Calcul d'isogénies entre courbes elliptiques

Introduction au domaine de recherche

Jean Kieffer

16 octobre 2017

Table des matières

1 Courbes elliptiques et isogénies **2**

2 Calcul d'isogénies **3**
2.1 Un peu d'histoire. 3
2.2 Les formules de Vélu. 4
2.3 La méthode de Stark. 5
2.4 La méthode d'Elkies. 6
2.5 L'algorithme de Couveignes. 8

3 Application au comptage de points **9**

Introduction

Une *isogénie* est un morphisme surjectif et de noyau fini entre variétés abéliennes. Ce sont des objets fondamentaux dans l'étude de ces variétés, et donc des courbes algébriques en général. Dans ce document, on parlera plus spécifiquement de *courbes elliptiques*, qui sont des variétés abéliennes de dimension 1 ; les isogénies sont les flèches non triviales dans la catégorie des courbes elliptiques sur un corps k donné, et ce sont des *quasi-isomorphismes* dans un certain sens.

Les isogénies sont aussi étroitement liées aux *sous-groupes de torsion* sur les courbes elliptiques. Un sous-groupe fini d'une courbe elliptique est toujours le noyau d'une isogénie, déterminée à isomorphisme près, et il est souvent intéressant de travailler avec celle-ci.

Vu ces liens profonds avec les sous-groupes de torsion d'une courbe et leur rôle de quasi-isomorphisme, les isogénies sont des objets centraux lorsque l'on regarde des représentations de Galois attachées aux courbes, des questions de modularité, ou les questions liées à la conjecture de Birch et Swinnerton-Dyer : en un mot, dans toutes les situations où l'on regarde les courbes

elliptiques comme *plus* qu'un simple groupe de points. Savoir *calculer* avec des isogénies est alors essentiel pour faire quoi que ce soit.

Ce document est organisé comme suit. Dans un premier temps, on expose le matériel nécessaire (courbes elliptiques et isogénies), et on présente ensuite différentes méthodes pour le calcul d'isogénies (des *algorithmes*, donc). Enfin on s'intéresse à une application au comptage de points d'une courbe elliptique sur un corps fini.

1 Courbes elliptiques et isogénies

Soit k un corps. Une *courbe elliptique* E sur k est une courbe algébrique projective, lisse, de genre 1 munie d'un point rationnel fixé 0_E. Par exemple, la courbe plane projective donnée sous *forme de Weierstrass* (réduite)

$$y^2 = x^3 + ax + b, \quad \text{où } a, b \in k \text{ et } 4a^3 - 27b^2 \neq 0$$

munie du point fixé $(0 : 1 : 0)$, est une courbe elliptique. On peut en fait montrer qu'en dehors des caractéristiques 2 et 3, toute courbe elliptique admet une équation de ce type. Si E est sous forme de Weierstrass comme ci-dessus, on peut la munir d'une forme différentielle sans zéros ni pôles :

$$\omega_E = \frac{dx}{y}.$$

Toutes les autres telles formes différentielles sont des multiples de ω_E : c'est ce que signifie *être une courbe de genre 1.*

Une propriété essentielle est que l'ensemble $E(K)$ des points de E sur tout corps K extension de k est un groupe abélien d'élément neutre le point marqué. Trois points alignés sont de somme nulle ; on peut utiliser cette propriété pour donner des formules explicites de cette loi de groupe dans les coordonnées x, y.

Une *isogénie* est un morphisme non nul $\phi : E \to E'$ entre courbes elliptiques. C'est un morphisme de groupes, mais aussi une application *régulière*, donnée par des fractions rationnelles en x, y : on appelle *degré* de l'isogénie le degré de ces fractions. C'est aussi, en général (dans le cas *séparable*, auquel on se restreint dans ce document) le nombre de préimages de chaque point : ainsi, le noyau d'une isogénie de degré ℓ sera un sous-groupe de cardinal ℓ. Le pullback $\phi^*\omega'_E$ est un multiple de ω_E : on en déduit qu'il existe un certain c et une fraction rationnelle ϕ_x tels que

$$\phi(x, y) = (\phi_x(x), cy\phi'_x(x)).$$

Les *endomorphismes* de E sont les isogénies de E vers E, plus 0. Par exemple, les multiplications scalaires pour $m \in \mathbb{Z}$

$$[m]_E : P \mapsto P + \cdots + P, \quad m \text{ fois}$$

sont des endomorphismes. L'isogénie $[m]$ est de degré m^2, et son noyau est noté $E[m]$, le sous-groupe des *points de m-torsion* de la courbe. En utilisant la loi de groupe, on peut calculer explicitement un polynôme de degré m^2-1 s'annulant sur les points de $E[m]$, le *polynôme de m-division* de E.

Cela donne une copie de $\mathbb{Z}$ à l'intérieur de $\mathrm{End}(E)$. Ce ne sont pas toujours les seuls endomorphismes, et même *jamais* lorsque k est un corps fini de cardinal q : le *morphisme de Frobenius*

$$\pi_E : (x, y) \mapsto (x^q, y^q)$$

est un endomorphisme qui n'est pas une multiplication scalaire [1].

Si E est une courbe elliptique sur $\mathbb{C}$, on montre que E est isomorphe à un *tore complexe* :

$$E \simeq \mathbb{C}/\Lambda, \quad \Lambda \text{ réseau de } \mathbb{C}.$$

La loi de groupe sur E coïncide avec celle de $\mathbb{C}/\Lambda$, et les isogénies deviennent simplement la multiplication par un nombre complexe : on a une isogénie $[\alpha] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ dès que $\alpha \in \mathbb{C}^*$ vérifie $\alpha\Lambda \subset \Lambda'$. Par exemple, le noyau de la multiplication scalaire $[m]$ est alors $E[m](\mathbb{C}) = \frac{1}{m}\Lambda/\Lambda$, un groupe isomorphe à $(\mathbb{Z}/m\mathbb{Z})^2$.

Les endomorphismes de E sont alors les $\alpha \in \mathbb{C}$ tels que $\alpha\Lambda \subset \Lambda$. Souvent, seuls les éléments de $\mathbb{Z}$ conviennent, mais pour certains réseaux, des endomorphismes supplémentaires apparaissent. L'anneau $\mathrm{End}(E)$ est dans ce cas un $\mathbb{Z}$-module de dimension 2 (en fait, un *ordre* $\mathcal{O}$ dans un corps quadratique imaginaire) ; on dit que E a *multiplication complexe* par $\mathcal{O}$.

Les références souvent données pour l'étude des courbes elliptiques sont [15, 16] ; voir aussi [13] pour un traitement plus moderne.

2 Calcul d'isogénies

2.1. Un peu d'histoire. « Calculer » une isogénie $\phi : E \to E'$ peut avoir plusieurs significations. Dans ce document, on s'intéresse à deux situations :

- On connaît E et $\mathrm{Ker}\,\phi$, et l'on souhaite calculer une équation de E' ainsi que des fractions rationnelles définissant ϕ (en somme, on souhaite construire un quotient *explicitement*).
- On connaît E, E' et éventuellement le degré de ϕ, et l'on souhaite retrouver le noyau de ϕ et des fractions rationnelles la définissant. On demande donc de calculer entièrement une isogénie lorsque l'on sait qu'elle existe.

1. Ce n'est pas tout à fait exact : il existe des exceptions lorsque q est un carré et E est une courbe elliptique *supersingulière*. Son anneau d'endomorphismes est cependant toujours plus grand que $\mathbb{Z}$.

La première question est résolue à l'aide des formules de Vélu, proposées en 1971 [19]. De nombreuses méthodes ont vu le jour pour calculer le noyau d'une isogénie, en commençant par la méthode de Stark [17], publiée en 1972 et qui concerne les endomorphismes d'une courbe elliptique à multiplication complexe.

L'histoire récente commence avec les travaux d'Elkies dans les années 1990 : il s'inspire des travaux de Stark et Vélu pour calculer les fractions rationnelles d'une isogénie, à condition qu'elle soit *normalisée*. Il fait circuler un manuscrit en 1991–92 (« Explicit isogenies ») puis en publie une version étendue en 1998 [5]. Dans le même temps, des techniques sont développées par Atkin, sous la forme de mails principalement : on peut trouver certains manuscrits à l'adresse `http://www.lix.polytechnique.fr/Labo/Francois.Morain/`. Ces méthodes ont fait l'objet d'articles au journal de théorie des nombres de Bordeaux [14, 12].

Il n'existe alors pas d'algorithme fonctionnant en petite caractéristique. En 1994, Couveignes publie sa thèse [2] contenant un algorithme à base de groupes formels qui résout ce problème. Cet algorithme est complexe, et cela pousse Lercier à développer en 1996 un algorithme dans le cas de la caractéristique 2 [10] de complexité non prouvée, mais très intéressant en pratique. Ce travail est ensuite généralisé par Couveignes [3], qui propose un algorithme basé sur l'*interpolation* de l'isogénie en certains points de la courbe.

Les progrès réalisés depuis prennent surtout la forme d'améliorations et généralisations de méthodes existantes : Bostan, Morain, Salvy et Schost améliorent en 2008 la méthode d'Elkies [1], Lercier et Sirvent proposent de l'utiliser après un relèvement dans les nombres p-adiques pour pouvoir l'utiliser en petite caractéristique [11], Lairez et Vaccon [9] précisent la précision p-adique nécessaire à cette dernière méthode. De Feo, dans sa thèse [6] et des articles ultérieurs [7] développe la méthode de Couveignes.

Après la présentation des formules de Vélu, on s'intéressera tout d'abord à la méthode de Stark, pour son intérêt historique et son caractère élémentaire, ainsi qu'à la méthode d'Elkies. On présente également la méthode d'interpolation de Couveignes, qui fournit une solution simple au problème du calcul d'isogénies en petite caractéristique.

2.2. Les formules de Vélu. Soit E une courbe elliptique donnée sous forme de Weierstrass

$$y^2 = x^3 + ax + b.$$

La question posée par Vélu [19] est la suivante : connaissant un sous-groupe fini G de $E(\bar{k})$, comment déterminer une isogénie dont ce sous-groupe est le noyau ? On supposera $\mathrm{Card}(G)$ impair pour simplifier.

Afin de déterminer une équation de la courbe image, on cherche des fonctions rationnelles x', y' sur E, G-périodiques et de degrés respectifs 2 et 3 (comme les x, y d'une équation de Weierstrass). On définit ainsi

$$\begin{aligned} x'(P) &= \sum_{g\in G} x(P+g) - \sum_{g\in G\setminus\{0_E\}} x(g), \\ y'(P) &= \sum_{g\in G} y(P+g) \end{aligned}$$

pour tout point $P \in E(\bar{k})$. Pour trouver une équation satisfaite par ces deux fonctions (c'est-à-dire l'équation de la courbe image), on trouve des fractions rationnelles f, g telles que $x' = f(x)$ et $y' = y\,g(x)$: on regroupe les termes $P+g$ et $P-g$, on utilise la loi de groupe et on trouve

$$\begin{aligned} x' &= x + \sum_{g\in G\setminus\{0_E\}} \left[\frac{3x^2(g)+a}{x-x(g)} + 2\frac{x^3(g)+ax(g)+b}{(x-x(g))^2}\right], \\ y' &= y - y\sum_{g\in G\setminus\{0_E\}} \left[\frac{3x^2(g)+a}{(x-x(g))^2} + 4\frac{x^3(g)+ax(g)+b}{(x-x(g))^3}\right]. \end{aligned} \tag{1}$$

On développe ces expressions en puissances négatives de x et on en déduit l'équation

$$y'^2 = x'^3 + a'x' + b'$$

avec

$$\begin{aligned} a' &= a - 5\sum_{g\in G\setminus\{0_E\}} (3x^2(g)+a) \\ b' &= b - 7\sum_{g\in G\setminus\{0_E\}} (5x^3(g)+3ax(g)+2b). \end{aligned} \tag{2}$$

Le terme constant de x a été ajusté pour trouver une équation réduite. On a ainsi l'équation de la courbe image, et les expressions (1) donnent l'isogénie sous forme de fractions rationnelles. Les relations (2) sont souvent exprimées en fonction des coefficients du polynôme dont les $x(g)$ sont les racines.

2.3. La méthode de Stark. Stark [17] s'intéresse au calcul d'endomorphismes d'une courbe elliptique E à multiplication complexe par $\mathcal{O}$, définie par exemple sur une extension finie de $\mathbb{Q}$ et donnée par une équation de la forme

$$y^2 = x^3 - ax - b.$$

On a vu qu'il existe un réseau Λ de $\mathbb{C}$ tel que $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Ce paramétrage est donné par

$$z \mapsto \left(\wp(z), \frac{\wp'(z)}{2}\right)$$

pour $z \in \mathbb{C}/\Lambda$, où $\wp$ est la fameuse *fonction de Weierstrass* associée à Λ. Si $\beta \in \mathcal{O}$, on a un endomorphisme $[\beta]_E$ de E qui s'écrit $z \mapsto \beta z$ dans le point de vue du tore complexe.

La question est alors d'exprimer cet endomorphisme du point de vue « algébrique » plutôt qu'analytique, c'est à dire en tant qu'application rationnelle sur la courbe E. Cela revient à trouver une fraction rationnelle f telle que l'on ait l'égalité de fonctions méromorphes sur $\mathbb{C}$:

$$\wp(\beta z) = f(\wp(z)).$$

La fraction f donne alors la coordonnée x de l'endomorphisme $[\beta]_E$. En regardant les zéros et pôles de ces séries de Laurent, on peut savoir que f s'écrit $\frac{p}{q}$, où les polynômes p et q sont de degrés respectifs $|\beta|^2$ et $|\beta|^2 - 1$. La quantité $|\beta|^2$ est le degré de cet endomorphisme.

Pour calculer ces deux polynômes, Stark utilise un algorithme de décomposition en *fraction continue* inspiré des nombres réels. Lorsque l'on se donne $\alpha \in \mathbb{Q}$, on définit $\alpha_0 = \alpha$ et pour tout $j \geq 0$,

$$a_j = \lfloor \alpha_j \rfloor, \quad \alpha_{j+1} = \frac{1}{\alpha_j - a_j}$$

et l'on s'arrête lorsque $\alpha_j = a_j$. Le rationnel α est alors égal à

$$\frac{p_j}{q_j} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_j}}}.$$

Le principe est exactement le même ici, et cela permet d'écrire facilement $\wp(\beta z)$ sous forme de fraction rationnelle en $\wp(z)$.

Bien sûr, on manipule dans cet algorithme uniquement un nombre *fini* de coefficients des séries de Laurent comme $\wp(z)$. On connaît le degré des polynômes p, q obtenus à la fin de l'algorithme, ce qui permet de contrôler le nombre de coefficients nécessaire au calcul. Ces coefficients sont obtenus à l'aide de l'équation différentielle $\wp'^2 = 4\wp^3 + 4a\wp + 4b$:

$$\wp(z) = \frac{1}{z^2} + \frac{a}{5}z^2 + \frac{b}{7}z^4 + \cdots$$

Telle qu'exposée ci-dessus, la méthode de Stark ne s'applique qu'à des endomorphismes et non à une isogénie générale.

2.4. La méthode d'Elkies. Les calculs proposés par Elkies [5] partent de l'idée d'« inverser » les formules de Vélu. Soit $\phi : E \to E'$ une isogénie de degré ℓ, avec $\ell = 2n + 1$ impair (on conserve cette simplification ici).

On se donne une équation de Weierstrass pour E et E' ; cette donnée est équivalente à celles de formes différentielles ω_E et $\omega_{E'}$. On dit que ϕ est *normalisée* si $\phi^*\omega_{E'} = \omega_E$.

On peut voir que l'isogénie quotient $E \to E/G$ donnée par les formules de Vélu est normalisée. L'idée d'Elkies est alors la suivante : *si ϕ est normalisée, alors l'équation de Weierstrass de E' est celle que l'on aurait obtenue en appliquant les formules de Vélu à partir de* $\operatorname{Ker}\phi$. Si le polynôme $K(X) = \sum(-1)^{n-i}\sigma_{n-i}X^i$ a pour racines les abscisses des éléments de $\operatorname{Ker}\phi$, les relations de Vélu (2) fournissent le coefficient σ_2 ainsi qu'une relation linéaire entre σ_1 et σ_3.

Comment continuer et calculer les coefficients suivants du polynôme ? Comme ϕ est normalisée, on peut écrire

$$\phi(x,y) = \left(\phi_x(x), y\phi'_x(x)\right), \quad \phi_x(x) = \frac{N(x)}{D(x)}$$

où N et D sont des polynômes de degrés ℓ et $\ell - 1$, et $D = K^2$. L'équation de E' donne donc une équation différentielle (notons l'analogie avec les idées de Stark) :

$$y^2\phi'^2_x(x) = \phi_x(x)^3 + a'\phi_x(x) + b' \tag{3}$$

où l'on remplace y^2 par $x^3 + ax + b$ et que l'on différencie pour obtenir une équation du second ordre :

$$(3x^2 + a)\phi'_x + 2(x^3 + ax + b)\phi''_x = 3\phi_x^2 + a'. \tag{4}$$

On développe ensuite ϕ_x en série de x^{-1} :

$$\phi_x(x) = x + \sum_{i\geq 1} \frac{h_i}{x^i}.$$

L'équation différentielle (4) donne une relation de récurrence liant les coefficients h_i, qui s'initialise grâce aux relations tirées de (2)

$$h_1 = \frac{a - a'}{5}, \quad h_2 = \frac{b - b'}{7}.$$

On peut retrouver les coefficients de K à partir de ceux de ϕ_x, puisque l'on peut réarranger (1) en

$$\phi_x(x) = \ell x - \sigma_1 - (3x^2 + a)\frac{K'(x)}{K(x)} - 2(x^3 + ax + b)\left(\frac{K'(x)}{K(x)}\right)'. \tag{5}$$

On obtient une relation de récurrence qui permet de déterminer les coefficients de K. Cependant, pour l'utiliser, il faut connaître la quantité σ_1 (la somme des racines de K). On peut parfois la déterminer par d'autres méthodes, mais on ne dispose pas toujours de ce renseignement.

L'algorithme d'Elkies est *quadratique* en ℓ en termes d'opérations dans le corps de base. Tel qu'exposé ci-dessus, il s'applique aux isogénies normalisées pour lesquelles on dispose d'un renseignement supplémentaire, et n'est donc pas utilisable directement en général.

Bostan, Morain, Salvy et Schost [1] reprennent cette méthode en 2008 en proposant deux améliorations. La première est l'utilisation d'une *itération de Newton* afin de résoudre l'équation (3) dans les séries formelles ; on passe ainsi d'un algorithme quadratique en ℓ à une complexité *quasi-optimale*, linéaire en ℓ à facteurs logarithmiques près. Atteindre cette complexité nécessite de plus d'utiliser des algorithmes rapides pour la manipulation des polynômes et séries formelles, que l'on peut trouver par exemple dans le livre de von zur Gathen et Gerhardt [8].

La seconde idée est de récupérer le polynôme $K(x)$ non pas à partir de la relation (5), mais directement à partir de la série formelle $\phi_x = \frac{N(x)}{K(x)^2}$ à l'aide d'un algorithme dit de *reconstruction rationnelle*. Cela nécessite de calculer un peu plus de coefficients de ϕ_x, mais connaître la somme des racines de K n'est plus nécessaire. En revanche, on demande toujours une isogénie normalisée.

Remarquons que résoudre les différentes relations de récurrences (ou l'application de la méthode de Newton) nécessite de diviser par beaucoup de petits entiers dans le corps de base. Cet algorithme n'est donc pas utilisable en petite caractéristique. De plus, on ne sait pas « normaliser » une isogénie en temps quasi-linéaire : proposer un algorithme quasi-linéaire dans tous les cas reste une question ouverte.

2.5. L'algorithme de Couveignes. L'algorithme de Couveignes permet de donner une solution au problème de calcul d'isogénie en petite caractéristique. Soit p un nombre premier, $q = p^r$ et $E/\mathbb{F}_q$ une courbe elliptique. L'endomorphisme $[p]$ de E n'est pas séparable : dans la plupart des cas, E est une courbe dite *ordinaire*, et l'on a pour tout $j \geq 1$

$$E[p^j](\bar{k}) \simeq \mathbb{Z}/p^j\mathbb{Z}.$$

L'inséparabilité se voit bien : « il n'y a pas assez de points » dans ce noyau par rapport au degré.

Lorsque $\phi : E \to E'$ est une isogénie de degré ℓ premier à p, elle définit une bijection

$$E[p^j](\bar{k}) \xrightarrow{\sim} E'[p^j](\bar{k}).$$

Pour simplifier, fixons $j \geq 1$ et supposons que les points de p^j-torsion de E sont définis sur $\mathbb{F}_q$. C'est alors vrai sur E' également, puisque ce sont les images par ϕ des points de E. Choisissons deux points P, P' qui engendrent respectivement les groupes cycliques $E[p^j](\bar{k})$, $E'[p^j](\bar{k})$. Il existe alors un unique $a \in (\mathbb{Z}/p^j\mathbb{Z})^\times$ tel que $\phi(P) = [a]P'$. Comme ϕ est un morphisme de

groupes, elle envoie également le point $[m]P$ sur $[am]P'$ pour tout entier m. Couveignes propose donc de choisir un coefficient a et de tenter d'*interpoler* l'isogénie entre ces points ; si cela échoue, on prend un autre coefficient a jusqu'à trouver le bon !

Afin d'interpoler une fraction rationnelle de degré ℓ, il faut disposer de suffisamment de points : il faut choisir l'entier j tel que $p^j > 4\ell$. Pour trouver un générateur de $E[p^j](\mathbb{F}_q)$, on calcule un polynôme de division T_j définissant $E[p^j]$ et on en cherche une racine dans $\mathbb{F}_q$, à l'aide de l'algorithme de Cantor–Zassenhaus [8].

Bien sûr, en général les points de $E[p^j]$ ne sont pas $\mathbb{F}_q$-rationnels, et il faut manipuler des extensions du corps $\mathbb{F}_q$. Si T_j se scinde sur $\mathbb{F}_q$ en f facteurs irréductibles de degré d

$$T_j = \prod_{k=1}^{f} U_{k,j} \ ,$$

il est intéressant de travailler avec les d extensions $\mathbb{F}_q[X]/U_{k,j}$ munies d'isomorphismes compatibles, plutôt que dans le gros anneau $\mathbb{F}_q[X]/T_j$. On peut aussi calculer intelligemment des isomorphismes avec les analogues de ces corps que l'on obtient avec la courbe E' [4]. Afin d'obtenir une meilleure complexité, il faut également utiliser des méthodes rapides pour la manipulation de polynômes [8] [2]. Lorsque $\ell \gg p$, on obtient un algorithme de coût essentiellement quadratique en ℓ en termes de $\mathbb{F}_q$-opérations.

En revanche, le coût est exponentiel en $\log p$, puisqu'il faut manipuler des polynômes de degré au moins $p-1$. Pour cette raison, l'algorithme de Couveignes n'est pas adapté lorsque $\log p$ n'est pas très petit. Pour traiter le cas de la caractéristique « intermédiaire » (lorsqu'un algorithme de grande caractéristique comme la méthode d'Elkies n'est pas applicable du fait de divisions par zéro sans que p soit petit), on peut étendre l'algorithme de Couveignes en interpolant sur la n^k-torsion pour un premier n distinct de ℓ et p : voir par exemple De Feo, Hugounenq, Plût et Schost [7].

3 Application au comptage de points

Soit p un grand nombre premier et $E/\mathbb{F}_p$ une courbe elliptique. On souhaite calculer le cardinal du groupe $E(\mathbb{F}_p)$. Cette question est naturelle dans de nombreux contextes : par exemple, dans l'optique d'utiliser la courbe E dans un protocole cryptographique, il est souvent important que le cardinal de $E(\mathbb{F}_p)$ ait un grand facteur premier. Nous allons voir comment utiliser des isogénies permet d'accélérer ce calcul.

2. On utilise aussi des méthodes spécifiques pour d'autres étapes du calcul, comme l'interpolation : on renvoie pour cela à [6, 7].

Pour compter les points d'une courbe elliptique en grande caractéristique en temps polynomial, on utilise l'algorithme de Schoof [14]. On peut montrer

$$\text{Card}\, E(\mathbb{F}_p) = p + 1 - t,$$

où t est un nombre entier vérifiant $|t| \leq 2\sqrt{p}$ et tel que le Frobenius π_E vérifie

$$\pi_E^2 - t\pi_E + p = 0.$$

Comment alors déterminer t ? Si $P = (x, y)$ est un point de E, on doit avoir

$$(x^{p^2}, y^{p^2}) - [t](x^p, y^p) + [p](x, y) = 0_E \tag{6}$$

On peut donc choisir un point générique P, et tester cette égalité pour toutes les valeurs permises de t. Vu les bornes de Hasse, cela donne un algorithme exponentiel en $\log(p)$.

Cependant, si P est un point de ℓ-torsion pour un premier ℓ, alors l'égalité (6) restera vraie en remplaçant t par le reste de t modulo ℓ. On peut ainsi proposer un algorithme *multimodulaire* : on choisit des premiers ℓ_i tels que $\prod \ell_i > 4\sqrt{p}$ (ce qui peut se faire avec $\ell_i = O(\log p)$), puis on calcule t modulo chaque ℓ_i en testant l'égalité (6) comme ci-dessus. On récupère alors t *via* les restes chinois. On obtient un algorithme polynomial en $\log(p)$, mais de degré élevé puisque le polynôme de ℓ-division est de degré $\ell^2 - 1$.

Utiliser des isogénies permet de réduire ce degré : c'est une amélioration proposée par Elkies à l'algorithme de Schoof. Plus précisément, on peut montrer que le polynôme $X^2 - tX + p$ est le polynôme caractéristique de π_E vu comme endomorphisme du $(\mathbb{Z}/\ell\mathbb{Z})$-espace vectoriel $E[\ell](\overline{\mathbb{F}_p})$ de dimension 2. Lorsque ce polynôme est scindé modulo ℓ (ce qui survient une fois sur 2 environ), il existe des sous-espaces propres pour le Frobenius : ce sont des sous-groupes rationnels de cardinal ℓ, donc il existe une isogénie rationnelle de degré ℓ au départ de E. On dit alors que ℓ est un nombre premier *d'Elkies*, et on procède comme suit :

- On détermine une courbe liée à E par une ℓ-isogénie (à l'aide d'une équation modulaire, ce dont on ne parlera pas ici) ;
- On détermine son noyau à l'aide de l'algorithme d'Elkies (il faut d'abord *normaliser* l'isogénie, ce dont on ne parlera pas non plus) ; on connaît alors une droite stable par le Frobenius de $E[\ell]$;
- On détermine la *valeur propre* v_ℓ de π_E sur cette droite ;
- On récupère $t = v_\ell + \frac{p}{v_\ell} \mod \ell$, vu le polynôme caractéristique.

Ainsi, on ne manipule plus le polynôme de ℓ-division de degré $\ell^2 - 1$, mais seulement un polynôme définissant un sous-groupe de cardinal ℓ, de

degré $\frac{\ell-1}{2}$. Il s'agit d'une amélioration importante en pratique. Cependant, on ne sait pas montrer en général qu'il existe suffisamment de nombres premiers d'Elkies pour pouvoir diminuer la complexité *théorique* de l'algorithme de Schoof. D'autres améliorations ont été proposées par Atkin dans le cas des autres premiers, d'où l'algorithme SEA fréquemment utilisé pour cet algorithme, implanté entre autres dans PARI [18] et Magma.

Références

[1] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of computation*, 77(263) :1755–1778, 2008.

[2] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. PhD thesis, 1994.

[3] J.-M. Couveignes. Computing ℓ-isogenies with the p-torsion. *Algorithmic Number Theory, ANTS II, L.N.C.S.*, 1122 :59–65, 1996.

[4] J.-M. Couveignes. Isomorphisms between Artin–Schreier towers. *Math. Comp.*, 69(232) :1625 – 1631, 2000.

[5] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues, 1997. Preprint.

[6] L. De Feo. *Fast algorithms for towers of finite fields and isogenies*. PhD thesis, École Polytechnique, 2010.

[7] L. De Feo, C. Hugounenq, J. Plût, and É. Schost. Explicit isogenies in quadratic time in any characteristic. *LMS J. Comp. Math.*, 19(A) :267–282, 2016.

[8] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[9] P. Lairez and T. Vaccon. On p-adic differential equations with separation of variables. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 319–323, 2016.

[10] R. Lercier. Computing isogenies in $\mathbb{F}_{2^n}$. *Algorithmic Number Theory, ANTS II, L.N.C.S.*, 1122 :197–212, 1996.

[11] R. Lercier and T. Sirvent. On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field. *Journal de théorie des nombres de Bordeaux*, 20(3) :783–797, 2008.

[12] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *Journal de théorie des nombres de Bordeaux*, 7(1) :255–282, 1995.

[13] J. Nekovár. Algebraic theory of elliptic curves, 2004. Cours de DEA/M2.

[14] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1) :219–254, 1995.

[15] J. H. Silverman. *The arithmetic of elliptic curves*. Springer, 1986.

[16] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 1994.

[17] H. M. Stark. Class number of complex quadratic fields. In W. Kuyk, editor, *Modular fonctions of one variable I*, pages 153–174. Antwerp, 1972.

[18] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.9.0`, 2017. available from `http://pari.math.u-bordeaux.fr/`.

[19] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-rendus de l'Académie des Sciences, Série I*, 273 :238–241, 1971.