Avec les notations précédentes, on a :*

$$
\begin{gathered}
\ell^2 W_\ell(A) = \tilde{A} \quad et \quad \ell^2 W_\ell(\tilde{A}) = \hat{A}, \\
\ell^3 W_\ell(B) = \tilde{B} \quad et \quad \ell^3 W_\ell(\tilde{B}) = \hat{B}, \\
\ell W_\ell(p_1) = \tilde{p}_1.
\end{gathered}
$$

Démonstration : Les formes modulaires de poids $2k$ pour un groupe Γ vérifie $f(\frac{az+b}{cz+d}) = (cz+d)^{2k} f(z)$ avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. En particulier, si f est de poids $2k$, alors $f(-1/\ell z) = (\ell z)^{2k} f(\ell z)$. L'action de W_ℓ sur une forme modulaire f de poids $2k$ est donnée par la relation $W_\ell(f)(z) = \ell^{-k} z^{-2k} f(-1/\ell z)$. Les égalités en découlent immédiatement. □

Proposition 33 *On a* $\tilde{p}_1 = -\ell p_1$.

Démonstration : On démontre d'abord que la forme modulaire $\mathcal{E}_2$, de poids 2, est anti-invariante, c'est à dire, par définition, $W_\ell(\mathcal{E}_2) = -\mathcal{E}_2$. En effet, on a
$(W_\ell(\mathcal{E}_2))(z) = \ell^{-1} z^{-2} \mathcal{E}_2(-1/\ell z) = \ell^{-1} z^{-2}(\ell E_2(-1/z) - E_2(-1/\ell z))$ ainsi

$$
(W_\ell(\mathcal{E}_2))(z) = \ell^{-1} z^{-2}\{\ell z^2 (E_2(z) + \frac{12}{2i\pi z}) - z^2\ell^2 (E_2(\ell z) + \frac{12}{2i\pi \ell z})\},
$$

d'où le résultat.

D'autre part, $W_\ell(\mathcal{E}_2)(z) = \ell^{-1} z^{-2} \mathcal{E}_2(-1/\ell z) = \ell\mathcal{E}_2(\ell z)$ car $\mathcal{E}_2$ est une forme modulaire de poids 2, ainsi $\ell\mathcal{E}_2(\ell z) = -\mathcal{E}_2(z)$ donc $\tilde{p}_1 = -\ell p_1$. □

On en déduit l'action de W_ℓ sur les p_k et par suite les valeurs des $\tilde{p}_k$ puisque l'on a les relations récurrentes (R_2) suivante :

$$
\tilde{A} - \ell^4 A = 5(6\tilde{p}_2 + 2\tilde{A}\tilde{p}_0),
$$

$$
\tilde{B} - \ell^6 B = 7(10\tilde{p}_3 + 6\tilde{A}\tilde{p}_1 + 4\tilde{B}\tilde{p}_0) \ldots .
$$

Exemple : On considère la courbe elliptique E d'équation $y^2 = x^3 + 2x + 5$ dans $\mathbb{F}_{53}$ d'invariant $j_0 = 51$. Les racines dans $\mathbb{F}_{53}$ de

$$
\Phi_7(F, 51) \equiv (8+F)(18+F)(31+39F+20F^2+F^3)(35+23F+35F^2+F^3)
$$

sont $F_\alpha = 35$ et $F_\beta = 45$. De $F_\alpha = 35$, on calcule les valeurs $p_1 = 7, p_2 = 22, p_3 = 47$ d'où

$$h_\alpha = 14 + 40x + 46x^2 + x^3$$

est un facteur de f_7^E. Ce facteur est irréductible sur $\mathbb{F}_{53}$. Calculons maintenant le facteur correspondant à l'autre valeur propre (remarquer que l'on change de courbes et donc de polynôme de division).

Des valeurs $\tilde{A} = 24, \tilde{B} = 51, \tilde{p}_1 = -7.7 = 4$ on peut calculer $\tilde{p}_1 = 4, \tilde{p}_2 = 44, \tilde{p}_3 = 19$ et donc

$$\tilde{h}_\beta = x^3 - 4x^2 + 6x - 9$$

est un facteur du polynôme de division $\tilde{f}_7^{E_\beta}$ de la courbe E_β d'équation $y^2 = x^3 + 24x + 51$ 7-isogène à E. Ce facteur est quant à lui réductible sur $\mathbb{F}_{53}$, en effet, on a

$$\tilde{h}_\beta = (x + 12)(x + 40)(x + 50).$$

A noter que cela signifie que la valeur propre β a un semi-ordre égal à 1.

On peut résumer le changement de directions de la manière suivante. L'approche d'Elkies est une procédure de construction des polynômes h_α à partir des quantités (A, B, p_1). On a démontré que le calcul de h_β est simplement l'application de cette procédure aux quantités $(\ell^4 A, \ell^6 B, -\ell p_1)$.

On décrit, maintenant, de manière plus algorithmique, comment l'involution d'Atkin-Lehner nous permet un déplacement dans un tableau de cycles de courbes ℓ-isogène.

3.5.2 Déplacement dans le cycle

On considère le schéma de courbes ℓ-isogène suivant :

$$\begin{array}{ccccc} E_{1,1} & \xrightarrow{\varrho_1^\beta} & E_{1,2} & \xrightarrow{\varrho_2^\beta} & E_{1,3} \quad \rightarrow \\ \varrho_1^\alpha \downarrow & & \hat{\varrho}_1^\beta \downarrow & & \hat{\varrho}_2^\beta \downarrow \\ E_{2,1} & \xrightarrow{\hat{\varrho}_1^\alpha} & E_{2,2} & \xrightarrow{\varrho_1^\beta} & E_{2,3} \quad \rightarrow \end{array}$$

La direction horizontale correspond à la valeur propre β et la direction verticale à α. Les courbes sur une même diagonale sont isomorphes.

Soient $E_{i,j}$ une courbe elliptique et ℓ un nombre premier d'Elkies pour lequel on a deux valeurs propres . On peut par la méthode habituelle déterminer deux facteurs $h_{i,j}^\alpha$ et $h_{i,j}^\beta$ de degré d du polynôme de division d'indice ℓ de $E_{i,j}$. L'action de l'involution W_ℓ permet de se déplacer dans le diagramme précédent. Ce déplacement se fait (malheureusement) en diagonale c'est à dire que l'on prend la direction perpendiculaire à celle que l'on a en utilisant (R_2).

Les formules de récurrences (R_1) et (R_2) permettent d'écrire :

$$R_1(A, B, p_1, \tilde{A}, \tilde{B}) = (p_k, k = 1, \ldots, d),$$
$$R_1^{-1}(A, B, p_1, p_2, p_3) = (\tilde{A}, \tilde{B}),$$

et

$$R_2(A, B, \tilde{p}_1, \tilde{A}, \tilde{B}) = (\tilde{p}_k, k = 1, \ldots, d),$$
$$R_2^{-1}(\tilde{A}, \tilde{B}, \tilde{p}_1, \tilde{p}_2, \tilde{p}_3) = (A, B).$$

A noter que l'on a également la relation importante suivante $\tilde{p}_1 = -\ell p_1$.
Considérons, maintenant, le diagramme suivant :

$$\begin{array}{ccccc} & & E_{i-1,j} & & \\ & & \downarrow & & \\ E_{i,j-1} & \rightarrow & E_{i,j} & \rightarrow & E_{i,j+1} \\ & & \downarrow & & \downarrow \\ & & E_{i+1,j} & \rightarrow & E_{i+1,j+1} \end{array}$$

On peut passer de $h_{i,j}^{\alpha}$ au polynôme $h_{i,j-1}^{\beta}$, en reculant dans le cycle, qui est un facteur du polynôme de division de $E_{i,j-1}$ ou de passer au polynôme $h_{i+1,j}^{\beta}$ en descendant dans le cycle. De même on peut passer de $h_{i,j}^{\beta}$ à $h_{i-1,j}^{\alpha}$ en remontant ou au polynôme $h_{i,j+1}^{\alpha}$ en avançant.

Explicitement, pour passer, par exemple, de $h_{i,j}^{\alpha}$ à $h_{i,j-1}^{\beta}$, on procède de la manière suivante :

1. on calcule $R_2^{-1}(A_{i,j}, B_{i,j}, p_{k_{i,j}}^{\alpha}(k = 1, 2, 3)) = (A_{i,j-1}, B_{i,j-1})$,
2. on calcule $p_{1_{i,j-1}}^{\beta} = -p_{1_{i,j}}^{\alpha}/\ell$,
3. et $R_1(A_{i,j-1}, B_{i,j-1}, p_{1_{i,j-1}}^{\beta}, A_{i,j}, B_{i,j}) = p_{k_{i,j-1}}^{\beta}$.

Ce procédé se simplifie en remarquant que $E_{i,j-1} \simeq E_{i+1,j}$ ce qui permet de supprimer l'utilisation de (R_2). Il suffit donc de calculer

$$R_1(A_{i+1,j}/\ell^4, B_{i+1,j}/\ell^6, -p_{1_{i,j}}^{\alpha}/\ell, A_{i,j}, B_{i,j})$$

pour déterminer le polynôme $h_{i,j-1}^{\beta}$.

Nous allons voir deux applications pratiques de cette notion de déplacement. La première consiste à réduire à une seule factorisation l'utilisation d'un facteur de h_{α} dans le cycle. La seconde consiste à determiner un facteur de f_{ℓ^2} en utilisant qu'une seule détermination de racines de l'équation modulaire.

3.5.3 Applications

Notons, à titre d'exemple, que l'on peut avoir un facteur du polynôme de division f_{ℓ^2} de la courbe elliptique $E_{i,j-1}$ à partir de $h^{\beta}_{i,j-1}$ et $h^{\beta}_{i,j}$ et donc en ne calculant qu'un seul pgcd.

Exemple : On considère la courbe elliptique E d'équation $y^2 = x^3 + 23x + 39$ sur $\mathbb{F}_{53}$. On veut déterminer un facteur de f_{25} de E ce qui est possible puisque 5 est un nombre premier d'Elkies. On obtient, tout d'abord,

$$h_{\alpha^2} = x^2 + 17x + 28$$

avec la première courbe 5-isogène à E d'équation $y^2 = x^3 + 46x + 11$ obtenue à partir de $F_\alpha = 5$ et $h_{\alpha\beta} = x^2 + 47x + 47$ avec la courbe dans l'autre direction d'équation $y^2 = x^3 + 31x + 13$ ($F_\beta = 11$).

La courbe qui précède E est $(31/5^4, 13/5^6) = (2,4)$ ce qui simplifie les relations de récurrence R_2 en $\tilde{p}_1 = -\ell p_1$ et permet le calcul d'un facteur du polynôme de division de la courbe $(2,4)$ avec (R_1) : on obtient

$$h_\alpha = x^2 + 33x + 27.$$

Avec les polynômes h_α et h_{α^2} on détermine, en calculant le numérateur de $h_{\alpha^2} \circ \varrho_\alpha$ un facteur du polynôme f_{25} de $(2,4)$ à savoir

$$h_{25} = 7 + x + 30x^2 + 44x^3 + 38x^4 + 2x^5 + 45x^6 + 5x^7 + 44x^8 + 43x^9 + x^{10}.$$

Toutefois, au lieu d'utiliser "l'inversion" des formules d'Elkies introduite précédemment, on peut employer efficacement les isomorphismes présents dans les cycles. Cela permet de changer de courbes de manière plus rapide du point de vue de la complexité [14]. En effet, à partir de la proposition décrite précédemment, on a immédiatement :

$$\begin{array}{ccc} E & \xrightarrow{\varrho_1} & E_1 \\ \varrho_1 \downarrow & \overset{i_0}{\nwarrow} & \varrho_{1,2} \downarrow \\ E_2 & & E_{1,2} \end{array}$$

Si $E = [A,B]$ alors $E_{12} = [\ell^4 A, \ell^6 B]$ et $i_0 : (X,Y) \mapsto (X/\ell^2, Y/\ell^3)$. De plus, E_{12} peut-être construite à partir de E_1 utilisant $W_\ell(F_1)$ (avec F_1 la racine dans la direction E_1) et $p_1(E_{1,2}) = -\ell p_1(E)$.

- Première améliorations :

Comme nous l'avons déjà dit, on peut, lorsque ℓ n'est pas trop grand, utiliser efficacement la possible réductibilité du facteur h de f_ℓ trouvé. On sait qu'il faut d'abord prendre la

direction ayant un semi ordre le plus faible (on aura ainsi l'un des facteurs de plus bas degré de f_ℓ). Mais, si l'on veut itérer cette idée dans l'algorithme de calcul de t mod ℓ^n, il faut factoriser le polynôme h à chaque étape de l'algorithme (à chaque utilisation d'une isogénie). On montre comment procéder pour ne faire qu'une factorisation de polynôme. On se réfère ici aux travaux de François Morain [14]. Considérons le diagramme suivant (pour simplifier, on a adopter la notation suivante $E_{\alpha^2\beta^3} = E_{2,3}$) :

$$\begin{array}{ccccccc} E_{1,1} & \xrightarrow{\varrho_1^\beta} & E_{1,2} & \xrightarrow{\varrho_2^\beta} & E_{1,3} & \xrightarrow{\varrho_3^\beta} & E_{1,4} \\ & \overset{i_0}{\nwarrow} & \hat{\varrho}_1^\beta \downarrow & \overset{i_1}{\nwarrow} & \hat{\varrho}_2^\beta \downarrow & \overset{i_2}{\nwarrow} & \hat{\varrho}_3^\beta \downarrow \\ & & E_{2,2} & & E_{2,3} & & E_{2,4} \end{array}$$

Rappelons que pour le calcul de t mod ℓ^n on peut commencer par n'importe qu'elle courbe de ce diagramme puisque qu'elles ont toutes le même nombre de points défini sur $\mathbb{F}_q$.

Considérons $\hat{h}^\beta$ un facteur du polynôme de division $f_\ell^{E_{1,2}}$ obtenu dans la direction α. Alors le numérateur de $\hat{h}^\beta \circ i_1 \circ \hat{\varrho}_2^\beta$ nous donne un facteur $\hat{h}^{\beta^2}$ de $f_{\ell^2}^{E_{1,3}}$ obtenu toujours dans la direction de α. De la même manière, on obtient un facteur $\hat{h}^{\beta^3}$ de $f_{\ell^3}^{E_{1,4}}$ comme étant le numérateur de $\hat{h}^{\beta^2} \circ i_2 \circ \hat{\varrho}_3^\beta$.

On résume la méthode dans l'algorithme suivant :

1. Trouver les racines de $\Phi_\ell(X, j(E)) = 0$ dans $\mathbb{F}_q$,
2. si Φ_ℓ a deux racines rationnelles distinctes alors
   (a) calculer un facteur h de f_ℓ^E,
   (b) déterminer la valeur propre correspondante α et en déduire l'autre valeur propre β,
   (c) renommer les directions de telle manière que la direction de la valeur propre β soit celle dont le semi-ordre soit le plus faible. Calculer le facteur h de $h_{\alpha\beta}$ de plus bas degré et poser $\lambda_1 = \beta$.
   (d) pour $n = 2$ à $nmax$ faire :
      i. (Trouver la courbe suivante dans la direction β.) Calculer $E_{1,n}$, $E_{2,n}$ et $\hat{\varrho}_n^\beta$,
      ii. (Calcul du nouveau facteur.) On note h le numérateur de $h \circ i_{n-1} \circ \hat{\varrho}_n^\beta \circ \ldots \circ \varrho_\lambda$ (Le polynôme h est alors un facteur du polynôme de division $f_{\ell^n}^{E_{1,n}}$ de degré $s(\beta)\ell^{n-1}$))
      iii. (Trouver la valeur propre modulo ℓ^n.) trouver $\bar{\lambda}$, $0 \leq \bar{\lambda} < \ell$ tel que $\lambda_n = \lambda_{n-1} + \bar{\lambda}\ell^{n-1}$ satisfait à l'égalité $(X^q, Y^q) = [\lambda_{n-1}](X, Y) \oplus [\bar{\lambda}](\ell^{n-1}(X, Y))$ dans $\mathbb{F}_q[X, Y]/(\mathcal{F}_\lambda(X, Y), h(X))$.

- **Seconde améliorations :**

On peut tirer un autre avantage du saut de courbes en utilisant la décomposition atypique sur $\mathbb{F}_q$ du polynôme $\Phi_\ell(X, j(E))$. En effet, lorsque l'on recherche une racine dans $\mathbb{F}_q$ de l'équation $\Phi_\ell(X, j(E)) = 0$ et que ℓ est un nombre premier d'Elkies on a immédiatement les deux racines F_α et F_β et donc h_α et h_β. En remontant dans le cycle le polynôme h_α ou h_β, on a directement un facteur du polynôme f_{ℓ^2} sans recalculer de pgcd (dans la méthode originale on doit calculer le

$$\text{pgcd}(X^q - X, \Phi_\ell(X, j(E_\alpha))/(X - W_\ell(F_\alpha))$$

pour avoir la valeur de F_{α^2}). De cette manière, on ramène le calcul de $t \bmod \ell^n$ à celui de $t \bmod \ell^{n/2}$ en ne calculant un pgcd qu'une fois sur deux. Pour transcrire cette idée sur le plan algorithmique nous allons nous déplacer à reculons dans le cycle. Pour cela on note ${}_{m,n}E$ la courbe elliptique dans la position m, n, c'est à dire m courbes avant $E_{1,1}$ dans la direction β et n courbes avant $E_{1,1}$ dans la direction α. On prend une notation similaire pour les isogénies. Considérons alors le diagramme suivant :

$$\begin{array}{ccccccc}
{}_{3,1}E & \xrightarrow{\varrho^\beta_{-3}} & {}_{2,1}E & \xrightarrow{\varrho^\beta_{-2}} & {}_{1,1}E & \xrightarrow{\varrho^\beta_{-1}} & E_{1,1} \\
 & \overset{i_{-3}}{\nwarrow} & \hat{\varrho}^\beta_{-2}\downarrow & \overset{i_{-2}}{\nwarrow} & \hat{\varrho}^\beta_{-1}\downarrow & \overset{i_1}{\nwarrow} & \hat{\varrho}^\beta_1\downarrow \\
 & & {}_{2,2}E & & {}_{2,1}E & & E_{2,1}
\end{array}$$

Le facteur de ${}_1h$ de $f_\ell^{1,1E}$ est le numérateur de $h_1 \circ \varrho^\beta_{-1}$. De la même manière, on obtient un facteur de $f_{\ell^3}^{2,1E}$ en déterminant le numérateur de $h_1 \circ \varrho^\beta_{-1} \circ \varrho^\beta_{-2}$ ou de façon équivalente comme le numérateur de ${}_1h \circ \varrho^\beta_{-2}$.

On résume la méthode dans l'algorithme (de Morain) qui suit :

1. Trouver les racines de $\Phi_\ell(X, j(E)) = 0$ dans $\mathbb{F}_q$,
2. si Φ_ℓ a deux racines rationnelles distinctes alors
   (a) calculer un facteur h_α de f_ℓ^E,
   (b) déterminer α et en déduire β,
   (c) renommer les directions de telle manière que la direction de la valeur propre β soit celle dont le semi-ordre soit le plus faible. Calculer le facteur h de h_α de plus bas degré et poser $\lambda_1 = \beta$,
   (d) Déterminer E_2 en utilisant la seconde racine de $\phi_\ell(X, j(E))$,
   (e) pour $n = 2$ à $nmax$ faire :
      i. (Trouver la courbe précédente dans la direction β.) Calculer ${}_{1,n}E$ utilisant l'isomorphisme i_{-1} et poser ${}_1F = W_\ell(F_2)$.

ii. Calculer l'isogénie ϱ^{β}_{-1} entre les courbes ${}_{1,1}E$ et E.

iii. (Calcul du nouveau facteur.) déterminer h le numérateur de $h \circ \varrho^{\beta}_{-1}$. (Le polynôme h est alors un facteur du polynôme de division $f^{E_{1,n}}_{\ell^n}$ de degré $s(\beta)\ell^{n-1}$).

iv. (Trouver la valeur propre modulo ℓ^n.) Trouver $\bar{\lambda}$, $0 \leq \bar{\lambda} < \ell$ tel que $\lambda_n = \lambda_{n-1} + \bar{\lambda}\ell^{n-1}$ satisfait à l'égalité $(X^q, Y^q) = [\lambda_{n-1}](X,Y) \oplus [\bar{\lambda}](\ell^{n-1}(X,Y))$ dans $\mathbb{F}_q[X,Y]/(\mathcal{F}_\lambda(X,Y), h(X))$.

v. Si $n > nmax$ alors

   A. Calculer l'autre racine ${}_{2,1}F$ de $\phi_\ell(X, j({}_1E))$ en calculant

$$\text{pgcd}(X^q - X, \phi_\ell(X, j({}_1E))/(X -_{21} F))$$

   et en déduire ${}_{21}E$,

   B. Poser $F_2 =_{21} F, E_2 =_{21} E$ et $E =_1 E$,

Bibliographie

[1] V. AHO, HOPCROFT, ULLMAN : *The design and analysis of computer algorithms.* Addison-Wesley 1974.

[2] A. O. L. ATKIN : *The number of points on an elliptic curve modulo a prime (I).* Draft, 1988.

[3] A. O. L. ATKIN : *The number of points on an elliptic curve modulo a prime (II).* Draft, 1992.

[4] 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).pp153.174

[5] R.P. BRENT, H.T. KUNG : *Fast algorithms for manipulating formal power series.* J.Assoc.Comput.Mach.,25:581-595,1978.

[6] J. BUCHMANN, V. MÜLLER : *Computing the number of points of elliptic curves over finite fields.* In ISSAC'91, S.M.Watt, Ed., pp179-182. Proceedings of the International Symposium on Symbolic and Algebraic Computation, July 15-17, Bonn, Germany.

[7] L. CHARLAP, D. ROBBINS : *An elementary introduction to elliptic curves.* CRD Expository Report n31, Institute for defense Analyses Princeton, December 1988.

[8] L. S. CHARLAP, R. COLEY, D. P. ROBBINS : *Enumeration of rational points on elliptic curves over finite fields.* Draft,1991.

[9] H. COHEN : *A course in algorithmic algebraic number theory.* Graduate Texts in Math.138, Springer Verlag Berlin-Heidelberg-New-York 1993.

[10] J.M COUVEIGNES : *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, Juillet 1994.

[11] J.M COUVEIGNES : *Computing isogenies in any characteristic.* En préparation, 1995.

[12] J.M COUVEIGNES : *Computing ℓ isogenies with the p-torsion.* A paraitre dans Proc. of ANTS-II, Janvier 1996.

[13] J-M COUVEIGNES, F. MORAIN : *Schoof's algorithm and isogeny cycles.* In L.Adleman and M.-D Huang, editors, ANTS-I, volume 877 of lectures Notes in Comput. Sci., pages 43-58. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, Mai 6-9, 1994.

[14] J-M COUVEIGNES,L. DEWAGHE, F. MORAIN : *Isogeny cycles and the Schoof-Elkies-Atkin algorithm.* Rapport de Recherches LIX/RR/96/03, Ecole polytechnique - LIX, Août 1996.

[15] L. DEWAGHE : *Polynômes de division et "associés" à une courbe elliptique E définie sur* $\mathbb{F}_p$. En préparation, Mai 1995.

[16] MC.ELIECE : *Finite fields for computer scientists and engineers.* Kluwer Boston 1987.

[17] N. D. ELKIES : *Explicit Isogenies.* Draft, 1991.

[18] S. GOLDWASSER, J. KILLIAN : *Almost all prime can be quickly certified.* In Proc 18th. STOC (berkeley, May 1986, 28-30) pp 316-323.

[19] D. HUSEMÖLLER : *Elliptic curves.* Volume 111 de Graduate Texts in Mathematics. Springer, 1987.

[20] D. E. KNUTH : *The Art of Computer Programming : Seminumerical Algorithms.* Addison-Wesley, 1981.

[21] N. KOBLITZ : *Introduction to elliptic curves and modular forms.* Graduate Texts in Math.97, Springer Verlag Berlin-Heidelberg-New-York 1984.

[22] N. KOBLITZ : *Elliptic curve cryptosystems.* Math.Comp.(48) : 203-209, 1987.

[23] N. KOBLITZ : *CM curves with cryptographic properties.* Advance in Cryptology. Proc. Crypto. 91 ; Lectures Notes in Computer Sciences, Vol 537. Springer Verlag. Berlin (1992),279-287.

[24] S. LANG : *Elliptic Functions.* Addison Wesley, Reading MA, 1973.

[25] F. LEHMANN, M. MAURER, V. MÜLLER AND V. SHOUP : *Counting the number of points on an elliptic curves over finite fields of characteristic greater than three.* In ANTS I (1994), L.Adleman and M.-D. Huang, Eds., vol.877 de Lectures Notes in Comput. Sci., Springer-Verlag, pp 60-70. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[26] R. LERCIER : *Computing isogenies in characteristic* 2. A paraitre dans Proc. of ANTS-II, Décembre 1995.

[27] R. LERCIER, 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 cryptology - EUROCRYPT'95, number 921 in Lectures notes in Comput. Sci. pp79-94, 1995. Internationnal conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, Mai 1995, Proceedings.

[28] R. LERCIER, F. MORAIN : *Counting points on elliptic curves over $\mathbb{F}_{p^n}$ using Couveignes's algorithm.* Rapport de Recherches LIX/RR/95/09, Ecole polytechnique - LIX, Septembre 1995.

[29] A.MENEZES, S.VANSTONE, R.ZUCCHERATO : *Counting points on elliptic curves over $\mathbb{F}_{2^m}$* . Math. Comp.(60) : 407-420, 1993.

[30] V. MILLER : *Use of elliptic curve in cryptography.* Advance in Cryptology. Proc.Crypto.85 ; Lectures notes in Computer Sciences, Vol 218. Springer Verlag.Berlin (1985),417-426.

[31] 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.

[32] F. MORAIN : *Record.* e-mail 26 Janvier 1995.

[33] V.MÜLLER : *Looking for the eigenvalue in Schoof's algorithm.* en préparation, Octobre 1994.

[34] A. ODLYZKO : *Discrete logarithms and their cryptographic significance.* Advances in Cryptology : Proceedings of Eurocrypt 84, Lectures Notes in Computer Science 209 (1985), Springer Verlag, 224-314.

[35] R. SCHOOF : *Elliptic curves over finite fields and the computation of square roots mod p.* Math.Comp.(44) : 483-494, 1985.

[36] R. SCHOOF : *Counting points on elliptic curves over finite fields.* J. Théor. Nombres Bordeaux 7 (1995), 219-254.

[37] J. P SERRE : *Cours d'arithmétique.* P.U.F 1970.

[38] D. SHANKS : *Class number, A theory of factorization and genera.* Proc;Sympos.Pure Math. Vol.20,Amer.Math.Soc. 1970,415-440

[39] V.SHOUP : *A new polynomial factorization algorithm and its implementation.* J Symbolic Comput. (1995) Vol 20, 363-397.

[40] J. H. SILVERMAN : *The arithmetic of elliptic curves, vol 106 of Graduate Texts in Mathematics.* Spinger, 1986.

[41] J. VÉLU : *Isogenies entre courbes elliptiques.* Comptes rendus de l'Acad. des sciences de Paris A273(7/1971) : 238-241.

Table des matières