Anneau d'endomorphismes et cardinalité des courbes elliptiques : aspects algorithmiques

Mireille Fouquet

17 décembre 2001

Table des matières

Introduction

La cryptologie moderne commence à acquérir ses lettres de noblesse. Après 20 ans de recherche académique sur le sujet, des applications dans le monde réel commencent à fleurir ici et là. En particulier, INTERNET est un terrain de choix pour le développement de la crytographie à clé publique. Les nouveaux types de cryptosystèmes s'appuient sur des problèmes mathématiques qui théoriquement ont une solution mais ne sont pas résolubles en pratique (i.e. en temps polynomial par exemple). Le premier de ces systèmes a été proposé en novembre 1976 par W. Diffie et M.E. Hellman [DH76]. Le problème sur lequel il repose est le suivant : soit G un groupe cyclique d'ordre n de générateur g noté multiplicativement et soit x un entier, il est facile de calculer g^x ; par contre, renverser cette opération i.e. "étant donnés g et g^x calculer x" est difficile en général. C'est le problème du logarithme discret. Un autre de ces problèmes mathématiques est la factorisation d'entiers qui est mise à profit en particulier dans le cryptosystème RSA proposé par L.M. Adleman, R.L. Rivest et A. Shamir [ARS78]. La théorie algorithmique des nombres a ainsi trouvé une place de choix en cryptologie.

Afin de développer des cryptosystèmes utilisant le problème du logarithme discret, il a fallu rechercher des groupes pour lesquel résoudre ce problème est difficile. Les meilleures attaques connues ne reposant sur aucune propriété particulière de structure du groupe sont les attaques proposées par D. Shanks [Sha71] et par J.M. Pollard [Pol78]. Ces algorithmes permettent de calculer le logarithme discret en $O(\sqrt{n})$ opérations où n est la taille du groupe considéré. Les premiers groupes proposés furent les groupes multiplicatifs de corps finis, mais il existe une attaque sous-exponentielle dans ces groupes. Les courbes elliptiques et les jacobiennes des courbes hyperelliptiques définies sur des corps finis ont ensuite été proposées [Mil87, Kob87, Kob89]. Cependant dans le cas des courbes hyperelliptiques, des algorithmes sous-exponentiels effectifs sur des courbes de genre supérieur ou égal à 4 ont été développés [ADH94, MST99, Eng99a, Gau00a, EG00]. L'avantage majeur de l'utilisation des courbes elliptiques réside donc dans le fait que, pour le moment, on ne connaît aucun algorithme sous-exponentiel qui permette de résoudre le problème du logarithme discret sur l'ensemble des courbes elliptiques.

Malgré cela, il faut tout de même se montrer prudent dans le choix des courbes elliptiques utilisées. Tout d'abord elles ne doivent pas faire partie d'une classe de courbes pour laquelle on connaît une attaque spécifique : par exemple, les courbes supersingulières déconseillées à cause de la réduction MOV [MOV91, FR94, Vol97], les courbes de trace 1 [SA98, Sma99]. En dehors de ces cas particuliers, il faut s'assurer que la cardinalité du groupe n'est pas friable pour résister à la réduction de Pohlig et Hellman [PH78]. Il est donc nécessaire de calculer le nombre de points d'une courbe. Le premier algorithme de calcul de cardinalité en temps polynomial a été proposé par R. Schoof en 1985 [Sch85]. L'idée de cet algorithme est de regarder l'action du Frobenius dans les sous-groupes de ℓ-torsion de la courbe où ℓ est un nombre premier, ce qui permet d'obtenir la cardinalité de la courbe modulo ℓ. Il suffit alors de réaliser cette même opération pour un ensemble de nombres premiers suffisamment grand défini grâce à une borne sur la cardinalité pour retrouver le nombre de points de la courbe à l'aide du théorème chinois. Le problème de cette méthode est qu'elle est limitée par la croissance rapide du degré des polynômes définissant les sous-groupes de ℓ-torsion. Les idées d'A.O.L. Atkin et N.D. Elkies permettent de calculer un petit facteur de ces polynômes en calculant des isogénies particulières et donc de réduire la complexité de l'algorithme. C'est la naissance de l'algorithme SEA. J.-M. Couveignes et R. Lercier [Cou94, Cou96, Ler97b] ont rendus possibles les calculs d'isogénies en petite caractéristique. Tous ces résultats ont énormément fait évoluer le calcul de la cardinalité d'une courbe : l'algorithme original de Schoof est limité à des courbes définies sur des corps à 10^{50} éléments alors que l'utilisation de l'algorithme SEA et des améliorations sur le calcul des isogénies a permis de calculer la cardinalité d'une courbe définie sur un corps à $10^{499}+153$ éléments [Mor95] et sur un corps à 2^{1999} éléments [Ver99].

Ce mémoire s'inscrit dans la continuation de ces travaux. Après avoir étudié la cardinalité de la courbe, il parait naturel de s'intéresser à son anneau d'endomorphismes. La théorie concernant cet invariant de la courbe est connue depuis de nombreuses années grâce aux travaux de Deuring [Deu41] et de Waterhouse [Wat69] (voir aussi [Sch87]), mais ce n'est que récemment que des algorithmes pour le calculer ont été développés par D. Kohel [Koh96]. L'étude de ces derniers dans le cas des courbes elliptiques ordinaires nous a amené à considérer une structure de courbes isogènes qui nous permet de déterminer l'anneau d'endomorphismes de chacune des courbes mais aussi de connaitre la relation entre deux courbes isogènes et leurs anneaux d'endomorphismes. Cette construction a aussi permis d'apporter des réponses à des problèmes de l'algorithme SEA rencontrés pour des valeurs particulières d'entiers ℓ premiers. Ces travaux ont été réalisés en collaboration avec F. Morain [FM00].

En 1999, Satoh [Sat00] a proposé un nouvel algorithme de calcul de cardinalité d'une courbe définie sur un corps de caractéristique différente de 2 et 3. L'idée principale de cette méthode est de relever canoniquement la courbe dans un anneau local dont le corps résiduel est le corps de définition de la courbe. L'algorithme de relèvement utilise un théorème de Lubin, Serre et Tate [LST64]. Avec P. Gaudry et R. Harley [FGH00], nous avons étendu cet algorithme au cas des caractéristiques 2 et 3. Nous avons ainsi pu déterminer la cardinalité d'une courbe définie sur un corps à 2^{8007} éléments en 13 jours. Nous nous sommes alors servi de cette nouvelle méthode dans le cas de la petite caractéristique afin de dériver un algorithme performant pour fabriquer des courbes elliptiques à usage cryptographique [FGH01].

Organisation de ce manuscrit. Ce mémoire se décompose en trois parties. La première consiste en un ensemble de rappels théoriques concernant les courbes elliptiques en général, la deuxième est consacrée à la construction d'une structure que nous appellons un volcan d'isogénies et à ses applications et enfin la dernière partie développe les algorithmes les plus récents de calcul de cardinalité d'une courbe elliptique ordinaire définie sur un corps fini.

Nous commençons tout d'abord par introduire un ensemble de résultats sur les ordres d'un corps quadratique imaginaire. Nous nous attardons tout particulièrement sur le groupe de classes d'idéaux d'un ordre. Cette étude nous permet dans la suite du mémoire d'étudier l'ensemble de courbes elliptiques ordinaires qui ont même anneau d'endomorphismes. Dans ce chapitre nous voyons apparaître des réseaux sur $\mathbb{C}$. Le chapitre 2 sera consacré à ces réseaux, ce qui revient à étudier la théorie analytique des courbes elliptiques. Nous définissons la fonction de Weierstrass d'un réseau et son j-invariant. Nous introduisons aussi les fonctions modulaires et tout particulièrement le polynôme modulaire, objet mathématique qui nous sera d'une grande utilité par la suite. Ces études nous amènent à considérer la théorie de la multiplication complexe. Le dernier chapitre de cette partie est un ensemble de rappels sur les courbes elliptiques définies sur un corps $\mathbb{K}$ quelconque. Cette fois-ci nous utilisons le point de vue algébrique de la théorie. Il est aisé cependant de faire le rapprochement entre les fonctions elliptiques introduites au chapitre précédent avec les courbes elliptiques. Nous verrons ainsi que de cet objet nous tirons un groupe abélien ainsi qu'un ensemble de morphismes (les isogénies). Pour clôturer ce chapitre nous nous intéressons plus particulièrement aux courbes elliptiques définies sur un corps fini, objets qui nous intéressent en cryptologie.

La deuxième partie traite de l'algorithmique des courbes elliptiques sur un corps fini. Pour débuter, nous introduisons différentes méthodes de calcul d'une isogénie ainsi que les algorithmes déterminant la cardinalité d'une courbe elliptique. Le chapitre 5 expose les résultats de Kohel concernant le calcul de l'anneau d'endomorphismes d'une courbe elliptique ordinaire. L'ensemble de ces méthodes exploitent les liens entre deux courbes isogènes et leurs anneaux d'endomorphismes. Le développement de ces relations donne lieu dans le chapitre 6 à la création d'une structure, appelée volcan d'isogénie, décrivant la classe d'isogénies d'une courbe. Nous donnons un algorithme qui permet de construire cette structure ou plus exactement la charpente de celle-ci ce qui est suffisant pour nos applications. Malgré tout, il est aisé de construire la structure dans son intégralité à partir des algorithmes donnés. Le chapitre 7 montre les différentes applications de cette structure. En particulier, nous montrons comment un volcan d'isogénies nous permet d'obtenir un résultat plus complet sur la cardinalité modulo un ensemble de nombres premiers ℓ particuliers.

La dernière partie développe les récentes avancées dans le domaine de calcul de la cardinalité d'une courbe elliptique. Cette approche est totalement différente de l'approche classique introduite dans la partie précédente. Il va s'agir cette fois-ci de relever la courbe dans un anneau local qui admet pour corps résiduel le corps $\mathbb{F}_q$ sur lequel est définie notre courbe. Une fois la courbe relevée, nous calculons la trace de l'endomorphisme de Frobenius dans cet anneau. Afin de pouvoir comprendre ces algorithmes, nous introduisons dans le chapitre 8 la théorie liée à ces anneaux locaux et nous ferons aussi des considérations d'ordre calculatoire, i.e. quel objet choisir afin de simplifier les calculs. Le chapitre 9 est lui la retranscription du travail réalisé en collaboration avec P. Gaudry et R. Harley qui expose les résultats de T. Satoh et développe l'algorithme en caractéristique 2 et 3. À partir de cette implantation nous avons pu établir un nouveau record en calcul de cardinalité d'une courbe elliptique. Dans le chapitre 10, nous indiquons les différentes avancées réalisées depuis la publication de nos résultats. Cependant le sujet étant en pleine évolution ce chapitre ne se veut pas exhaustif et expose ce dont nous sommes au courant à ce jour. Enfin le dernier chapitre de ce manuscrit est consacré à la construction de "bonnes" courbes elliptiques cryptographiquement parlant. Pour cela, nous nous inspirons des travaux de R. Lercier et les appliquons à la nouvelle méthode de calcul de cardinalité.

Première partie

Rappels théoriques

Chapitre 1

Théorie des ordres sur les corps quadratiques

Dans ce chapitre, nous allons faire quelques rappels sur la théorie des ordres. Pour en savoir plus, les livres de Borevitch et Chafarevitch [BC67] ou encore Cox [Cox89] approfondissent plus amplement le sujet.

1.1 Introduction sur les ordres d'un corps quadratique

Soit un corps quadratique K. On peut l'écrire de manière unique comme étant de la forme $K = \mathbb{Q}(\sqrt{N})$, où N est un entier sans carré, ce que l'on supposera toujours par la suite. À ce corps K on peut associer différents invariants.

Définition 1.1.1 *On définit le discriminant d_K de $K = \mathbb{Q}(\sqrt{N})$ comme étant l'entier suivant :*

$$d_K = \begin{cases} N & \text{si } N \equiv 1 \mod 4 \\ 4N & \text{sinon.} \end{cases}$$

Définition 1.1.2 *L'anneau des entiers $\mathcal{O}_K$ de K est l'ensemble des entiers algébriques de K, i.e., l'ensemble des $\alpha \in K$ qui sont racines d'un polynôme unitaire à coefficients entiers relatifs.*

Dans K, on peut décrire l'anneau des entiers $\mathcal{O}_K$ comme étant :

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{si } N \not\equiv 1 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{si } N \equiv 1 \mod 4 \end{cases} \tag{1.1}$$

$$\text{ou bien encore } \mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]. \tag{1.2}$$

Définition 1.1.3 *Un ordre $\mathcal{O}$ dans un corps quadratique K est un sous-ensemble de K tel que :*

1. *$\mathcal{O}$ est un sous-anneau de K ;*
2. *$\mathcal{O}$ est un $\mathbb{Z}$-module libre de rang 2.*

L'anneau des entiers $\mathcal{O}_K$ de K est donc clairement un ordre. De plus, si $\alpha \in \mathcal{O}$ où $\mathcal{O}$ est un ordre de K, alors α est un entier algébrique de K et donc $\alpha \in \mathcal{O}_K$. Ainsi pour tout ordre $\mathcal{O}$, on a $\mathcal{O} \subseteq \mathcal{O}_K$, donc $\mathcal{O}_K$ est l'ordre maximal de K. D'après (1.2), on peut écrire $\mathcal{O}_K$ sous la forme

$$\mathcal{O}_K = [1, \omega_K] \text{ où } \omega_K = \frac{d_K + \sqrt{d_K}}{2} \tag{1.3}$$

où $[\alpha, \beta]$ désigne une base de $\mathbb{Z}$-module.

Lemme 1.1.1 *Soit $\mathcal{O}$ un ordre dans un corps quadratique K de discriminant d_K. Alors $\mathcal{O}$ a un indice fini dans $\mathcal{O}_K$, et si l'on note $f = [\mathcal{O}_K : \mathcal{O}]$, alors*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K],$$

où ω_K est comme dans (1.3).

Démonstration: Cox[Cox89, Lemme 7.7.2]. □

Définition 1.1.4 *Soit $\mathcal{O}$ un ordre de K, l'indice $f = [\mathcal{O}_K : \mathcal{O}]$ est appelé le* conducteur *de $\mathcal{O}$.*

Réciproquement, pour tout entier naturel f, le module $[1, f\omega_K]$ est un ordre de K. Il existe donc une bijection entre les ordres d'un corps quadratique et les entiers naturels. De plus, si on considère l'ordre partiel sur $\mathbb{N}$ tel que $m \preceq n$ si $m|n$, alors il induit un ordre partiel sur l'ensemble des ordres sur K : $m \preceq n$ si et seulement si $[1, n\omega] \subseteq [1, m\omega]$. On peut aussi définir un autre invariant d'un ordre, son discriminant.

Définition 1.1.5 *Soit $\alpha \mapsto \alpha'$ l'automorphisme non trivial d'un corps quadratique imaginaire K. Soit $\mathcal{O}$ un ordre de K, on supposera que $\mathcal{O} = [\alpha, \beta]$. Alors le discriminant de $\mathcal{O}$ est le nombre*

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2.$$

Le discriminant étant indépendant de la base de $\mathcal{O}$ utilisée pour le calculer, si l'on se sert de la base $\mathcal{O} = [1, f\omega_K]$, on trouve

$$D = f^2 d_K.$$

1.2 Idéaux d'un ordre

Nous allons tout d'abord donner des notions générales sur les idéaux d'un ordre avant de nous intéresser tout particulièrement aux idéaux fractionnaires.

1.2.1 Définitions et propiétés

Lemme 1.2.1 *Soit $\mathcal{O}$ un ordre de K et $\mathfrak{a}$ un idéal non nul de $\mathcal{O}$, alors l'anneau quotient $\mathcal{O}/\mathfrak{a}$ est fini.*

À partir de ce lemme, on définit la norme d'un idéal $\mathfrak{a}$ comme étant $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.

Définition 1.2.1 *Un idéal $\mathfrak{p}$ d'un ordre $\mathcal{O}$ est un idéal premier si $\mathfrak{p} \neq \mathcal{O}$ et si l'anneau quotient $\mathcal{O}/\mathfrak{p}$ est intègre.*

La proposition suivante nous donne le lien entre les idéaux premiers de norme ℓ et le corps quadratique imaginaire K.

Proposition 1.2.1 *Soit K un corps quadratique imaginaire de discriminant d_K, et soit l'automorphisme non-trivial de K noté par $\alpha \mapsto \bar{\alpha}$. Soit $\ell \in \mathbb{Z}$ un nombre premier.*

(i). Si $\left(\frac{d_K}{\ell}\right) = 0$, alors $\ell\mathcal{O}_K = \mathfrak{l}^2$ où $\mathfrak{l}$ est un idéal premier de $\mathcal{O}_K$.

(ii). Si $\left(\frac{d_K}{\ell}\right) = 1$, alors $\ell\mathcal{O}_K = \mathfrak{l}\bar{\mathfrak{l}}$ où $\mathfrak{l} \neq \bar{\mathfrak{l}}$ sont des idéaux premiers de $\mathcal{O}_K$.

(iii). Si $\left(\frac{d_K}{\ell}\right) = -1$, alors $\ell\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$.

Démonstration: Cox [Cox89, Prop. 5.16] □

Définition 1.2.2 *On dit qu'un idéal $\mathfrak{a}$ de $\mathcal{O}$ est propre si et seulement si*

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Par exemple, les idéaux principaux sont toujours propres et tous les idéaux de l'ordre maximal sont propres.

1.2.2 Idéaux fractionnaires

Définition 1.2.3 *Un idéal fractionnaire de $\mathcal{O}$ est un sous-ensemble de K qui est un $\mathcal{O}$-module non nul finiment engendré.*

On peut prouver qu'un idéal fractionnaire de $\mathcal{O}$ est de la forme $\alpha\mathfrak{a}$, où $\alpha \in K^*$ et $\mathfrak{a}$ est un idéal de $\mathcal{O}$. De plus, un idéal fractionnaire principal de $\mathcal{O}$ est de la forme $\alpha\mathcal{O}$, où $\alpha \in K^*$. Un idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}$ est *inversible* s'il existe un idéal fractionnaire de $\mathfrak{b}$ $\mathcal{O}$ tel que $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. On peut aussi prouver qu'un idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}$ s'écrit sous la forme $[\alpha, \beta]$ où $\alpha, \beta \in K$.

Proposition 1.2.2 *Soit $\mathcal{O}$ un ordre de K, et soit $\mathfrak{a}$ un $\mathcal{O}$-idéal fractionnaire. Alors $\mathfrak{a}$ est propre si et seulement si $\mathfrak{a}$ est inversible.*

Démonstration: Cox [Cox89, Proposition 7.4]. □

On peut voir aussi les idéaux fractionnaires de $\mathcal{O}$ comme étant des $\mathbb{Z}$-modules libres de rang 2, donc si $\mathfrak{a}$ est un idéal fractionnaire, on peut l'écrire sous la forme $\mathfrak{a} = [\alpha, \beta]$, où α et β sont linéairement indépendants par rapport à $\mathbb{R}$.

1.3 Groupe de classes d'idéaux d'un ordre

Soit un ordre $\mathcal{O}$ de K. On notera $I(\mathcal{O})$ l'ensemble des idéaux fractionnaires propres de $\mathcal{O}$. La proposition (1.2.2) nous montre que $I(\mathcal{O})$ est un groupe avec une loi multiplicative. On notera aussi $P(\mathcal{O})$ le sous-groupe de $I(\mathcal{O})$ composé des idéaux fractionnaires principaux de $\mathcal{O}$.

Définition 1.3.1 *On appelle le groupe de classes d'idéaux de $\mathcal{O}$ le quotient $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$.*

Le groupe de classes d'idéaux a de nombreuses propriétés. En particulier, on peut trouver un isomorphisme avec les classes d'homothéties de réseaux et avec le groupe des classes de formes quadratiques. De plus, il est possible de dénombrer ses éléments.

1.3.1 Idéaux fractionnaires et formes quadratiques

Avant de montrer l'isomorphisme entre les idéaux fractionnaires et les formes quadratiques, on va rappeler quelques définitions sur les formes quadratiques.

Définition 1.3.2 *Une forme quadratique binaire f est une fonction $f(x,y) = ax^2 + bxy + cy^2$ où a, b et c sont des entiers. On dit que f est primitive si a, b et c sont premiers entre eux. Si f et g sont deux formes quadratiques, on dit que f et g sont équivalentes s'il existe une matrice $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ telle que $g(x,y) = f(\alpha x + \beta y, \gamma x + \delta y)$.*

À partir de ce point, nous ne considérerons que le cas du discriminant négatif. On notera, en général, une forme quadratique binaire $f(x,y) = ax^2 + bxy + cy^2$ par un triplet (a, b, c). On dira qu'une forme quadratique (a, b, c) est *positive* si $a > 0$. On définit aussi les formes réduites.

Définition 1.3.3 *Une forme quadratique positive (a, b, c) de discriminant $D < 0$ est dite réduite si $|b| \leqslant a \leqslant c$ et si, en plus, quand l'une des deux inégalités est une égalité (i.e. soit $|b| = a$ soit $a = c$), alors $b \geqslant 0$.*

On peut maintenant introduire la notion de groupe de classes de formes.

Définition 1.3.4 *Le groupe de classes de formes $C(D)$ est l'ensemble des classes d'équivalence des formes quadratiques primitives positives de discriminant D modulo $\mathrm{SL}(2, \mathbb{Z})$.*

On note $h(D)$ la cardinalité de ce groupe. Les formes réduites nous permettent de décrire le groupe de classes de formes.

Proposition 1.3.1 *Dans toute classe de formes quadratiques définies positives de discriminant $D < 0$ il existe exactement une forme réduite. En particulier $h(D)$ est égal au nombre de formes primitives réduites de discriminant D.*

Ce groupe de classes de formes est en bijection avec le groupe de classes d'idéaux. On peut, de plus, donner explicitement l'application qui, à une forme quadratique, fait correspondre un idéal fractionnaire.

Théorème 1.3.1 *Soit $\mathcal{O}$ un ordre de discriminant D dans un corps quadratique imaginaire K.*

1. *Si $f(x, y) = ax^2 + bxy + cy^2$ est une forme quadratique primitive positive de discriminant D, alors $[a, (-b + \sqrt{D})/2]$ est un idéal propre de $\mathcal{O}$.*
2. *L'application qui envoie $f(x, y)$ en $[a, (-b+\sqrt{D})/2]$ induit un isomorphisme entre le groupe de classes de formes $C(D)$ et le groupe de classes d'idéaux $C(\mathcal{O})$. Par suite, l'ordre de $C(\mathcal{O})$ est le nombre de classes $h(D)$.*

Démonstration: Cox [Cox89, Théorème 7.7] ou Cohen [Coh96a, Théorème 5.2.8]. □

1.3.2 Nombre de classes

Soit $\mathcal{O}$ un ordre de conducteur f. On cherche à calculer son nombre de classes, i.e. la cardinalité de $C(\mathcal{O})$. Cette cardinalité dépend du conducteur et du nombre de classes de l'anneau des entiers. En effet, le théorème suivant nous donne la formule pour trouver le nombre de classe $h(\mathcal{O})$ en fonction de f et de $h(\mathcal{O}_K)$. Il faut avant de l'énoncer faire un petit rappel sur les notations. Soit p un nombre premier, alors :

$$\left(\frac{d_K}{p}\right) = \begin{cases} \text{si } p \text{ est impair} & \text{symbole de Legendre} \\ \text{si } p = 2 & \begin{cases} 0 & \text{si } 2|d_K \\ 1 & \text{si } d_K \equiv 1 \mod 8 \\ -1 & \text{si } d_K \equiv 5 \mod 8. \end{cases} \end{cases}$$

Théorème 1.3.2 *Soit $\mathcal{O}$ un ordre de conducteur f dans un corps quadratique imaginaire K. Alors :*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

De plus, $h(\mathcal{O})$ est toujours un multiple de $h(\mathcal{O}_K)$.

Démonstration: Cox [Cox89, Théorème 7.24]. □

Mais on ne peut se servir de cette formule que si l'on connaît le nombre de classes de l'anneau des entiers. Pour ce faire, nous donnons l'algorithme sous-exponentiel de McCurley [McC89].

On donne ici les idées principales de l'algorithme[1]. Cet algorithme se base sur la recherche de multiples du nombre de classes.

Soit un ordre $\mathcal{O}$ de discriminant D dans un corps quadratique K. On va calculer son nombre de classes. Soit $\mathcal{P}$ un ensemble fini de nombres premiers p tel que $\left(\frac{D}{p}\right) = 1$ pour tout $p \in \mathcal{P}$. Pour chaque p, en utilisant la méthode de Shanks [Coh96a, Algorithme 5.4.10], on trouve une forme réduite telle que $f_p = (p, b_p, c_p)$ où b_p est tel que $b_p^2 \equiv D \mod 4p$ et $c_p = (b_p^2 - D)/(4p)$. Ces formes seront appellées formes premières. En admettant l'hypothèse généralisée de Riemann, on peut prouver qu'il existe une constante c, que l'on peut effectivement calculer, telle que si $\mathcal{P}$ contient tous les nombres premiers tels que $\left(\frac{D}{p}\right) = 1$ et $p \leqslant c^2 \ln^2 |D|$, alors les classes de formes f_p pour $p \in \mathcal{P}$ engendrent le groupe de classes. C'est-à-dire que si l'on pose $n = |\mathcal{P}|$, l'application

$$\begin{aligned} \phi : \mathbb{Z}^n &\to C(D) \\ (x_p)_{p \in \mathcal{P}} &\mapsto \prod_{p \in \mathcal{P}} f_p^{x_p} \end{aligned}$$

est un homomorphisme de groupe surjectif. Par conséquent, le noyau Λ de ϕ est un sous-réseau de $\mathbb{Z}^n$, et on a

$$\mathbb{Z}^n / \Lambda \cong C(D) \text{ et } |\det(\Lambda)| = h(D),$$

où on note par $\det(\Lambda)$ le déterminant d'une quelconque $\mathbb{Z}$-base de Λ. Le réseau Λ est le réseau des relations sur les formes f_p. Si l'on trouve un système à n éléments indépendants dans ce réseau, alors le déterminant de ce système sera un multiple du déterminant de Λ, donc un multiple de $h(D)$.

Pour trouver ces relations, on se sert du lemme suivant :

Lemme 1.3.1 *Soit (a, b, c) une forme primitive définie positive de discriminant $D < 0$, et $a = \prod_p p^{v_p}$ la décomposition en facteurs premiers de a. On a alors, à équivalence près :*

$$(a, b, c) = \prod_p f_p^{\epsilon_p v_p},$$

où $f_p = (p, b_p, c_p)$ est la forme première correspondant à p, et $\epsilon_p = \pm 1$ est défini par la congruence

$$b \equiv \epsilon_p b_p \mod 2p.$$

Démonstration: Cohen [Coh96a, Lemme 5.5.1]. □

On peut alors engendrer les relations dans Λ : on choisit aléatoirement des exposants entiers e_p et on calcule la forme réduite (a, b, c) équivalente à $\prod_{p \in \mathcal{P}} f_p^{e_p}$. Si tous les facteurs de a sont dans $\mathcal{P}$, on a alors la relation

$$\prod_{p \in \mathcal{P}} f_p^{e_p - \epsilon_p v_p} = 1,$$

ce qui nous donne l'élément

$$(e_p - \epsilon_p v_p)_{p \in \mathcal{P}} \in \Lambda \subset \mathbb{Z}^n.$$

En reprenant cette procédure, on peut espérer engendrer entièrement Λ si $\mathcal{P}$ a été choisi suffisamment grand. Le point crucial est donc le choix de $\mathcal{P}$. On pose

$$\mathcal{P} = \{p \leqslant P, \left(\frac{D}{p}\right) \neq -1\}$$

[1]Pour un approfondissement de l'algorithme, aller voir McCurley [McC89] ou encore Cohen [Coh96a, §5.5].

pour un certain P. Il faut trouver un compromis pour P : il doit être suffisamment grand sinon les nombres a ne se factoriseront pas en des nombres premiers inférieurs à P et suffisamment petit sinon la factorisation de a nécessite trop de temps. Mc-Curley propose de prendre P de l'ordre de $L(|D|)^\alpha$ où $L(x)$ est défini comme étant $e^{\sqrt{\ln x \ln \ln x}}$ et α dépend de l'implantation. De plus, en supposant l'hypothèse généralisée de Riemann, il faut que $P \geqslant 6 \ln^2|D|$ afin que les classes des formes primitives f_p avec $p \in \mathcal{P}$ engendrent le groupe de classes. On choisit donc

$$P = \max(6 \ln^2|D|, L(|D|)^\alpha).$$

Cet algorithme a été amélioré par Jacobson [Jac99] en adaptant à cette méthode un crible quadratique [Sil87]. On accélère ainsi la recherche de relations.

Chapitre 2

Réseaux sur $\mathbb{C}$

Après avoir introduit ces quelques notions sur les ordres dans un corps quadratique imaginaire, il est clair qu'elles sont très liées à la théorie des réseaux sur $\mathbb{C}$. Avant de faire apparaître ce lien entre les ordres et les réseaux dans la théorie de la multiplication complexe, nous allons tout d'abord revoir les fonctions elliptiques, le j-invariant d'un réseau et enfin les fonctions modulaires. On trouvera de plus amples détails dans le livre de Lang [Lan87] ainsi que dans le livre de Cox [Cox89].

2.1 Fonctions elliptiques

Tout d'abord, on rappelle qu'un *réseau* Λ est un sous-groupe additif Λ de $\mathbb{C}$ qui est engendré par deux nombres complexes ω_1 et ω_2 linéairement indépendants sur $\mathbb{R}$.

Les *fonctions elliptiques* sont des fonctions méromorphes sur le plan complexe qui sont invariantes par translation par un réseau Λ. Ainsi, les fonctions elliptiques sont bien définies sur le tore complexe $\mathbb{C}/\Lambda$. Elles nous permettront de paramétriser les courbes elliptiques sur $\mathbb{C}$.

2.1.1 La fonction de Weierstrass

La fonction elliptique classique d'étude est la fonction de Weierstrass $\wp$. Étant donné un réseau Λ, la fonction de Weierstrass $\wp$ est définie comme suit :

$$\wp(z;\Lambda) = z^{-2} + \sum_{\omega\in\Lambda-\{0\}} ((z-\omega)^{-2} - \omega^{-2}).$$

L'étude de cette fonction se justifie par le théorème suivant.

Théorème 2.1.1 *Le corps des fonctions elliptiques par rapport à Λ est engendré par $\wp(z;\Lambda)$ et $\wp'(z;\Lambda)$.*

Lorsque l'on parlera d'un réseau fixé Λ, on notera $\wp(z)$ au lieu de $\wp(z;\Lambda)$

Théorème 2.1.2 *Soit $\wp(z)$ la fonction de Weierstrass pour le réseau Λ.*

1. *$\wp(z)$ est une fonction elliptique pour Λ dont les singularités consistent en des pôles doubles aux points de Λ.*
2. *$\wp(z)$ satisfait l'équation différentielle*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

où les constantes $g_2(\Lambda)$ et $g_3(\Lambda)$ sont définies par

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4}$$
$$g_3(\Lambda) = 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}.$$

3. $\wp(z)$ satisfait la loi d'addition

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

pour tous z, $w \notin \Lambda$ et $z + w \notin \Lambda$.

Démonstration: Cox [Cox89, théorème 10.2] □

Étant donné un réseau Λ, on peut alors définir les constantes $g_2(\Lambda)$ et $g_3(\Lambda)$ qui apparaissent dans l'équation différentielle de $\wp(z)$. On pose

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

Proposition 2.1.1 *Si Λ est un réseau, alors $\Delta(\Lambda) \neq 0$.*

Démonstration: Cox [Cox89, proposition 10.7] □

Les fonctions elliptiques dépendent du réseau sur lesquelles on les définit, mais il peut arriver que deux réseaux différents aient la même fonction elliptique à une constante près. On dira que deux réseaux Λ et Λ' sont *homothétiques* s'il existe un nombre complexe α tel que $\Lambda' = \alpha\Lambda$. Si $f(z)$ est une fonction elliptique pour Λ, alors $f(\alpha z)$ est une fonction elliptique pour $\alpha\Lambda$. De plus, la fonction $\wp$ se transforme comme

$$\wp(\alpha z; \alpha\Lambda) = \alpha^{-2}\wp(z; \Lambda).$$

et on a $\Delta(\Lambda) = \alpha^{12}\Delta(\alpha\Lambda)$.

2.1.2 j-invariant d'un réseau

Le *j-invariant* $j(\Lambda)$ du réseau Λ est défini par le nombre complexe

$$j(\Lambda) = 1728\,\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\,\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

On remarque que $j(\Lambda)$ est toujours défini puisque $\Delta(\Lambda) \neq 0$. Le j-invariant $j(\Lambda)$ caractérise le réseau Λ à homothétie près :

Théorème 2.1.3 *Si Λ et Λ' sont deux réseaux de $\mathbb{C}$, alors $j(\Lambda) = j(\Lambda')$ si et seulement si Λ et Λ' sont homothétiques.*

Démonstration: Cox [Cox89, théorème 10.9] □

Soit $\mathcal{H}$ le demi-plan supérieur de $\mathbb{C}$, i.e. $\mathcal{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$. Soit $\tau \in \mathcal{H}$, on peut alors définir $j(\tau) = j([1,\tau])$. Les propriétés de $j(\tau)$ sont liées à l'action de $\mathrm{SL}(2,\mathbb{Z})$ sur le demi-plan supérieur $\mathcal{H}$. Cette action est définie de la manière suivante : soit $\tau \in \mathcal{H}$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, alors $\gamma\tau = \frac{a\tau+b}{c\tau+d}$. On peut vérifier que $\gamma\tau \in \mathcal{H}$ et on dira alors que τ et $\gamma\tau$ sont $\mathrm{SL}(2,\mathbb{Z})$-équivalents. Alors la fonction j a les propriétés suivantes :

Théorème 2.1.4 *1. $j(\tau)$ est une fonction holomorphe sur $\mathcal{H}$.*

2. Si τ et τ' sont dans $\mathcal{H}$, alors $j(\tau) = j(\tau')$ si et seulement si τ et τ' sont $\mathrm{SL}(2, \mathbb{Z})$-équivalents. $j(\tau)$ est donc invariant sous l'action de $\mathrm{SL}(2, \mathbb{Z})$.

3. $j : \mathcal{H} \to \mathbb{C}$ est surjective.

Démonstration: Cox [Cox89, théorème 11.2] □

On déduit de la surjectivité de la fonction j le corollaire suivant.

Corollaire 2.1.1 *Soient g_2 et g_3 deux constantes complexes arbitraires telles que $g_2^3 - 27g_3^2 \neq 0$. Il existe alors un réseau Λ tel que $g_2(\Lambda) = g_2$ et $g_3(\Lambda) = g_3$.*

Comme $j(\tau)$ est invariant sous l'action de $\mathrm{SL}(2, \mathbb{Z})$, on a

$$j(\tau + 1) = j\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau\right) = j(\tau).$$

$j(\tau)$ est donc une fonction holomorphe en $q = q(\tau) = e^{2\pi i\tau}$, définie pour $0 < |q| < 1$. Par conséquent, $j(\tau)$ a un développement en série de Laurent

$$j(\tau) = \sum_{n=-\infty}^{+\infty} c_n q^n,$$

que l'on appellera le *q-développement* de $j(\tau)$. On peut le spécifier :

Théorème 2.1.5 *Le q-développement de $j(\tau)$ est*

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n=0}^{+\infty} c_n q^n, \tag{2.1}$$

où les coefficients c_n sont des entiers pour tout $n \geqslant 0$.

Démonstration: Apostol [Apo76, §1], Lang [Lan87, §4.1] ou bien encore [Ser70, §7.3]. □

2.1.3 Courbes elliptiques définies sur $\mathbb{C}$

L'étude des réseaux sur $\mathbb{C}$ et des fonctions elliptiques se justifie par l'isomorphisme suivant.

Théorème 2.1.6 *Soient Λ un réseau de $\mathbb{C}$ et les constantes g_2 et g_3 définies comme dans le théorème 2.1.2. Alors la correspondance définie de $\mathbb{C}/\Lambda$ vers la courbe elliptique $E : y^2 = 4x^3 - g_2x - g_3$ donnée par :*

$$z \mapsto \begin{cases} (\wp(z), \wp'(z)) \text{ si } z \neq 0, \\ O_E \text{ sinon,} \end{cases}$$

est un isomorphisme.

Il est donc clair que les résultats que nous allons présenter par la suite concernant les réseaux pourrons s'appliquer à la théorie des courbes elliptiques.

2.2 Fonctions et équations modulaires

Avant de pouvoir introduire des notions de multiplication complexe, il nous faut d'abord introduire les notions de fonctions modulaires et d'équations modulaires.

2.2.1 Fonctions modulaires

On peut définir les fonctions modulaires sur n'importe quel sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$. Dans notre cas, nous nous intéresserons plus particulièrement aux sous-groupes $\Gamma_0(m)$ de $\mathrm{SL}(2,\mathbb{Z})$, qui sont définis de la manière suivante :

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \mod m \right\}.$$

Une *fonction modulaire pour* $\Gamma_0(m)$ est une fonction complexe $f(\tau)$ définie sur le demi-plan supérieur $\mathcal{H}$, sauf pour des singularités isolées, qui satisfait les trois conditions suivantes :

1. $f(\tau)$ est méromorphe sur $\mathcal{H}$.
2. $f(\tau)$ est invariant sous l'action de $\Gamma_0(m)$, i.e. $\forall \tau \in \mathcal{H}$ et $\forall \gamma \in \Gamma_0(m), f(\gamma\tau) = f(\tau)$.
3. pour tout γ dans $\mathrm{SL}(2,\mathbb{Z})$, le q-développement de $f(\gamma\tau)$ a un nombre fini de coefficients non nuls pour les exposants negatifs.

On peut traduire la condition (3) comme suit. Supposons que $f(\tau)$ satisfasse (1) et (2) et soit $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ alors $f(\gamma\tau)$ est périodique de période m. En effet, on remarque que $\tau + m = U\tau$, où $U = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, on voit alors que $\gamma U \gamma^{-1} \in \Gamma_0(m)$ et on a donc

$$f(\gamma(\tau + m)) = f(\gamma U \tau) = f(\gamma U \gamma^{-1} \gamma \tau) = f(\gamma\tau)$$

puisque $f(\tau)$ est invariant sous l'action de $\Gamma_0(m)$. Par conséquent, si $q = q(\tau) = e^{2\pi i\tau}$, alors $f(\gamma\tau)$ est une fonction holomorphe en $q^{1/m}$, définie pour $0 < |q^{1/m}| < 1$. Donc $f(\gamma\tau)$ admet un développement en série de Laurent

$$f(\gamma\tau) = \sum_{n=-\infty}^{+\infty} a_n q^{n/m}.$$

Par abus de langage, cette série sera appelé le q-développement de $f(\gamma\tau)$. Ainsi, pour prouver qu'une fonction est une fonction modulaire en $\Gamma_0(m)$, il va falloir s'intéresser au q-développement de $f(\gamma\tau)$ pour tout $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. Comme $f(\tau)$ est $\Gamma_0(m)$-invariant, on devra considérer uniquement les q-développements des $f(\gamma_i\tau)$ où les γ_i sont des représentants des classes à droite modulo $\Gamma_0(m)$ de $\mathrm{SL}(2,\mathbb{Z})$. Par conséquent, il y a un nombre fini de q-développpements à vérifier.
D'après cette définition, on remarque que $j(\tau)$ est une fonction modulaire pour $\mathrm{SL}(2,\mathbb{Z}) = \Gamma_0(1)$. De plus, on peut décrire les fonctions modulaires pour $\mathrm{SL}(2,\mathbb{Z})$ et celles pour $\Gamma_0(m)$ avec la fonction j.

Théorème 2.2.1 *Soit m un entier positif.*

1. *$j(\tau)$ est une fonction modulaire pour $\mathrm{SL}(2,\mathbb{Z})$, et toute fonction modulaire pour $\mathrm{SL}(2,\mathbb{Z})$ est une fonction rationnelle en $j(\tau)$.*
2. *$j(\tau)$ et $j(m\tau)$ sont des fonctions modulaires pour $\Gamma_0(m)$, et toute fonction modulaire pour $\Gamma_0(m)$ est une fonction rationnelle en $j(\tau)$ et en $j(m\tau)$.*

Démonstration: On ne donnera pas tous les détails de la démonstration. On peut retrouver différentes démonstrations dans [Lan87, §5.2] et dans [Cox89, Théorème 11.9].

On remarque tout d'abord que la propriété (1) est juste un cas particulier de la propriété (2). Cependant, nous prouverons en premier l'assertion (1) qui nous sera utile pour démontrer l'assertion (2).
Démonstration de (1) : On dira qu'une fonction modulaire est *holomorphe à l'infini* si son q-développement n'admet aucune puissance négative de q.

Lemme 2.2.1 *(i). Une fonction modulaire holomorphe pour* $\mathrm{SL}(2,\mathbb{Z})$ *qui est holomorphe à l'infini est constante.*

(ii). Une fonction modulaire holomorphe pour $\mathrm{SL}(2,\mathbb{Z})$ *est polynômiale en* $j(\tau)$.

Démonstration: (*i*) Soit $f(\tau)$ une fonction modulaire holomorphe pour $\mathrm{SL}(2,\mathbb{Z})$ qui est holomorphe à l'infini. On prouve que $f(\mathcal{H}\cup\{\infty\})$ est compact et par le principe du maximum, alors $f(\tau)$ est constante. (*ii*) Soit $f(\tau)$ une fonction moulaire holomorphe pour $\mathrm{SL}(2,\mathbb{Z})$, alors son q-développement a un nombre fini de termes ayant une puissance négative de q, donc il existe un polynôme $A(x)$ tel que $f(\tau)-A(j(\tau))$ soit holomorphe à l'infini. Donc (*i*) nous donne le résultat souhaité. □

Cas général : Soit $f(\tau)$ une fonction modulaire quelconque pour $\mathrm{SL}(2,\mathbb{Z})$. Si l'on trouve un polynôme $B(x)$ tel que $B(j(\tau))f(\tau)$ est holomorphe sur $\mathcal{H}$, alors $f(\tau)$ est rationnelle en $j(\tau)$. Comme $f(\tau)$ a un q-développement méromorphe, donc $f(\tau)$ un nombre fini de pôles dans la région $R=\{\tau\in\mathcal{H} : |\Re(\tau)|\leqslant 1/2, |\Im(\tau)|\geqslant 1/2\}$. Par ailleurs, on peut prouver que tout pôle est $\mathrm{SL}(2,\mathbb{Z})$-équivalent à un pôle dans R, donc si $f(\tau)$ n'admet aucun pôle dans R, alors elle est holomorphe sur $\mathcal{H}$. En ne se souciant que des pôles dans R, on peut alors trouver $B(x)$ tel que $B(j(\tau))f(\tau)$ est holomorphe sur $\mathcal{H}$.

Démonstration de 2 : $j(\tau)$ est une fonction modulaire pour $\Gamma_0(m)$. Pour prouver que $j(m\tau)$ est $\Gamma_0(m)$-invariante, on remarque que pour tout $\gamma\in\Gamma_0(m)$ il existe $\gamma'\in\mathrm{SL}(2,\mathbb{Z})$ tel que $m\gamma=\gamma' m$. La démonstration du fait que, pour tout γ dans $\mathrm{SL}(2,\mathbb{Z})$, le q-développement de $j(m\gamma\tau)$ n'admet pas d'exposants négatifs, nous amène à introduire l'ensemble suivant :

$$C(m)=\left\{\begin{pmatrix} a & b\\ 0 & d\end{pmatrix} : ad=m, a>0, 0\leqslant b<d, \mathrm{pgcd}(a,b,d)=1\right\}.$$

La matrice $\sigma_0=\begin{pmatrix} m & 0\\ 0 & 1\end{pmatrix}\in C(m)$ a deux propriétés intéressantes : premièrement, $\sigma_0\tau=m\tau$ et deuxièmement,

$$\Gamma_0(m)=(\sigma_0^{-1}\mathrm{SL}(2,\mathbb{Z})\sigma_0)\cap\mathrm{SL}(2,\mathbb{Z}).$$

De plus, cet ensemble nous permet de dénombrer les classes à droite de $\mathrm{SL}(2,\mathbb{Z})$ modulo $\Gamma_0(m)$. On a en effet le lemme suivant :

Lemme 2.2.2 *Soit* $\sigma\in C(m)$, *alors l'ensemble*

$$(\sigma_0^{-1}\mathrm{SL}(2,\mathbb{Z})\sigma)\cap\mathrm{SL}(2,\mathbb{Z})$$

est une classe à droite de $\mathrm{SL}(2,\mathbb{Z})$ *modulo* $\Gamma_0(m)$. *De plus, on a une bijection entre les classes à droite modulo* $\Gamma_0(m)$ *et les éléments de* $C(m)$.

On a donc $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(m)]=|C(m)|$, où $|C(m)|=m\prod_{p|m}\left(1+\frac{1}{p}\right)$, ce qui nous permet de calculer les q-développements. Soit $\gamma\in\mathrm{SL}(2,\mathbb{Z})$ et soit $\sigma\in C(m)$ tel que γ soit dans la classe à droite engendrée par σ (Lemme 2.2.2). Il existe donc $\widetilde{\gamma}\in\mathrm{SL}(2,\mathbb{Z})$ tel que $\sigma_0\gamma=\widetilde{\gamma}\sigma$, d'où $j(m\gamma\tau)=j(\sigma_0\gamma\tau)=j(\widetilde{\gamma}\sigma\tau)=j(\sigma\tau)$ puisque $j(\tau)$ est $\mathrm{SL}(2,\mathbb{Z})$-invariant. Par suite,

$$j(m\gamma\tau)=j(\sigma\tau). \tag{2.2}$$

En considérant le q-développement de $j(\sigma\tau)$, on trouve que le q-développement de $j(m\gamma\tau)$ a un nombre fini d'exposants négatifs, donc $j(m\tau)$ est une fonction modulaire pour $\Gamma_0(m)$.

Pour prouver que toute fonction modulaire pour $\Gamma_0(m)$ est une fonction rationnelle en $j(\tau)$ et en $j(m\tau)$, il faut introduire la notion d'équation modulaire. Soit $\Gamma_0(m)\gamma_i$ où $\gamma_i = 1, \ldots, |C(m)|$ les classes à droite de $\mathrm{SL}(2, \mathbb{Z})$ modulo $\Gamma_0(m)$. On considère le polynôme en X

$$\Phi_m(X, \tau) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i \tau)).$$

On va prouver que cette expression est un polynôme en X et en $j(\tau)$. Pour cela, on s'intéresse aux coefficients de $\Phi_m(X, j(m\gamma_i\tau))$ et on va prouver que ce sont des fonctions modulaires holomorphes. On montre leur invariance sous l'action de $\mathrm{SL}(2, \mathbb{Z})$, le fait qu'ils sont méromorphes à l'infini[2]. Par conséquent, les coefficients de $\Phi_m(X, j(m\gamma_i\tau))$ sont des polynômes en $j(\tau)$ (lemme 2.2.1). Il existe donc un polynôme

$$\Phi_m(X, Y) \in \mathbb{C}[X, Y]$$

tel que

$$\Phi_m(X, \tau) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i \tau)). \tag{2.3}$$

L'équation $\Phi_m(X, Y) = 0$ est appelée l'*équation modulaire* pour m.

Par (2.2), tout $j(m\gamma_i\tau)$ peut être écrit sous la forme $j(\sigma\tau)$ pour un unique $\sigma \in C(m)$ donc

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau)). \tag{2.4}$$

On remarque que $\Phi_m(j(m\tau), j(\tau)) = 0$ puisque $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$ et que le degré de $\Phi_m(X, Y)$ en X est $|C(m)|$.

Soit $f(\tau)$une fonction modulaire quelconque pour $\Gamma_0(m)$. Afin de montrer que $f(\tau)$ est une fonction rationnelle rationnelle en $j(\tau)$ et en $j(m\tau)$, on considère la fonction

$$G(X, \tau) = \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i\tau)}{X - j(m\gamma_i\tau)} \tag{2.5}$$

$$= \sum_{i=1}^{|C(m)|} f(\gamma_i\tau) \prod_{k \neq i} (X - j(m\gamma_k\tau)). \tag{2.6}$$

$G(X, \tau)$ est un polynôme en X, et ses coefficients sont des fonctions modulaires[3] pour $\mathrm{SL}(2, \mathbb{Z})$. Par suite, ce sont des fonctions rationnelles en $j(\tau)$ et $G(X, \tau)$ est un polynôme $G(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$.

En différentiant $\Phi_m(X, j(\tau))$ par rapport à X et en substituant ce résultat dans $G(j(m\tau), j(\tau))$, on trouve

$$G(j(m\tau), j(\tau)) = f(\tau)\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)).$$

Or $\Phi_m(X, j(\tau))$ est irréductible et donc séparable, donc formellement

$$(\partial/\partial X)\Phi_m(j(m\tau), j(\tau)) \neq 0.$$

[2]Pour cela au lieu de considérer les exposants des développements en puissance de q, on regarde ceux des développements en puissance de $q^{1/m}$ et on prouve qu'il n'y a qu'un nombre fini d'exposants négatifs.

[3]La preuve est similaire à celle utilisée pour l'équation modulaire.

On peut donc écrire
$$f(\tau) = \frac{G(j(m\tau), j(\tau))}{\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau))},$$
ce qui termine la démonstration. □

2.2.2 L'équation modulaire $\Phi_m(X, Y)$

L'équation modulaire, définie par l'équation (2.3) ou (2.4), a des propriétés arithmétiques données par le théorème suivant :

Théorème 2.2.2 *Soit m un entier positif.*

1. $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.
2. $\Phi_m(X, Y)$ *est irréductible en tant que polynôme en* X.
3. $\Phi_m(X, Y) = \Phi_m(Y, X)$ *si* $m > 1$.
4. *Si m n'est pas un carré parfait , alors $\Phi_m(X, X)$ est un polynôme de degré > 1 dont le coefficient dominant est ± 1.*
5. *Si m est un premier p, alors $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \mod p\mathbb{Z}[X, Y]$.*

Démonstration: Cox [Cox89, Théorème 11.18] ou Lang [Lan87, §5.2] □

Comme les coefficients deviennent rapidement grand quand ℓ augmente, on ne va donc rappeler que les équations modulaires Φ_2 et Φ_3 :

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + c_1(XY^2 + X^2Y) - c_2(X^2 + Y^2) + c_3XY + c_4(X + Y) - c_5,$$

où : $c_1 = 1488$, $c_2 = 162000$, $c_3 = 40773375$, $c_4 = 8748000000$, $c_5 = 157464000000000$

$$\Phi_3(X, Y) = X^4 + Y^4 - X^3Y^3 + d_1(X^3Y^2 + X^2Y^3) - d_2(X^3Y + XY^3) + d_3(X^3 + Y^3)$$
$$+d_4X^2Y^2 + d_5(X^2Y + XY^2) + d_6(X^2 + Y^2) - d_7XY + d_8(X + Y)$$

où : $d_1 = 2232$, $d_2 = 1069956$, $d_3 = 36864000$, $d_4 = 2587918086$, $d_5 = 8900222976000$, $d_6 = 452984832000000$, $d_7 = 770845966336000000$ et $d_8 = 1855425871872000000000$.

On peut aussi relier les équations modulaires entre elles ce qui est agréable lorsqu'il est nécessaire de les calculer.

Proposition 2.2.1 *Soit $m > 1$ un entier et soit $\Psi(m) = m\prod_{p|m}(1 + 1/p)$ qui est le degré de $\Phi_m(X, Y)$ en tant que polynôme en X.*

(i). Si $m = m_1m_2$ avec m_1 et m_2 premiers entre eux, alors
$$\Phi_m(X, Y) = \mathrm{Res}_Z(\Phi_{m_1}(X, Z), \Phi_{m_2}(Y, Z)).$$

(ii). Si $m = p^a$ où p est un entier premier et $a > 1$, alors
$$\Phi_m(X, Y) = \begin{cases} \frac{\mathrm{Res}_Z(\Phi_p(X,Z), \Phi_{p^{a-1}}(Y,Z))}{\Phi_{p^{a-2}}(X,Y)^p}, & a > 2 \\ \frac{\mathrm{Res}_Z(\Phi_p(X,Z), \Phi_p(Y,Z))}{(X-Y)^{p+1}}, & a = 2, \end{cases}$$

Démonstration: Weber [Web02, Chap.69] □

On peut maintenant comprendre l'équation modulaire en terme de j-invariant d'un réseau. Il faut, tout d'abord, définir la notion de *sous-réseau cyclique.*

Définition 2.2.1 *Soit Λ un réseau et soit $\Lambda' \subset \Lambda$ un sous-réseau de Λ tel que :*

1. *Λ' est un sous-réseau d'indice m dans Λ, i.e. $[\Lambda : \Lambda'] = m$.*
2. *Le quotient Λ/Λ' est un groupe cyclique.*

On dit alors que Λ' est un sous-réseau cyclique de Λ.

On a alors le théorème suivant :

Théorème 2.2.3 *Soit m un entier positif. Si $u, v \in \mathbb{C}$, alors $\Phi_m(u,v) = 0$ si et seulement si il existe un réseau λ et un sous-réseau cyclique $\Lambda' \subset \Lambda$ d'indice m tel que $u = j(\Lambda')$ et $v = j(\Lambda)$.*

Démonstration: Pour démontrer ce théorème, on va d'abord s'intéresser aux sous-réseaux cycliques du réseau $[1, \tau]$ avec $\tau \in \mathcal{H}$.

Lemme 2.2.3 *Soit $\tau \in \mathcal{H}$, et consdérons le réseau $[1, \tau]$.*

1. *Étant donné un sous-réseau cyclique $\Lambda' \subset [1, \tau]$ d'indice m, il existe un unique $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, tel que $\Lambda' = d[1, \sigma\tau]$.*
2. *Inversement, si $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, alors $d[1, \sigma\tau]$ est un sous-réseau cyclique d'indice m.*

Démonstration: Cox [Cox89, Lemme 11.24] □

Par ce lemme, les j-invariants des sous-réseaux cycliques Λ' d'indice m du réseau $[1, \tau]$ sont donnés par

$$j(\Lambda') = j(d[1, \sigma\tau]) = j([1, \sigma\tau]) = j(\sigma\tau).$$

Par (2.4), il s'ensuit que les racines de $\Phi_m(X, j(\tau)) = 0$ sont exactement les j-invariants des sous-réseaux cycliques d'indice m du réseau $[1, \tau]$. De plus, on sait que la fonction j est surjective, donc le théorème est démontré. □

2.3 Multiplication complexe

On remarque tout d'abord que les ordres dans des corps quadratiques imaginaires nous donnent une classe particulière de réseaux dans $\mathbb{C}$. En effet soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K et soit $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$. Comme $\mathfrak{a} = [\alpha, \beta]$ où $\alpha, \beta \in K$ et K est un corps quadratique imaginaire, α et β sont linéairement indépendants sur $\mathbb{R}$. Comme K peut être considéré comme un sous ensemble de $\mathbb{C}$, $\mathfrak{a}$ est un réseau de $\mathbb{C}$ et donc le j-invariant $j(\mathfrak{a})$ est bien défini.

Nous allons discuter de la rationnalité de $\wp(\alpha z : \Lambda)$ en $\wp(z : \Lambda)$ où Λ est un réseau de $\mathbb{C}$ et $\alpha \in \mathbb{C}$. En se servant de la loi d'addition de $\wp(z : \Lambda)$ donnée en 2.1.2 et en utilisant la loi de L'Hospital, on prouve par induction que $\wp(nz : \Lambda)$ est rationnelle en $\wp(z : \Lambda)$ pour tout $n \in \mathbb{Z}$. Il ne nous reste plus qu'à traiter le cas où α n'est pas un entier relatif.

Théorème 2.3.1 *Soit Λ un réseau de $\mathbb{C}$ et soit $\wp(z)$ la fonction de Weierstrass pour Λ. Alors pour tout nombre $\alpha \in \mathbb{C} - \mathbb{Z}$ les propsitions suivantes sont équivalentes :*

1. *$\wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$;*
2. *$\alpha\Lambda \subset \Lambda$;*
3. *il existe un ordre $\mathcal{O}$ dans un corps quadratique imaginaire K tel que $\alpha \in \mathcal{O}$ et Λ est homothétique à un idéal fractionnaire propre de $\mathcal{O}$.*

De plus, si ces conditions sont satisfaites, alors $\wp(\alpha z)$ peut être écrit sous la forme

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

où $A(x)$ et $B(x)$ sont des polynômes premiers entre eux tels que

$$\deg A(x) = \deg B(x) + 1 = [\Lambda : \alpha\Lambda] = N(\alpha).$$

Démonstration: Cox [Cox89, Théorème 10.14] □

Ce théorème montre que si une fonction elliptique est à multiplication par $\alpha \in \mathbb{C} - \mathbb{Z}$, alors elle est à multiplication par tout un ordre $\mathcal{O}$ dans un corps quadratique imaginaire. On remarque que tous les élements de $\mathcal{O} - \mathbb{Z}$ sont de vrais complexes (i.e. ne sont pas des réels), d'où le nom de *multiplication complexe*.

À partir du theorème 2.3.1, on peut donner une relation entre les classes d'homothétie d'un réseau et le groupe de classes d'idéaux d'un ordre.

Corollaire 2.3.1 *Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire. Alors il existe une bijection entre le groupe de classes d'idéaux $C(\mathcal{O})$ et les classes d'homothétie de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$.*

Démonstration: On considère l'ensemble des réseaux $\Lambda \subset \mathbb{C}$ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$. D'après le théorème 2.3.1, on déduit qu'un tel réseau Λ est un idéal fractionnaire propre de $\mathcal{O}$ et inversement que tout idéal propre fractionnaire de $\mathcal{O}$ est un tel réseau. Il ne nous reste plus qu'à prouver que deux idéaux propres fractionnaires de $\mathcal{O}$ sont homothétiques en tant que réseaux si et seulement s'ils déterminent la même classe d'équivalence dans le groupe de classe d'idéaux $C(\mathcal{O})$.
Supposons que $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux propres fractionnaires de $\mathcal{O}$ tels qu'il existe $\lambda \in \mathbb{C}$ tel que $\mathfrak{a} = \lambda\mathfrak{b}$. On a donc $\mathfrak{a} = \lambda\mathcal{O}\mathfrak{b}$ d'où $\mathfrak{a}$ et $\mathfrak{b}$ représentent bien la même classe d'équivalence dans $C(\mathcal{O})$.

Supposons que $\mathfrak{a}$ et $\mathfrak{b}$ représentent la même classe d'équivalence dans $C(\mathcal{O})$. Il existe donc un idéal fractionnaire principal $\mathfrak{m}$ de $\mathcal{O}$ tel que $\mathfrak{a} = \mathfrak{m}\mathfrak{b}$. Comme $\mathfrak{m}$ est principal, alors $\mathfrak{m} = m\mathcal{O}$, pour $m \in K$. Donc $\mathfrak{a} = m\mathcal{O}\mathfrak{b}$ d'où $\mathfrak{a} = m\mathfrak{b}$. On a bien le résultat voulu.

Il existe donc une bijection entre la classe d'homothéties de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$ et le groupe de classe d'idéaux $C(\mathcal{O})$. □

Après avoir déterminé les conditions nécessaires à la rationnalité de $\wp(\alpha z)$ en $\wp(z)$, on va maintenant se concentrer sur le j-invariant d'un idéal fractionnaire propre d'un ordre $\mathcal{O}$ dans un corps quadratique imaginaire. Ce résultat est appelé le premier théorème de multiplication complexe.

Théorème 2.3.2 *Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K, et soit $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$. Alors le j-invariant $j(\mathfrak{a})$ est un entier algébrique et $K(j(\mathfrak{a}))$ est le corps de classes d'anneau de l'ordre $\mathcal{O}$.*

Démonstration: Cox [Cox89, Théorème 11.1] □

Il est donc intéressant de considérer le polynôme minimal de $j(\mathfrak{a})$.

Définition 2.3.1 *Soit un ordre $\mathcal{O}$ dans K.* L'équation de classe *$H_{\mathcal{O}}(X)$ de $\mathcal{O}$ est le polynome minimal unitaire de $j(\mathcal{O})$ sur $\mathbb{Q}$.*

Les coefficients de $H_{\mathcal{O}}(X)$ sont entiers. On peut exprimer de manière plus explicitement ce polynôme.

Proposition 2.3.1 *Soit $\mathcal{O}$ un ordre dans K et soit $\mathfrak{a}_i$, $i = 1, \ldots, h$ les représentants des classes d'idéaux (donc h est le nombre de classe). Alors l'équation de classe est donnée par :*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)) \tag{2.7}$$

Chapitre 3

Introduction aux courbes elliptiques

La théorie des réseaux sur $\mathbb{C}$ et plus particulièrement des fonctions elliptiques est une introduction analytique à la théorie des courbes elliptiques. Dans ce chapitre, on va s'attarder sur la partie algébrique de cette théorie. Pour approfondir le sujet, de nombreux livres sont à notre dispositions. Nous citerons en particulier le livre de Silverman [Sil86], mais aussi [Kna92, Cas91].

3.1 Courbes elliptiques et équations de Weierstrass

Soit $\mathbb{K}$ un corps. On définit sur $\mathbb{K}$ une équation de Weierstrass comme étant une équation de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.1}$$

où les coefficients a_1, a_2, a_3, a_4 et a_6 sont des éléments de $\mathbb{K}$. On définit les notations suivantes :

$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \text{ d'où } 4b_8 = b_2b_6 - b_4^2.$$

On définit aussi :

$$c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \text{ d'où } 12^3\Delta = c_4^3 - c_6^2,$$

$$j = c_4^3/\Delta,$$

$$\omega = \mathrm{d}x/(2y + a_1x + a_3).$$

La constante Δ est appelée *discriminant* de l'équation de Weierstrass. La courbe définie par l'équation de Weierstrass (3.1) est non-singulière si et seulement si Δ est non nul. La constante j définit un autre invariant de la courbe : le *j-invariant.*

Définition 3.1.1 *Une courbe elliptique E sur $\mathbb{K}$ est une courbe définie par une équation de Weierstrass (3.1) non singulière.*

On notera souvent l'équation de Weierstrass définissant une courbe elliptique E par :

$$F_E(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

Il est possible de simplifier la forme de l'équation de Weierstrass selon la caractéristique du corps sur lequel on considère la courbe.

Lemme 3.1.1 *Soit E une courbe elliptique sur $\mathbb{K}$.*

- *Si* $\mathrm{car}(\mathbb{K}) \neq 2, 3$*, alors* E *peut être définie par une équation de Weierstrass de la forme* $y^2 = x^3 + a_4x + a_6$*;*
- *Si* $\mathrm{car}(\mathbb{K}) = 3$ *et* $j(E) \neq 0$*, alors* E *peut être définie par une équation de Weierstrass de la forme* $y^2 = x^3 + a_2x^2 + a_6$*;*
- *Si* $\mathrm{car}(\mathbb{K}) = 3$ *et* $j(E) = 0$*, alors* E *peut être définie par une équation de Weierstrass de la forme* $y^2 = x^3 + a_4x + a_6$*;*
- *Si* $\mathrm{car}(\mathbb{K}) = 2$ *et* $j(E) \neq 0$*, alors* E *peut être définie par une équation de Weierstrass de la forme* $y^2 + xy = x^3 + a_2x^2 + a_6$*;*
- *Si* $\mathrm{car}(\mathbb{K}) = 3$ *et* $j(E) = 0$*, alors* E *peut être définie par une équation de Weierstrass de la forme* $y^2 + a_3y = x^3 + a_4x + a_6$*;*

Pour pouvoir définir l'ensemble des points de E définis sur $\mathbb{K}$, il faut d'abord introduire la notion d'espace projectif.

Définition 3.1.2 *On appelle espace projectif de dimension* 2 *associé à un corps* $\mathbb{K}$ *et on note* $\mathbb{P}^2(\mathbb{K})$*, l'ensemble des classes* $(X : Y : Z)$ *de la relation d'équivalence*

$$\forall (X, Y, Z) \in \mathbb{K}^3 \setminus \{0, 0, 0\}, (X, Y, Z) \equiv (X', Y', Z') \Leftrightarrow \exists c \in \mathbb{K}^*, X' = cX, Y' = cY, Z' = cZ.$$

On peut maintenant définir l'ensemble des points d'une courbe elliptique E sur $\mathbb{K}$, ensemble noté $E(\mathbb{K})$.

Définition 3.1.3 *Étant donnée une courbe elliptique* E *sur* $\mathbb{K}$*, on définit* $E(\mathbb{K})$ *comme étant l'ensemble :*

$$E(\mathbb{K}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{K}) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}.$$

Un seul point correspond à $Z = 0$, il s'agit de $O_E = (0 : 1 : 0)$ appelé point à l'infini et chaque classe différente de O_E a un unique représentant $(X : Y : 1)$. On peut donc considérer $E(\mathbb{K})$ comme étant

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O_E\}.$$

3.2 Loi de groupe

On peut définir sur $E(\overline{\mathbb{K}})$ une loi de groupe abélien. Si l'on a $\mathbb{K} \subseteq \mathbb{K}_1 \subset \overline{\mathbb{K}}$, alors $E(\mathbb{K}_1)$ est un sous- groupe de $E(\overline{\mathbb{K}})$.

On définit la loi d'addition suivante où O_E est l'élément neutre :

Définition 3.2.1 *(Loi d'addition) Soient* P, $Q \in E(\overline{\mathbb{K}})$*,* L *la droite entre* P *et* Q *(la tangente si* $P = Q$*) et* R *le troisième point d'intersection de* L *avec* E*. Soit* L' *la droite entre* R *et* O_E*. Alors* $P + Q$ *est le point tel que* L' *intersecte* E *en* R*,* O_E *et* $P + Q$*.*

Voir Silverman [Sil86, Proposition III.2.2] pour s'assurer que cette loi définit bien une loi de groupe abélien sur $E(\overline{\mathbb{K}})$.

On a alors les formules suivantes :

- Pour tout point $P = (x_P, y_P)$ de $E(\mathbb{K})$, $P + O_E = O_E + P = P$ et $-P = (x_p, -y_p - a_1x_P - a_3)$
- Pour tous points $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ tels que $P \neq -Q$, les coordonnées (x_R, y_R) du point $R = P + Q$ sont déterminées par les formules suivantes :

$$\begin{cases} x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q \\ y_R = -(\lambda + a_1)x_R - \nu - a_3 \end{cases}$$

$$\text{avec } \lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{si } P \neq Q, \\ (3x_P^2 + 2a_2x_P + a_4 - a_1y_P)/(2y_P + a_1x_P + a_3) & \text{sinon,} \end{cases}$$
et $\nu = y_P - \lambda x_P$.

Multiplication par m

À partir de la loi de groupe, on peut définir l'application

$$\begin{aligned} [m] : & E \longrightarrow E \\ & P \longrightarrow \underbrace{P + \cdots + P}_{m \text{ fois}} \end{aligned}$$

qui à un point P associe la somme de ce point m fois. On peut exprimer cette application par des fonctions rationnelles que l'on peut déterminer récursivement à l'aide de la loi de groupe sur E. Il existe des polynômes premiers entre eux ϕ_m, ψ_m et ω_m dans $\mathbb{K}[x, y]$ telles que $[m]$ soit définie de la manière suivante

$$\begin{aligned} [m] : \ & E \to E \\ & P \mapsto [m]P = \begin{cases} O_E & \text{si} P \in E[m] \\ \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right) & \text{si} P = (x, y) \in E[\overline{\mathbb{K}}] - E[m] \end{cases} \end{aligned}$$

Définition 3.2.2 *Les polynômes ϕ_m, ψ_m et ω_m sont appelés les polynômes de m-division sur E.*

Ces polynômes sont reliés par les équations $\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$ et $2\psi_m\omega_m = \psi_{2m} - \psi_m^2(a_1\phi_m + a_3\psi_m^2)$.

En utilisant la loi de groupe, on peut expliciter les polynômes de division. On a :

$$\psi_m(x, y) = \begin{cases} (2y + a_1x + a_3)f_m(x) & \text{si } m \text{ est pair,} \\ f_m(x) & \text{sinon.} \end{cases}$$

La fonction f_m est définie récursivement à l'aide des formules suivantes :

$$f_0(x) = 0,\ f_1(x) = 1,\ f_2(x) = 1,\ f_3(x) = 3x^4 + d_2x^3 + 3d_4x^2 + 3d_6x + d_8,$$
$$f_4(x) = 2x^6 + d_2x^5 + 5d_4x^4 + 10d_6x^3 + 10d_8x^2 + (d_2d_8 - d_4d_6)x + (d_4d_8 - d_6^2),$$

et si on pose $F(x) = 4x^3 + d_2x^2 + 2d_4x + d_6$,

- $f_{2m} = f_m(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)$,
- $f_{2m+1} = \begin{cases} F^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 & \text{si } m \text{ est pair,} \\ f_{m+2}f_m^3 - F^2 f_{m-1}f_{m+1}^3 & \text{sinon.} \end{cases}$

Pour les corps de caractéristiques différentes de 2, ces formules nous donne une construction explicite de l'application $[m]$. Il faut être, par contre, plus attentif dans le cas où le corps est de caractéristique 2.

Définition 3.2.3 *Les éléments du noyau de la multiplication par m dans E sont appelés* les points de m-torsion. *On note $E[m]$ l'ensemble des points de m-torsion.*

À partir des polynômes de division, on peut déterminer si un point P appartient à $E[m]$.

Proposition 3.2.1 *Soit $P \in E(\bar{\mathbb{K}})$. Alors pour tout $m \neq 2 \in \mathbb{Z}$ et $[2]P \neq O_E$, $P \in E[m]$ si et seulement si $P = O_E$ ou lorsque $P = (X, Y)$, $f_m(X) = 0$.*

3.3 Isogénies

On va tout d'abord introduire les notions de base sur les isogénies pour pouvoir après s'intéresser aux endomorphismes, aux isomorphismes et enfin à la construction d'isogénies.

3.3.1 Définitions et propriétés

Une isogénie est définie comme suit :

Définition 3.3.1 *Soient E_1 et E_2 deux courbes elliptiques. Une* isogénie *de E_1 dans E_2 est un morphisme*

$$\varphi : E_1 \to E_2$$

satisfaisant $\varphi(O_{E_1}) = O_{E_2}$.

On dira que E_1 et E_2 sont isogènes s'il existe une isogénie φ non nulle entre elles (où $\varphi(E_1) \neq \{O_{E_2}\}$). Il serait normal de vouloir s'intéresser aux isogénies qui sont des homomorphismes pour la loi de groupe. Mais il n'y a pas à se restreindre à cette classe d'isogénies puisque d'après le théorème suivant toute isogénie est un homomorphisme de groupe.

Théorème 3.3.1 *Soit $\varphi : E_1 \to E_2$ une isogénie. Alors*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q).$$

Démonstration: Silverman [Sil86, Théorème III.4.8]. □

Exemple d'isogénie : La loi de groupe abélien $E \times E \to E$ est un morphisme de variétés défini sur $\mathbb{K}$. La multiplication par m est donc une isogénie.

Comme toute isogénie $\varphi : E_1 \to E_2$ est un homomorphisme de groupe, pour tout entier n on a $[n]_{E_2} \circ \varphi = \varphi \circ [n]_{E_1}$. Plus généralement, le noyau et l'image d'une isogénie satisfont les conditions suivantes.

Théorème 3.3.2 *Soit φ une isogénie non nulle définie d'une courbe E_1 vers une courbe E_2 sur un corps $\mathbb{K}$. Alors :*

1. *Ker(φ) est un groupe fini.*
2. *Si $\mathbb{K}$ est un corps algébriquement clos, φ est surjective.*

Démonstration: Silverman [Sil86, §II.2]. □

Lorsque φ est surjective, elle induit l'injection suivante sur les corps de fonctions associés à E_1 et E_2 :

$$\begin{aligned} \varphi^* \ : \ \mathbb{K}(E_2) &\to \mathbb{K}(E_1), \\ f &\mapsto f \circ \varphi. \end{aligned}$$

On peut alors définir le degré d'une isogénie.

Définition 3.3.2 *Si $\mathbb{K}$ est un corps algébriquement clos, une isogénie φ entre deux courbes elliptiques E_1 et E_2 définies sur $\mathbb{K}$ est dite* séparable *ou* inséparable *selon les propriétés de l'extension $[\mathbb{K}(E_1) : \varphi^*(\mathbb{K}(E_2))]$. On note alors $\deg_s(\varphi)$ et $\deg_i(\varphi)$ les degrés correspondants. Le degré de φ est alors égal à $\deg(\varphi) = \deg_s(\varphi)\deg_i(\varphi)$.*

Nous avons alors les propriétés suivantes.

Théorème 3.3.3 *Soit φ une isogénie non constante d'une courbe E_1 vers une courbe E_2 sur un corps algébriquement clos $\mathbb{K}$. Alors :*

1. *pour tout point S de $E_2(\mathbb{K})$, nous notons $\varphi^{-1}(S)$ le sous-ensemble de $E_1(\mathbb{K})$ qui a pour image S. Le cardinal de $\varphi^{-1}(S)$ est fini et égal à* $\deg_s(\varphi)$ *;*
2. *si m est un entier positif, $[m]$ est une isogénie de degré m^2.*

Démonstration: Silverman [Sil86, Théorème 4.10]. □

Lorsque le corps $\mathbb{K}$ n'est pas algébriquement clos, nous définissons le degré d'une isogénie comme étant le degré de l'isogénie considérée comme définie sur la clôture algébrique de $\mathbb{K}$.

On notera $\mathrm{Hom}_{\mathbb{K}}(E_1, E_2)$ l'ensemble des homomorphismes de E_1 dans E_2 sur $\mathbb{K}$, et $\mathrm{End}_{\mathbb{K}}(E) = \mathrm{Hom}_{\mathbb{K}}(E, E)$. On écrira $\mathrm{Hom}(E_1, E_2)$ au lieu de $\mathrm{Hom}_{\overline{\mathbb{K}}}(E_1, E_2)$ et $\mathrm{End}(E)$ au lieu de $\mathrm{End}_{\overline{\mathbb{K}}}(E)$. La structure de groupe de E_2 détermine une structure de groupe sur $\mathrm{Hom}(E_1, E_2)$ tel que, en tant que $\mathbb{Z}$-module, $\mathrm{Hom}(E_1, E_2)$ est libre de rang au plus 4 [Sil86, Corollaire III.7.5].

3.3.2 L'isogénie duale

Théorème 3.3.4 *Soit φ une isogénie non constante définie d'une courbe E_1 vers une courbe E_2 sur un corps $\mathbb{K}$. Alors, il existe une unique isogénie $\widehat{\varphi}$ de E_2 vers E_1 telle que $\widehat{\varphi} \circ \varphi = [\deg(\varphi)]_{E_1}$. Cette isogénie est appelée* l'isogénie duale *de φ.*

Démonstration: Silverman [Sil86, Théorème 6.2]. □

Les propriétés de l'isogénie duale vont nous donner des renseignements en particulier sur le noyau de la multiplication par m, i.e. sur l'ensemble $E[m]$ des points de m-torsion de la courbe.

Théorème 3.3.5 *Soit $\varphi : E_1 \to E_2$ une isogénie.*

1. *Soit $\lambda : E_2 \to E_3$ une autre isogénie. Alors :*
$$\widehat{\lambda \circ \varphi} = \hat{\varphi} \circ \hat{\lambda}.$$
2. *Soit $\psi : E_1 \to E_2$ une autre isogénie. Alors :*
$$\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}.$$
3. *Pour tout $m \in \mathbb{Z}$,*
$$\widehat{[m]} = [m] \text{ et } \deg[m] = m^2.$$
4. $\deg\hat{\varphi} = \deg\varphi$.
5. $\hat{\hat{\varphi}} = \varphi$.

Démonstration: [Sil86]. □

Corollaire 3.3.1 *Soit E une courbe elliptique et $m \in \mathbb{Z}$, $m \neq 0$.*

1. *Si* $\mathrm{car}(\mathbb{K}) = 0$ *ou si m est premier à* $\mathrm{car}(\mathbb{K})$, *alors*
$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$
2. *Si* $\mathrm{car}(\mathbb{K}) = p$, *alors :*
$$\text{soit } E[p^e] \cong \{O_E\} \text{ pour tout } e \geqslant 1;$$
$$\text{soit } E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \text{ pour tout } e \geqslant 1.$$

3.3.3 Endomorphismes

La composition d'endomorphismes donne une structure d'anneau sur $\mathcal{O} = \mathrm{End}(E)$, et on appellera $\mathcal{O}$ l'anneau d'endomorphisme de E. L'anneau d'endomorphismes d'une courbe contient toujours au minimum $\mathbb{Z}$. En effet la multiplication par m nous permet de définir un homomorphisme d'anneau injectif :

$$[\,] : \mathbb{Z} \longrightarrow \mathrm{End}(E).$$

En revanche, il est tout à fait possible que $\mathrm{End}(E)$ ne soit pas réduit qu'à $\mathbb{Z}$.

Définition 3.3.3 *Une courbe elliptique E est dite à multiplication complexe si* $\mathrm{End}(E)$ *contient un endomorphisme différent de $[m]_E$ pour tout entier m.*

Dans tous les cas, la structure de $\mathrm{End}(E)$ est donnée par le théorème suivant.

Théorème 3.3.6 $\mathrm{End}(E)$ *est soit isomorphe à $\mathbb{Z}$, soit isomorphe à un ordre dans un corps de nombre quadratique imaginaire, soit isomorphe à un ordre dans une algèbre de quaternions.*

Démonstration: Silverman [Sil86, Corollaire 9.4]. □

3.3.4 Isomorphismes

Deux courbes elliptiques sont dites isomorphes si elles sont isomorphes en tant que variétés algébriques projectives. Le j-invariant de E est défini par $j = c_4^3/\Delta$. Il détermine l'ensemble des courbes elliptiques isomorphes à E sur $\overline{\mathbb{K}}$. En effet, on a le théorème suivant.

Théorème 3.3.7 *Deux courbes elliptiques sont isomorphes (sur $\overline{\mathbb{K}}$) si et seulement si elles ont le même j-invariant.*

Démonstration: Silverman [Sil86, Proposition III.1.4]. □

3.4 Courbes elliptiques définies sur un corps fini

Dans cette section nous ne considérons que des courbes elliptiques définies sur un corps fini $\mathbb{F}_q$ où $q = p^d$ et p premier. Le fait de considérer une courbe elliptique sur un corps fini nous donne un groupe abélien fini, celui des points rationnels de la courbe. Afin de pouvoir étudier ce groupe (sa cardinalité, sa structure), nous allons tout d'abord regarder un endomorphisme particulier des courbes définies sur un corps fini : l'*endomorphisme de Frobenius*.

Par la suite, nous supposons que E est une courbe elliptique définie sur $\mathbb{F}_q$.

3.4.1 L'endomorphisme de Frobenius

Définition 3.4.1 *L'application $\pi : (x, y) \mapsto (x^q, y^q)$ définit un homomorphisme de groupe. Cette application est appelée* endomorphisme de Frobenius.

L'endomorphisme de Frobenius nous permet de déterminer plus précisément le type d'anneau d'endomorphismes de la courbe elliptique.

Théorème 3.4.1 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soit π l'endomorphisme de Frobenius relatif à $\mathbb{F}_q$. Les conditions suivantes sont équivalentes :*

1. *$E[p^r] = 0$ pour tout $r \geqslant 1$;*
2. *le dual $\widehat{\pi}$ de l'endomorphisme de Frobenius est purement inséparable ;*
3. *la trace de l'endomorphisme de Frobenius est divisible par p ;*

4. *l'anneau d'endomorphisme* End(E) *défini sur* $\overline{\mathbb{F}_q}$ *est un ordre dans une algèbre de quaternions.*

Si les conditions précédentes ne sont pas satisfaites, alors l'ensemble des affirmations suivantes sont satisfaites :

1. $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ *pour tout* $r \geqslant 1$ *;*
2. *le dual* $\widehat{\pi}$ *de l'endomorphisme de Frobenius est séparable ;*
3. *la trace de l'endomorphisme de Frobenius est relativement première à* p *;*
4. *l'anneau d'endomorphisme* End(E) *de* E *est un ordre dans une extension quadratique imaginaire de* $\mathbb{Q}$.

Démonstration: [Sil86, Théorème V.3.1]. □

Dans le premier cas du théorème, on dira que la courbe est *supersingulière* ; dans l'autre cas, on dit que la courbe est *ordinaire*.

3.4.2 Cardinalité de E

L'endomorphisme de Frobenius admet pour équation caractéristique :

$$\pi^2 - t\pi + q = 0. \tag{3.2}$$

L'élément t est appelé la *trace* de l'endomorphisme de Frobenius. Cette équation a un rôle déterminant dans le calcul de la cardinalité d'une courbe elliptique définie sur un corps fini.

Proposition 3.4.1 *Soit* E *une courbe elliptique définie sur un corps fini à* q *éléments alors* $\#E(\mathbb{F}_q) = q + 1 - t$ *où* t *est défini comme précédemment.*

En utilisant les propriétés du degré, on trouve une borne sur la trace du Frobenius.

Proposition 3.4.2 *La trace du Frobenius satisfait*

$$|t| \leqslant 2\sqrt{q}.$$

À partir de la cardinalité d'une courbe elliptique on peut déterminer les courbes qui lui sont isogènes sur $\mathbb{F}_q$.

Théorème 3.4.2 *Deux courbes elliptiques sont isogènes sur* $\mathbb{F}_q$ *si et seulement si elles ont même cardinalité.*

3.4.3 Structure du groupe des points rationnels de E

Théorème 3.4.3 *Le groupe abélien* $E(\mathbb{F}_q)$ *est de rang 1 ou 2. Il est isomorphe à* $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ *où* n_2 *divise* n_1 *et de plus* n_2 *divise* $q - 1$.

On peut, grâce à l'endomorphisme de Frobenius, déterminer de manière plus précise le groupe des points rationnels de E en fonction de la structure de l'anneau d'endomorphismes .

Théorème 3.4.4 *Soit* E *une courbe elliptique sur* $\mathbb{F}_q$. *Soit* π *l'endomorphisme de Frobenius de* E. *De plus, soit* $\mathcal{K}$ *une extension finie de* $\mathbb{F}_q$ *de degré* r.

1. *Supposons que* $\pi \notin \mathbb{Z}$. *Alors* $\mathrm{End}_{\mathbb{F}_q}(E)$ *est de rang 2 sur* $\mathbb{Z}$, *et il existe un isomorphisme*

$$E(\mathcal{K}) \cong \frac{\mathrm{End}_{\mathbb{F}_q}(E)}{(\pi^r - 1)}.$$

2. Supposons que $\pi \in \mathbb{Z}$. *Alors* $\mathrm{End}_{\mathbb{F}_q}(E)$ *est de rang 4 sur* $\mathbb{Z}$, *et l'on a*

$$E(\mathcal{K}) \cong \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)} \oplus \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)}$$

comme groupes abéliens, et ce groupe a, à isomorphismes près, exactement une structure de $\mathrm{End}_{\mathbb{F}_q}(E)$*-module gauche. Plus précisément, on a*

$$E(\mathcal{K}) \oplus E(\mathcal{K}) \cong \frac{\mathrm{End}_{\mathbb{F}_q}(E)}{(\pi^r - 1)}$$

comme $\mathrm{End}_{\mathbb{F}_q}(E)$*-modules.*

Démonstration: Lenstra [Len96, Théorème 1]. □

3.4.4 Réduction et relèvement de courbes elliptiques

Les deux théorèmes de Deuring nous montrent que lors de la réduction ou du relèvement d'une courbe, nous pouvons conserver son anneau d'endomorphismes.

Théorème 3.4.5 *Soient* $\mathcal{O}$ *un ordre dans un corps quadratique imaginaire* K, L *le corps de classes d'anneau de* $\mathcal{O}$, $p \in \mathbb{Z}$ *premier qui se décompose complètement dans* L *et* $\mathfrak{P}$ *un idéal premier de* L *qui est au-dessus de* $p = \mathfrak{p}\mathfrak{p}'$. *Soit* E *une courbe elliptique sur* L *avec* $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. *Si* E *a bonne réduction modulo* $\mathfrak{P}$, *alors il existe* $\pi \in \mathcal{O}$ *tel que* $p = \pi\overline{\pi}$ *et*

$$|\overline{E}(\mathbb{F}_p)| = p + 1 - (\pi + \overline{\pi}).$$

De plus, $\mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}) = \mathcal{O}$, *et toute courbe elliptique sur* $\mathbb{F}_p$ *dont l'anneau d'endomorphisme (sur* $\overline{\mathbb{F}_p}$*) est égal à* $\mathcal{O}$ *peut être relevée de cette manière.*

Démonstration: Lang [Lan87, Chapitre 13, Théorème 12 et Théorème 14]. □

3.4.5 Nombre de courbes elliptiques isogènes sur un corps fini

Soit E' une courbe elliptique définie sur $\mathbb{F}_q$. On dit que E' est dans la classe d'endomorphismes de E si E et E' sont isogènes mais non isomorphes et ont le même anneau d'endomorphismes $\mathcal{O}$. Cette classe d'équivalence est notée $\mathcal{C}(E)$.

Théorème 3.4.6 *Soit* E *une courbe elliptique ordinaire définie sur un corps fini et soit* $\mathcal{O}$ *l'anneau d'endomorphismes de* E.

Il existe alors une bijection entre $C(\mathcal{O})$ *et la classe d'endomorphismes* $\mathcal{C}(E)$ *de* E.

Démonstration: À l'aide des théorèmes de Deuring 3.4.5, on va travailler sur des courbes elliptiques définies sur $\mathbb{C}$ qui ont $\mathcal{O}$ comme anneau d'endomorphismes. Une courbe elliptique définie sur $\mathbb{C}$ est déterminée par le réseau par lequel on la définit. Grâce au théorème (2.3.1), on sait qu'il y a une bijection entre la classe d'homothéties de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$ et le groupe de classes d'idéaux $C(\mathcal{O})$. Or, dans $\mathbb{C}$, deux courbes sont isomorphes si et seulement si elles ont le même j-invariant, donc si et seulement si les deux réseaux sur lesquelles elles sont respectivement définies sont homothétiques. Par conséquent, les classes d'endomorphismes de E sont en bijection avec les classes d'homothéties de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$. Par suite, il existe bien une bijection entre $C(\mathcal{O})$ et les classes d'endomorphismes de E. □

Définition 3.4.2 *Soit* d *un entier positif ou nul. Le nombre de classes de Hurwitz* $\mathrm{H}(-d)$ *est défini comme suit.*

1. *Si* $d \equiv 1$ ou $2 \mod 4$ *alors* $\mathrm{H}(-d) = 0$ *;*
2. *Si* $d = 0$ *alors* $\mathrm{H}(0) = -1/12$ *;*
3. *Sinon (i.e. si* $d \equiv 0$ ou $3 \mod 4$ *et* $d > 0$*) on définit* $\mathrm{H}(-d)$ *comme étant le nombre de classes des formes quadratiques définies positives pas nécessairement primitives de discriminant* $-d$*, sauf les formes équivalentes à* $a(x^2+y^2)$ *qui seront comptées avec un coefficient* $1/2$ *et celles équivalentes à* $a(x^2+xy+y^2)$ *avec un coefficient* $1/3$.

Donc si on regarde l'ensemble des courbes elliptiques sur $\mathbb{K}$ isogènes à E il y en a au moins $\mathrm{H}(-g^2D)$ où g est le conducteur de l'ordre $\mathbb{Z}[\pi]$ (π est le morphisme de Frobenius).

Théorème 3.4.7 *Soit* $p > 3$ *un entier premier et soit* $N = p+1-t$ *un entier tel que* $-2\sqrt{p} \leqslant t \leqslant 2\sqrt{p}$*. Alors le nombre de courbes elliptiques ordinaires non-isomorphes sur* $\mathbb{F}_p$ *tel que* $|E(\mathbb{F}_p)| = N = p+1-t$ *est :*

$$H(t^2 - 4p)$$

Démonstration: [Sch87] $\square$

Deuxième partie

Courbes elliptiques sur les corps finis

Chapitre 4

Algorithmique des courbes elliptiques

Après avoir introduit la théorie sur les courbes elliptiques en général et en particulier celle concernant les courbes définies sur un corps fini $\mathbb{F}_q$, nous allons nous interesser aux aspects calculatoires des courbes elliptiques. Ce chapitre ne se veut pas exhaustif, nous allons nous attarder sur l'algorithmique qui va nous servir par la suite, à savoir la construction d'isogénies et le calcul de cardinalité d'une courbe sur $\mathbb{F}_q$.

4.1 Isogénies

Les isogénies jouent un rôle prédominant dans l'algorithmique des courbes elliptiques sur un corps fini. En effet, ces objets vont nous permettre par exemple d'obtenir facilement des sous-groupes de la ℓ-torsion (4.2) ou bien encore de déplacer des problèmes cryptographiques d'une courbe vers une autre ([Gal99]).

4.1.1 Formules de Vélu

Dans cette section, on va décrire comment à partir d'un sous-groupe fini F d'une courbe elliptique E on peut construire la courbe isogène E/F et l'isogénie $f : E \to E/F$. Ces résultats sont fondés sur l'article de Vélu [Vél71].

Soit E une courbe elliptique sur un corps $\mathbb{K}$ qui a pour équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Soit F un sous-groupe fini de E. On note F_2 l'ensemble des points d'ordre 2 de $F - O_E$, par R une partie de $F - \{O_E\} - F_2$ telle que

$$F - \{O_E\} - F_2 = R \cup (-R) \text{ et } R \cap (-R) = \varnothing;$$

enfin, on notera S l'union de F_2 et R. L'isogénie $f : E \to E/F$ admet les équations

$$\begin{cases} X = x + \sum_{Q\in S} \left[\frac{t_Q}{x-x_Q} + \frac{u_Q}{(x-x_Q)^2}\right] \\ Y = y + \sum_{Q\in S} \left[u_Q \frac{2y+a_1x+a_3}{(x-x_Q)^3} + t_Q \frac{a_1(x-x_Q)+y-y_Q}{(x-x_Q)^2} + \frac{a_1u_Q - g_Q^x g_Q^y}{(x-x_Q)^2}\right] \end{cases} \tag{4.1}$$

avec les notations :

$$\begin{cases} Q = (x_Q, y_Q), \\ g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q, \\ g_Q^y = -2y_Q - a_1x_Q - a_3, \\ t_Q = \begin{cases} g_Q^x & \text{si } Q \in F_2, \\ 2g_Q^x - a_1g_Q^y = 6x_Q^2 + b_2x_Q + b_4 & \text{si } Q \notin F_2, \end{cases} \\ u_Q = (g_Q^y)^2 = 4x_Q^3 2 + b_2x_Q^2 + 2b_4x_Q + b_6 \end{cases} \tag{4.2}$$

où les b_i sont définis comme en 3.1.On pose aussi

$$t = \sum_{Q \in S} t_Q, w = \sum_{Q \in S} (u_Q + x_Qt_Q).$$

On obtient l'équation de Weierstrass suivante pour la courbe elliptique E/F :

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

avec

$$A_1 = a_1, A_2 = a_2, A_3 = a_3, A_4 = a_4 - 5t, A_6 = a_6 - b_2t - 7w.$$

Les travaux de Dewaghe [Dew95] et de Lercier et Morain [LM98] réécrivent ces formules dans le cas d'isogénies de degré ℓ premier impair sous une forme plus pratique. Nous allons rappeler ici ces résultats. Le but est de réécrire les formules précédentes en fonction du polynôme

$$H(X) = \prod_{Q \in S} (X - x_Q) = X^d - h_1X^{d-1} + h_2X^{d-2} + \cdots + (-1)^dh_d.$$

Il nous faut tout d'abord évaluer :

$$S_1 = \sum_{Q \in R} x_Q,\ S_2 = \sum_{Q \in R} x_Q^2,\ S_3 = \sum_{Q \in R} x_Q^3,$$

$$\Sigma_1 = \sum_{Q \in R} \frac{1}{X - x_Q},\ \Sigma_2 = \sum_{Q \in R} \frac{1}{(X - x_Q)^2},\ \Sigma_3 = \sum_{Q \in R} \frac{1}{(X - x_Q)^3}.$$

Lemme 4.1.1 *On a alors :*

$$S_1 = h_1,\ S_2 = h_1^2 - 2h_2,\ S_3 = h_1^3 - 3h_1h_2 + 3h_3;$$

$$\Sigma_1 = \frac{H'}{H},\ \Sigma_2 = -\left(\frac{H'}{H}\right)'.$$

Si $\mathrm{Car}(\mathbb{K}) \neq 2$,

$$\Sigma_3 = \frac{1}{2}\left(\frac{H'}{H}\right)''$$

et si $\mathrm{Car}(\mathbb{K}) = 2$,

$$\Sigma_3 = \frac{1}{H^3}\left(H^2\frac{H^{(3)}}{2} + HH'\frac{H''}{2} + H'^3\right)$$

où les dérivées de H sont calculées dans $\mathbb{Q}$, divisées par 2 et ensuite réduite modulo 2.

En remplaçant ces coefficients dans les formules précédentes, on obtient alors la formulation de l'isogénie I.

Proposition 4.1.1 *L'isogénie I de degré ℓ qui associe au point (X, Y) le point (X^*, Y^*) peut être écrite sous la forme*

$$I(X,Y) = \left(\frac{G(X)}{H(X)^2}, \frac{J(X,Y)}{H(X)^3}\right),$$

où $G(X)$ est de degré ℓ, $H(X)$ est de degré $(\ell-1)/2$, et $J(X,Y)$ est un polynôme de degré 1 en Y.

4.1.2 Isogénies et équations modulaires

Les équations modulaires introduites en (2.2.2) ont une application directe dans le cadre des isogénies. En effet, on peut traduire le théorème 2.2.3 en termes de courbes elliptiques.

Théorème 4.1.1 *Soient E et E' deux courbes elliptiques définies sur un corps $\mathbb{K}$. Alors E et E' sont ℓ-isogènes sur $\bar{\mathbb{K}}$ si et seulement si $\Phi_\ell(j(E), j(E')) = 0$.*

Si l'on pose $\mathbb{K} = \mathbb{F}_q$ et que l'on se restreint aux courbes isogènes sur $\mathbb{F}_q$, ce théorème devient : E et E' sont ℓ-isogènes sur $\mathbb{F}_q$ seulement si $\Phi_\ell(j(E), j(E')) = 0$. En effet, dans $\mathbb{F}_q$ soient E et E' deux courbes ℓ-isogènes et soit E^t la tordue de E alors $\Phi_\ell(j(E^t), j(E')) = 0$, puisque une courbe elliptique et sa tordue ont le même j-invariant. Pourtant E^t et E' n'ont pas le même nombre de points sur $\mathbb{F}_q$ et donc ne sont pas isogènes sur $\mathbb{F}_q$.

D'après le corollaire 3.3.1, si ℓ est un nombre premier différent de p, alors la structure du groupe de ℓ-torsion est

$$E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z}).$$

Le groupe $E[\ell]$ est donc engendré par deux points P et Q et contient $\ell+1$ sous-groupes $C_0 =< P >$, $C_i =< P + iQ >$ pour tout $i \in [1..\ell-1]$ et $C_\ell =< Q >$. Ces sous-groupes ont les propriétés suivantes :
- $C_j \cap C_{j'} = \{O_E\}$ pour tous $j, j' \in [0..\ell]$ et $j \neq j'$;
- $\bigcup_{i\in[0..\ell]} C_i = E[\ell]$.

Chacun des C_i est le noyau d'une ℓ-isogénie. Le théorème suivant nous indique dans quel extension de $\mathbb{F}_q$ ces ℓ-isogénies sont rationnelles.

Théorème 4.1.2 *Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$ de j-invariant $j \neq 0, 1728$. Alors*

1. *le polynôme $\Phi_\ell(X, j)$ admet une racine $\tilde{j} \in \mathbb{F}_{q^r}$ si et seulement si le noyau C de l'isogénie correspondante*
$$\varphi : E \to E/C$$
est un espace propre de dimension 1 de π^r dans $E[\ell]$ (ici $\tilde{j} = j(E/C)$),
2. *le polynôme $\Phi_\ell(X, j)$ se décompose complètement dans $\mathbb{F}_{q^r}[X]$ si et seulement si π^r agit comme une matrice scalaire sur $E[\ell]$.*

La proposition suivante va spécifier la valeur de r.

Proposition 4.1.2 *Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ de j-invariant $j \neq 0, 1728$. Soit $\Phi_\ell(X, j) = h_1 h_2 \ldots h_s$ la décomposition de $\Phi_\ell(X, j) \in \mathbb{F}_q[X]$ en polynômes irréductibles. Alors les degrés de h_1, h_2, …, h_s satisfont l'une des propositions suivantes :*

(i). soit 1 et ℓ (dans ce cas on pose $r = \ell$) soit 1,1, …, 1 (dans ce cas on pose $r = \ell$), dans chacune de ces situations ℓ divise le discriminant du Frobenius, i.e. $t^2 - 4q \equiv 0 \bmod \ell$;

(ii). 1, 1, r, r, …, r, dans ce cas, $t^2 - 4q$ *est un carré modulo* ℓ, r *divise* $\ell - 1$ *et* π *agit sur* $E[\ell]$ *comme une matrice*

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

où $\alpha,\ \beta \in \mathbb{F}_\ell^*$ *;*

(iii). $r, r, \ldots, r$ *pour un entier* $r > 1$, *dans ce cas* $t^2 - 4q$ *n'est pas un carré modulo* ℓ, r *divise* $\ell + 1$ *et* π *agit sur* $E[\ell]$ *comme une matrice* $(2,2)$ *dont le polynôme caractéristique (égal à* $X^2 - tX + q$*) est irréductible sur* $\mathbb{F}_\ell$.

Dans tous les cas, r est le plus petit entier tel que

$$\exists \lambda \in \mathbb{N},\ \forall P \in E[\ell],\ \pi^r(P) = \lambda P.$$

Les démonstrations de ce théorème et de cette proposition sont données dans [Ler97a, Sch95]. Ces deux résultats sont la base des améliorations de l'algorithme de Schoof de calcul de la cardinalité d'une courbe proposées par Atkin et Elkies et décrites en 4.2.2.

4.1.3 Calcul de courbes ℓ-isogènes à E.

Pour calculer les courbes reliées à E via une ℓ-isogénie, on doit résoudre l'équation $\Phi_\ell(X, j(E)) = 0$, ce qui donne leurs invariants potentiels. Supposons que j^* est l'une de ces racines. La courbe E^* que l'on recherche est connue à sa tordue près et nous devons trouver son équation. Des formules pour calculer l'équation de E^* sont données dans [Sch95]. On suppose que E a pour équation $Y^2 = X^3 + AX + B$ (resp. $E^* : Y^2 = X^3 + A^*X + B^*$) et invariant j (resp. j^*) et on écrit $\Phi_X = \partial\Phi_\ell/\partial X$ (resp. $\Phi_Y = \partial\Phi_\ell/\partial Y$). Il faut supposer que ni j ni j^* n'appartiennent à $\{0, 1728\}$.

Théorème 4.1.3 *Supposons que* Φ_X *et* Φ_Y *soient non-nuls. On définit*

$$\kappa = -\frac{18}{\ell}\,\frac{B}{A}\,\frac{\Phi_X(j, j^*)}{\Phi_Y(j, j^*)}\,j.$$

Alors

$$A^* = \frac{3j^*}{1728 - j^*}\left(\frac{\kappa}{12j^*}\right)^2 \ell^4, \quad B^* = \frac{2j^*}{1728 - j^*}\left(\frac{\kappa}{12j^*}\right)^3 \ell^6.$$

Il nous reste encore les cas où j ou j^* sont dans $\{0, 1728\}$ ou $\Phi_X = \Phi_Y = 0$ pour lesquels le théorème précédent ne peut être appliqué.

Lorsque $\Phi_X = \Phi_Y = 0$, on peut calculer $G(Y) = \gcd(\Phi_X(j, Y), \Phi_Y(j, Y))$ et calculer Φ_X/Φ_Y comme étant égal à

$$(\Phi_X(j, Y)/G(Y))/(\Phi_Y(j, Y)/G(Y))$$

évalué au point $Y = j^*$.

Dans le cas de la caractéristique 2 et de la caractéristique 3, on obtient des formules bien plus simples. En effet dans le cas de la caractéritique 2, l'équation canonique de la courbe E à j-invariant non-nul est $y^2 + xy = x^3 + a_2x + a_6$. Comme deux courbes ayant une équation de ce type sont isomorphes si elles ont le même coefficient a_6 et des coefficients a_2 de même trace, on en déduit de j^* l'équation de la courbe isogène à E :

$$E^* : y^2 + xy = x^3 + a_2x + 1/j^*.$$

Pour la caractéristique 3, on obtient des résultats similaires. Dans ce cas, l'équation canonique de la courbe E à j-invariant non-nul est $y^2 = x^3 + a_2x^2 + a_6$. Alors l'équation de la courbe isogène à E de j-invariant j^* est :

$$E^* : y^2 = x^3 + a_2x^2 - a_2^3/j^*.$$

4.1.4 Calcul d'isogénie en grande caractéristique

On se propose ici d'exposer un algorithme pour calculer les isogénies en grande caractéristique proposé par Elkies [Elk91, Elk98] et décrit et développé dans [CCR91, Sch95, Mor95].

Soit $E : Y^2 = X^3 + a_4X + a_6$ une courbe elliptique définie sur $\mathbb{F}_q$. On considère son relèvement $\mathcal{E}_a$ dans $\mathbb{C}$ et on pose $\mathcal{E} : Y^2 = X^3 + A_4X + A_6$. Elle est alors isomorphe au quotient de $\mathbb{C}$ par un réseau $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Lorsque $\mathcal{E}$ admet une isogénie $\mathcal{I}$ de degré ℓ, on obtient en utilisant le théorème 4.1.3 l'équation de la courbe isogène $\tilde{\mathcal{E}} : Y^2 = X^3 + \tilde{A}_4X + \tilde{A}_6$ isomorphe au quotient de $\mathbb{C}$ par le réseau $\frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}$. En terme de réseau, on peut exprimer $\mathcal{I}$ comme :

$$\begin{aligned} \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) &\to \mathbb{C}/(\frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}) \\ z &\mapsto z. \end{aligned}$$

Nous notons $\wp(z)$ et $\tilde{\wp}(z)$ les fonctions de Weierstrass respectivement associées à $\mathcal{E}$ et $\tilde{\mathcal{E}}$. Considérons

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k} \text{ et } \tilde{\wp}(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} \tilde{c}_k z^{2k}$$

les développements de Laurent à l'infini de $\wp(z)$ et $\tilde{\wp}(z)$. On a alors :

$$c_1 = -\frac{A_4}{5},\ c_2 = -\frac{A_6}{7}, c_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j} \text{ pour } k \geqslant 3$$

et

$$\tilde{c}_1 = -\frac{\tilde{A}_4}{5},\ \tilde{c}_2 = -\frac{\tilde{A}_6}{7}, \tilde{c}_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} \tilde{c}_j \tilde{c}_{k-1-j} \text{ pour } k \geqslant 3.$$

On peut déjà exprimer $\tilde{\wp}(z)$ en fonction de $\wp(z)$.

Théorème 4.1.4 *Soient $\wp(z)$ et $\tilde{\wp}(z)$ deux fonctions de Weierstrass associées respectivement aux réseaux $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ et $\frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}$. Alors*

$$\forall z \in \mathbb{C},\ \tilde{\wp}(z) = \sum_{i=0}^{\ell-1} \wp\left(z + i\frac{\omega_1}{\ell}\right) - \sum_{i=0}^{\ell-1} \wp\left(i\frac{\omega_1}{\ell}\right).$$

Notons $I(X) = G(X)/H^2(X)$ l'image par $\mathcal{I}$ d'un point (X, Y) de $\mathcal{E}$. On a

$$\tilde{\wp}(z) = I(\wp(z)).$$

D'après les formules de Vélu, il suffit de calculer $H(X)$ égal ici à

$$H(X) = \prod_{i=1}^{(\ell-1)/2} \left(X - \wp\left(i\frac{\omega_1}{\ell}\right)\right).$$

On cherche donc à calculer

$$p_k = \sum_{i=1}^{(\ell-1)/2} \wp^k\left(i\frac{\omega_1}{\ell}\right),\ k \in \mathbb{N}.$$

Pour cela, on utilise la relation

$$\forall k \in \mathbb{N}^*,\ \forall z \in \mathbb{C},\ \frac{d^{2k}\wp}{dz^{2k}}(z) = (2k+2)!\wp^{k+1} + \dots.$$

En substituant $\frac{\omega_1}{\ell}, \dots, \frac{(\ell-1)\omega_1}{\ell}$ à z dans cette équation et en sommant ces nouvelles relations, on obtient

$$\forall k \in \mathbb{N}^*, \sum_{i=1}^{\ell-1} \frac{d^{2k}\wp}{dz^{2k}}\left(i\frac{\omega_1}{\ell}\right) = 2((2k+2)!p_{k+1} + \cdots).$$

D'après le théorème 4.1.4, on démontre que

$$\sum_{i=1}^{\ell-1} \frac{d^{2k}\wp}{dz^{2k}}\left(i\frac{\omega_1}{\ell}\right) = (2k)!(\tilde{c}_k - c_k)$$

et donc

$$(2k)!(\tilde{c}_k - c_k) = 2((2k+2)!p_{k+1} + \cdots).$$

En particulier,

$$\begin{aligned} A_4 - \tilde{A}_4 &= 5(6p_2 + 2A_4p_0) \\ A_6 - \tilde{A}_6 &= 7(10p_3 + 6a_4p_1 + 4a_6p_0). \end{aligned}$$

On peut ainsi calculer de proche en proche les p_i.

4.1.5 Autres méthodes de construction d'isogénies

Afin de pouvoir appliquer la méthode de Vélu, il faut être en possession du sous-groupe F de E qui va être le noyau de notre isogénie. Couveignes et Lercier ont proposé trois autres méthodes pour calculer les isogénies sans connaître ce sous-groupe, en ne connaissant que le j-invariant de la courbe isogène à E. On ne décrira pas ces méthodes qui sont complexes et que nous n'utiliserons pas par la suite. Le lecteur trouvera ces algorithmes décrits dans [Cou94, Ler97a, Cou96, LM98, BSS99].

4.2 L'algorithme SEA

Schoof [Sch85] propose en 1985 le premier algorithme polynomial déterministe qui permet de calculer la cardinalité d'une courbe elliptique E sur un corps fini $\mathbb{F}_q$. Cet algorithme comme nous le verrons juste après est très limité par la croissance rapide du degré des polynômes de division. Elkies et Atkin se sont attachés à lui trouver des améliorations en ne se servant plus que d'un facteur du polynôme de division pour les calculs. Ces améliorations ont donné naissance à l'algorithme SEA.

4.2.1 L'algorithme de Schoof

Dans cette section nous n'allons décrire cet algorithme que de manière succinte. Pour des explications plus détaillées, voir [Ler97b, Elk98, BSS99].

On pose E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Comme on l'a déjà vu dans 3.4.1, l'endomorphisme de Frobenius π admet pour équation caractéristique :

$$\pi^2 - t\pi + q = 0 \tag{4.3}$$

où t est la trace de π. D'après la proposition 3.4.1, le nombre de point de E est égal à $q+1-t$. Ainsi déterminer la cardinalité d'une courbe elliptique revient à déterminer la trace de l'endomorphisme de Frobenius.

L'idée principale de cet algorithme est de considérer l'équation caractéristique 4.3 de l'endomorphisme de Frobenius sur le module de Tate. Si on note $\bar{\pi}$ la restriction de π à l'ensemble $E[\ell^n]$ des points de ℓ^n-torsion sur la courbe E, on peut alors réécrire l'équation caractéristique du Frobenius avec $\bar{\pi}$:

$$\bar{\pi}^2 - [t \bmod \ell^n]\bar{\pi} + [q \bmod \ell^n] = 0. \tag{4.4}$$

Dans $E[\ell]$, on va chercher $0 \leqslant \tau < \ell$ tel que $[\tau]\bar{\pi} \equiv \bar{\pi}^2 + [q \bmod \ell]$.

D'après la proposition 3.4.2, $|t| \leqslant 2\sqrt{q}$; il suffit donc de calculer la valeur de t modulo ℓ_i avec $\prod_i \ell_i > 4\sqrt{q}$ et en se servant du théorème du reste chinois on en déduit la valeur de t.

Afin de calculer la valeur de t modulo ℓ premier, on utilise les polynômes de division de E. On rappelle (voir 3.2.0.0) qu'il existe un polynôme $f_m(x)$ tel que soit $P = (X_P, Y_P)$ un point de E, si $m \geqslant 2$ et $[2]P \neq O_E$ alors $[m]P = 0_E$ ssi $f_m(X_P) = 0$.

En se servant du ℓ-ième polynôme de division on va réécrire l'équation 4.4.

Sur $E[\ell]$, $\bar{\pi}(X,Y) = (X^q, Y^q)$. Donc on a :

$$[\tau](X^q, Y^q) = (X^{q^2}, Y^{q^2}) + [q \bmod \ell](X,Y)$$
$$[\tau](X^q, Y^q) \bmod (f_\ell(X), F_E(X,Y)) = ((X^{q^2}, Y^{q^2}) + [q \bmod \ell](X,Y)) \bmod (f_\ell(X), F_E(X,Y))$$

Ainsi on en déduit un $\tau \bmod \ell$ unique qui satisfait cette relation. Alors $t \equiv \tau \bmod \ell$.

On peut faire exactement la même chose pour ℓ^n. On a :

$$([\tau_n](X^q, Y^q)) \bmod (f_{\ell^n}(X), F_E(X,Y)) = ((X^{q^2}, Y^{q^2}) + [q \bmod \ell^n]) \bmod (f_{\ell^n}(X), F_E(X,Y)).$$

Or on a $\tau_n \equiv \tau_1 \bmod \ell$ et $\tau_n \equiv \tau_{n-1} \bmod \ell^{n-1}$ donc $\tau_n = \tau_{n-1} + k\ell^{n-1}$ avec $0 \leqslant k < \ell$. Ainsi pour déterminer τ_n quand on connait déjà τ_{n-1}, il suffit de déterminer k. Pour cela on travaille dans $E[\ell^n]/E[\ell^{n-1}]$ donc modulo $f_{\ell^n}/f_{\ell^{n-1}}$.

La limite de cet algorithme réside dans la taille des polynômes de division. En effet, le polynôme de division $f_\ell(X)$ est de degré $\frac{\ell^2-1}{2}$.

4.2.2 Les améliorations d'Elkies et Atkin

L'idée qu'a proposé Elkies est de travailler non plus modulo le polynôme de division $f_\ell(X)$ mais modulo un facteur du polynôme de division de degré $\frac{\ell-1}{2}$ quand c'est possible.

Comme introduit au paragraphe 4.1.2, $E[\ell]$ a $\ell+1$ sous-groupes. Alors les isogénies qu'ils induisent nous donnent les diagrammes suivants d'après le théorème 3.3.4 :

$$\begin{tikzcd} E \arrow[rr, "{[\ell]}"] \arrow[dr, "\mathcal{I}_j"'] & & E \\ & E/C_j \arrow[ur, "\hat{\mathcal{I}}_j"'] & \end{tikzcd}$$

et donc

$$\mathrm{Ker}(\mathcal{I}_j) \subset \mathrm{Ker}([\ell]) \text{ avec } \#\mathrm{Ker}(\mathcal{I}_j) = \ell.$$

Déterminer ces isogénies va donc nous donner un facteur du polynôme de division $f_\ell(X)$.

Ces isogénies sont définies sur une certaine extension de $\mathbb{F}_q$ de degré r déterminé par le théorème 4.1.2. D'après le théorème 4.1.2, le degré r est aussi la puissance de π telle que π^r agit comme une matrice scalaire sur $E[\ell]$. On distingue deux cas différents selon la valeur de r. Si

$r = 1$ on dit alors que ℓ est un *nombre premier d'Elkies*, si $r > 1$ alors ℓ est un *nombre premier d'Atkin*.

D'après le théorème 4.1.2, si l'une de ces isogénies est définie sur $\mathbb{F}_q$, le discriminant de l'équation caractéristique (4.4) de $\bar{\pi}$ est un carré non nul dans $\mathbb{F}_\ell$ alors il existe deux sous-espaces vectoriels propres différents et donc deux valeurs propres différentes α et β qui agissent sur $E[\ell]$. Par conséquent, il existe P et Q dans $E[\ell]$ tel que tout élément de $E[\ell]$ est de la forme $rP+sQ$. P et Q satisfont alors $\pi(< P >) =< P >$ et $\pi(< Q >) =< Q >$, i.e. le sous-groupe engendré par le point P est stable sous l'action du Frobenius (il en est de même pour Q). De plus, $\pi(P) = [\alpha]P$ et $\pi(Q) = [\beta]Q$. Ce qu'Elkies propose de trouver est l'une de ces deux valeurs propres. Pour cela, on détermine à l'aide de l'équation modulaire $\Phi_\ell(X, j(E)) = 0$ une courbe elliptique E_1 ℓ-isogène à E ainsi que son isogénie $\mathcal{I}_1$ ce qui nous donne le facteur $h_\ell(X)$ du polynôme de division $f_\ell(X)$. Il ne reste plus qu'à calculer la valeur propre λ correspondante et pour cela on cherche une égalité parmi les $\ell - 1$ équations

$$(x^q, y^q) = [\lambda](x, y) \text{ où } (x, y) \in \mathbb{F}_q[X, Y]/(h_\ell(X), F_E(X, Y)).$$

Alors $t \equiv \lambda + q/\lambda \bmod \ell$.

Si par contre, il faut considérer une extension de degré r supérieur à 1 pour obtenir une solution à l'équation modulaire $\Phi_\ell(X, j) = 0$, on utilise alors une méthode de Dewaghe [Dew98]. On se place dans le corps $\mathbb{F}_{q^r}$, on calcule la courbe E_1 isogène à E dans $\mathbb{F}_{q^r}$ ainsi que son isogénie $\mathcal{I}_1$ et donc le polynôme $h_1(X)$. À partir de $h_1(X)$, on détermine un point de ℓ-torsion de E définie sur $\mathbb{F}_{q^r}$. Après il ne nous reste plus qu'à énumérer les entiers λ de $\mathbb{F}_\ell$ jusqu'à obtenir une solution à l'equation

$$\pi^2(P) + [q \bmod \ell](P) = [\lambda](\pi(P)).$$

Alors $t \equiv \lambda \bmod \ell$.

Chapitre 5

L'algorithme de Kohel

Dans sa thèse [Koh96], Kohel propose des algorithmes pour calculer l'anneau d'endomorphismes d'une courbe elliptique définie sur un corps fini. Dans cette partie, on ne va s'occuper que du cas où la courbe est ordinaire, c'est à dire du cas des courbes dont l'anneau d'endomorphismes est un ordre dans un corps quadratique imaginaire. Ce chapitre va présenter les trois algorithmes proposés par Kohel dans le cas ordinaire. Cette présentation va être assez succinte pour deux des méthodes et détaillée pour la dernière qui va être la base de la construction ce que nous appellerons les volcans d'isogénies.

Tout au long de ce chapitre, on supposera que E est une courbe elliptique ordinaire définie sur un corps fini $\mathbb{F}_q$ et on supposera aussi que l'on connait le nombre de points de cette courbe et donc la trace t de l'endomorphisme de Frobenius.

5.1 Préliminaires

La donnée de la cardinalité de E nous donne aussi le corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ dans lequel va se trouver l'anneau d'endomorphisme $\mathcal{O} = \mathrm{End}(E)$. De plus, on obtient aussi l'ordre $\mathbb{Z}[\pi]$ engendré par l'endomorphisme de Frobenius π et l'anneau des entiers $\mathcal{O}_K$ de K. En effet, le discriminant de $\mathbb{Z}[\pi]$ est déterminé par la formule $d_\pi = t^2 - 4q$. Or comme décrit en 1.1, on peut écrire $d_\pi = g^2 d_K$ où g est le conducteur de l'ordre $\mathbb{Z}[\pi]$ et d_K le discriminant du corps K et de $\mathcal{O}_K$. Ainsi on connaît l'espace dans lequel va se trouver l'anneau d'endomorphismes $\mathcal{O}$ de E. On a la relation suivante :

$$\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K. \tag{5.1}$$

Le premier problème se pose ici. Pour connaître $\mathbb{Z}[\pi]$ et $\mathcal{O}_K$, il faut pouvoir factoriser d_π. On suppose dans la suite de ce chapitre que d_π est factorisé.

D'après 1.1, on sait que si f est le conducteur de $\mathcal{O}$ alors $f \mid g$, i.e. si $g = \prod_{i=1}^{k} \ell_i^{s_i}$ où $\{\ell_i\}_{1 \leqslant i \leqslant k}$ un ensemble de nombres premiers deux à deux différents et pour tout $1 \leqslant i \leqslant k$, $s_i \geqslant 1 \in \mathbb{N}$ alors il existe un n-uplet $(r_i)_{1 \leqslant i \leqslant k}$ tel que $f = \prod_{i=1}^{k} \ell_i^{r_i}$ et pour tout $1 \leqslant i \leqslant k$, $0 \leqslant r_i \leqslant s_i$. Dans le cas où $g = 1$, alors les inclusions de 5.1 sont toutes en fait des égalités et donc on connaît déjà $\mathcal{O}$. On supposera donc que $g > 1$. L'idée de base est de déterminer pour tout $1 \leqslant i \leqslant k$ la valeur de r_i. Comme cela se fait indépendamment pour chaque i, on va considérer que l'on travaille sur le facteur ℓ de f, on notera r son exposant dans f et s son exposant dans g.

La donnée de g nous permet soit de chercher directement le conducteur f soit le facteur $h = g/f$ de g. Pour rechercher la valeur de h, il faut exprimer $\mathcal{O}_K$ en fonction de π.

Lemme 5.1.1 *Soient K un corps quadratique imaginaire et $\mathcal{O}_K$ son anneau d'entiers. Soient $\mathbb{Z}[\pi]$ un ordre de K, g son conducteur, t la trace de π et q sa norme. Alors il existe un entier a tel que*

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - a}{g}\right],$$

l'entier a satisfait alors l'équation $(X-a)^2 \equiv X^2 - tX + q \mod g$.

Démonstration: $[1, g\omega]$ et $[1, \pi]$ sont deux bases de $\mathbb{Z}[\pi]$. Si l'on exprime π dans la base $[1, g\omega]$, on trouve $\pi = a + g\omega$ où $a \in \mathbb{Z}$. Par suite, $\omega = \frac{\pi-a}{g}$, donc $\mathcal{O}_K = \mathbb{Z}[\frac{\pi-a}{g}]$. De plus, $\frac{\pi-a}{g} \in \mathcal{O}_K$ donc les coefficients du polynôme minimal de $\frac{\pi-a}{g}$ sont des entiers rationnels ; en particulier, sa trace et sa norme :

$$Tr\left(\frac{\pi - a}{g}\right) = \frac{t-2a}{g} \text{ et } N\left(\frac{\pi - a}{g}\right) = \frac{q - ta + a^2}{g^2}$$

On a donc : $2a \equiv t \mod g$ et $q - ta + a^2 \equiv 0 \mod g^2$. Donc a satisfait l'équation $(X-a)^2 \equiv X^2 - tX + q \mod g$. □

Or $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ donc d'après le lemme précédent, $\mathcal{O} = \mathbb{Z} + f\frac{\pi-a}{g}\mathbb{Z}$. Si l'on reprend la notation introduite précédemment, on trouve que $\mathcal{O} = \mathbb{Z} + \frac{\pi-a}{\prod_{i=1}^{k}\ell^{s_i - r_i}}\mathbb{Z}$. Donc on peut déterminer chacune des puissances $s_i - r_i$ indépendamment.

Pour calculer chacune de ces puissances, Kohel nous donne trois méthodes différentes. Avant de les présenter, nous allons tout d'abord donner l'algorithme général du calcul de l'anneau d'endomorphismes d'une courbe elliptique ordinaire.

Procédure CalculAnneauEndomorphismes
Entrée : Le j-invariant j_E d'une courbe elliptique E et $g = \prod_{i \in I} \ell_i^{s_i}$ le conducteur de $\mathbb{Z}[\pi]$ factorisé en facteurs ℓ_i premiers.
Sortie : f le conducteur de $\mathcal{O} = \mathrm{End}(E)$.

1. POUR tout $i \in I$, trouver r_i avec l'une des trois méthodes ;
2. RETURN $f = \prod_{i \in I} \ell_i^{r_i}$.

5.2 Méthode par les polynômes de division

Soit $F_E(x, y) = 0$ l'équation de Weierstrass définissant E. On notera g le conducteur de $\mathbb{Z}[\pi]$ et soit a un entier tel que $\pi - a \equiv 0 \mod g\mathcal{O}_K$. Comme E est ordinaire, la trace du Frobenius est première à q, donc g est relativement premier à q. En effet, on a $t^2 - 4q = g^2 d_K$, donc si g n'est pas premier à q, alors t ne peut être premier à q. π détermine alors un automorphisme linéaire

$$\pi : \mathcal{O}_K / g\mathcal{O}_K \to \mathcal{O}_K / g\mathcal{O}_K,$$

et l'entier a est la valeur propre double de π modulo g. L'objectif est de trouver le plus grand facteur e de g pour lequel $\pi - a$ est l'application nulle dans $\mathcal{O}/e\mathcal{O}$. En effet, on peut écrire $\mathcal{O}$ sous la forme $\mathbb{Z}[f\frac{\pi-a}{g}]$ i.e. $\mathbb{Z}[\frac{\pi-a}{h}]$. Par suite pour tout facteur e de h, $\frac{\pi-a}{e}$ est un élément de $\mathcal{O}$ alors que si e est un multiple de h alors $\frac{\pi-a}{e}$ n'est pas dans $\mathcal{O}$. La manière la plus directe pour savoir si un diviseur e de g divise $\pi - a$ dans $\mathcal{O}$ est de comparer les homomorphismes induits par π et a dans l'anneau

$$\frac{\mathbb{F}_q[x, y]}{(F_E(x, y), \psi_h(x, y))},$$

où $\psi_h(x,y)$ est le polynôme de division d'indice h. L'endomorphisme $\pi - a$ est égal à $h\alpha$ où $\alpha \in \mathrm{End}(E)$ si et seulement si le noyau de $\pi - a$ contient $E[h]$. On note π_1 et $[a]_1$ la projection des applications π et $[a]$ sur la première coordonnée. Soit $\psi_h(x)$ le générateur de $(\psi_h(x,y)) \cap \mathbb{F}_q[x]$. D'après 3.2.0.0,

$$[a]_1(x) = \frac{\phi_a(x)}{\psi_a(x,y)^2} \text{ et } \pi_1(x) = x^q,$$

alors l'équation $x^q\psi_a(x,y)^2 - \phi_a(x) \mod \psi_h(x)$ est égale à 0 si et seulement si h divise $\pi - a$ dans $\mathcal{O}$. En prenant $h = \ell, \ell^2, \ldots$ jusqu'à la plus grande puissance de ℓ divisant $[\mathcal{O}_K : \mathbb{Z}[\pi]]$, on trouve l'exposant de ℓ dans l'indice $[\mathcal{O} : \mathbb{Z}[\pi]]$.

Complexité : On peut calculer le noyau de $\pi - a$ sur $E[h]$ en temps $\mathrm{O}(h^2 \log h \log q)$.

5.3 Méthode par les équations modulaires

Cette méthode exploite la relation entre deux courbes ℓ-isogènes et leur anneau d'endomorphismes. Le lemme suivant nous donne cette relation.

Lemme 5.3.1 *Soit $\Phi : E \to E'$ une isogénie de degré ℓ. Alors soit $[\mathrm{End}(E) : \mathrm{End}(E')] = \ell$, soit $[\mathrm{End}(E') : \mathrm{End}(E)] = \ell$ soit $\mathrm{End}(E') = \mathrm{End}(E)$.*

Démonstration: Kohel [Koh96, Proposition 21]. □

On dira d'une ℓ-isogénie $\Phi : E \to E'$ qu'elle est :

- *montante* (symbolisé par $\uparrow$) si $[\mathrm{End}(E') : \mathrm{End}(E)] = \ell$;
- *horizontale* (symbolisé par $\rightarrow$) si $\mathrm{End}(E') = \mathrm{End}(E)$;
- *descendante* (symbolisé par $\downarrow$) si $[\mathrm{End}(E) : \mathrm{End}(E')] = \ell$.

Théorème 5.3.1 *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ et soit ℓ un nombre premier différent de la caractéristique du corps $\mathbb{F}_q$.*

- *Si $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ alors E admet $1 + \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies horizontales.*
- *Si $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ alors E admet une ℓ-isogénie montante.*
- *Si $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ alors E n'admet pas de ℓ-isogénie descendante.*
- *Si $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ alors E admet $\ell - \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies descendantes.*
- *Si $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ alors E admet ℓ ℓ-isogénies descendantes.*

Démonstration: On trouve dans la thèse de Kohel [Koh96, Proposition 23] une démonstration algébrique de ce théorème. On donne ici une démonstration qui se sert du relèvement de la courbe sur $\mathbb{C}$. On peut retrouver le même type de démonstration dans [Gal99].

En se servant du théorème de Deuring (3.4.5) sur les relèvements, on considère le relèvement canonique $\mathcal{E}$ de E sur $\mathbb{C}$. Alors $\mathrm{End}(\mathcal{E}) = \mathrm{End}(E) = \mathcal{O}$ et donc $\mathcal{E} \simeq \mathbb{C}/\mathfrak{a}$ où $\mathfrak{a}$ est un idéal propre fractionnaire de $\mathcal{O}$. Pour simplifier la suite, on considère que $\mathfrak{a} = \mathcal{O}$.

Soit $\mathcal{O} = < 1, f\omega_K >$. Si on pose $\omega_f = f\omega_K$ alors le polynôme minimal de ω_f est :

$$x^2 - fd_Kx + f^2d_K\frac{d_K - 1}{4} = 0. \tag{5.2}$$

Le discriminant de ce polynôme et donc de l'ordre $\mathcal{O}$ est $D = f^2d_K$ comme on s'y attendait.

Dans $\mathbb{C}$, il y a $\ell + 1$ courbes ℓ-isogènes à $\mathcal{E}$: pour tout $i \in [0, \ldots, \ell - 1]$, on définit $\mathcal{E}_i$ comme étant la courbe elliptique isomorphe à $\mathbb{C}/ < 1, \frac{\omega_f + i}{\ell} >$ et on définit $\mathcal{E}_\ell$ comme étant la courbe elliptique isomorphe à $\mathbb{C}/ < 1, \ell\omega_f >$.

On considère tout d'abord le cas de la courbe $\mathcal{E}_\ell$. On pose $\tau = \ell\omega_f$, son polynôme minimal est donc :

$$x^2 - \ell f d_K x + \ell^2 f^2 d_K \frac{d_K - 1}{4} = 0. \tag{5.3}$$

Le discriminant de ce polynôme est $D_\ell = \ell^2 D$. On en déduit que $\mathrm{End}(\mathcal{E}_\ell) \subset \mathrm{End}(\mathcal{E})$ et que $[\mathrm{End}(\mathcal{E}) : \mathrm{End}(\mathcal{E}_\ell)] = \ell$.

On regarde maintenant la courbe elliptique $\mathcal{E}_i$ où $i \in [0, \ldots, \ell - 1]$. On pose $\tau_i = \frac{\omega_f + i}{\ell}$. Alors τ_i satisfait l'équation :

$$\ell^2 x^2 - \ell(f d_K + 2i)x + \left(i^2 + f d_K i + f^2 d_K \frac{d_K - 1}{4}\right) = 0. \tag{5.4}$$

Pour déterminer le discriminant de l'ordre $\mathrm{End}(\mathcal{E}_i)$ il faut que les coefficients de l'équation 5.4 soient premiers entre eux. On pose $a_i = (f d_K + 2i)$ et $b_i = i^2 + f d_K i + f^2 d_K \frac{d_K - 1}{4}$.

Si $b_i \not\equiv 0 \mod \ell$ alors les coefficients de l'équation 5.4 sont premiers entre eux et donc le discriminant D_i de $\mathrm{End}(\mathcal{E}_i)$ est égal à $\ell^2 D$ et $\mathrm{End}(\mathcal{E}_i) \subset \mathrm{End}(\mathcal{E})$ et $[\mathrm{End}(\mathcal{E}) : \mathrm{End}(\mathcal{E}_i)] = \ell$.

On suppose que $b_i \equiv 0 \mod \ell$. Deux cas se présentent :

1. $a_i \not\equiv 0 \mod \ell$ ou $b_i \not\equiv 0 \mod \ell^2$ ce qui implique que ℓ, a_i et b_i/ℓ sont premiers entre eux. Le discriminant D_i de $\mathrm{End}(\mathcal{E}_i)$ est égal à D et donc $\mathrm{End}(\mathcal{E}_i) = \mathrm{End}(\mathcal{E})$.
2. $a_i \equiv 0 \mod \ell$ et $b_i \equiv 0 \mod \ell^2$. Le discriminant D_i de $\mathrm{End}(\mathcal{E}_i)$ est égal à D/ℓ^2 et donc $\mathrm{End}(\mathcal{E}) \subset \mathrm{End}(\mathcal{E}_i)$ et $[\mathrm{End}(\mathcal{E}_i) : \mathrm{End}(\mathcal{E})] = \ell$.

On remarque que le cas 2 implique que $\ell | f$.

Il nous reste à déterminer pour quels $i \in [0, \ldots, \ell - 1]$, ces cas vont arriver. Le discriminant de $i^2 + f d_K i + f^2 d_K \frac{d_K - 1}{4} = 0$ est égal à D.

- Si ℓ est inerte dans $\mathcal{O}$ alors il n'existe pas de $i \in [0, \ldots, \ell - 1]$ tels que $b_i \equiv 0 \mod \ell$;
- Si ℓ se ramifie dans $\mathcal{O}$ alors il existe un unique $i_0 \in [0, \ldots, \ell - 1]$ tel que $b_{i_0} \equiv 0 \mod \ell$;
- Si ℓ se scinde dans $\mathcal{O}$ alors il existe i_1 et $i_2 \in [0, \ldots, \ell - 1]$ tels que $b_{i_1} \equiv b_{i_2} \equiv 0 \mod \ell$;

Si ℓ se ramifie dans $\mathcal{O}$ alors ℓ divise soit f, soit d_K, soit les deux. La solution est alors $i_0 = 0$. Si $\ell \nmid f$, on se retrouve dans le cas 1 ; sinon on est dans le cas 2.

Si ℓ se scinde alors $\ell \nmid f$ et $\ell \nmid d_K$; on se retrouve donc obligatoirement dans le cas 1.

En résumé, si $\ell | f$, on a une ℓ-isogénie montante et ℓ ℓ-isogénies descendantes.

Si par contre $\ell \nmid f$, on a $1 + \frac{d_K}{\ell}$ ℓ-isogénies horizontales et $\ell - \frac{d_K}{\ell}$ ℓ-isogénies descendantes.

Le fait d'avoir supposé que $\mathcal{E} \simeq \mathbb{C}/\mathcal{O}$ ne change rien au résultat final. Le fait d'avoir $\mathcal{E} \simeq \mathbb{C}/\mathfrak{a}$ où $\mathfrak{a} \neq \mathcal{O}$ entraîne juste des valeurs différentes de $i \in [0, \ldots, \ell]$ pour les ℓ-isogénies descendantes, montantes ou horizontales.

La dernière étape de cette démonstration consiste en la réduction de ces courbes sur $\mathbb{F}_q$. Il faut faire attention lors de cette réduction aux ℓ-isogénies qui ne sont pas rationnelles sur $\mathbb{F}_q$, c'est à dire aux courbes $\mathcal{E}_i$ telles que $\mathrm{End}(\mathcal{E}_i) \subset \mathbb{Z}[\pi]$. Donc en particulier si $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, il ne peut y avoir de ℓ-isogénies descendantes. □

De ce théorème on tire un algorithme pour calculer la valuation ell-adique du conducteur de $\mathrm{End}(E)$. L'idée principale de cet algorithme consiste en la construction d'une suite de courbes isogènes dont l'anneau d'endomorphismes va toujours être inclus dans celui de la précédente. Cette suite s'arrête lorsque l'on trouve une courbe E' telle que $\ell \nmid [\mathrm{End}(E') : \mathbb{Z}[\pi]]$. La taille de cette suite est alors la valuation ℓ-adique de g/f. Une démonstration de cet algorithme est donnée en 6.2.6.0.

Procédure CALCULFACTEURDUCONDUCTEUR
Entrée : Le j-invariant j_E d'une courbe elliptique E tel que $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ et la valuation

ℓ-adique n de g le conducteur de $\mathbb{Z}[\pi]$.
Sortie : La valuationℓ-adique m de g/f où f le conducteur de $\mathcal{O} = \mathrm{End}(E)$.

1. $R \leftarrow$ Racines de $\Phi_\ell(X, j_E)$;
2. SI $\#R = 1$ ALORS RETURN 0 ;
3. $m \leftarrow 1$;
4. $stop = faux$;
5. POUR $i := 1$ À 2 FAIRE
   (a) $G[i] \leftarrow j_E$;
   (b) $G'[i] \leftarrow R[i]$;
   (c) SI $G'[i] = 0$ OU $G'[i] = 1728$ ALORS $S[i] \leftarrow \emptyset$ SINON $S[i] \leftarrow$ Racines de $\Phi_\ell(X, G'[i])$;
6. TANT QUE $m \leqslant n$ ET $stop = faux$ FAIRE POUR $i := 1$ À 2 FAIRE
   (à ce stade, $G'[i]$ est le j-invariant de l'une des courbes ℓ-isogènes à celle qui correspond au j-invariant $G[i]$ et $S[i]$ contient une liste de j-invariants correspondants à ceux des courbes ℓ-isogènes à celle qui correspond à $G'[i]$)
   – SI $S[i] = \emptyset$ ALORS utiliser le i suivant ;
   – SI $\#S[i] = 1$ ALORS $\{stop = vrai\,;\}$
   – SINON
     (a) $m \leftarrow m + 1$
     (b) SI $(S[i][1] = G[i])$ ALORS {(on ne veut pas revenir sur la courbe précédente) $G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][2]$;} ;
     SINON $\{G[i] \leftarrow G'[i]\,;\ G'[i] \leftarrow S[i][1]\,;\}$;
     (c) SI $G'[i] = 0$ OU $G'[i] = 1728$ ALORS $S[i] \leftarrow \emptyset$ SINON $S[i] \leftarrow$ Racines de $\Phi_\ell(X, G'[i])$;
7. SI $m > n$ ALORS $m \leftarrow n$;
8. RETURN m.

Complexité : La complexité de l'algorithme CALCULFACTEURDUCONDUCTEUR est $O(n\mathcal{F}(\ell))$ où n est la valuation ℓ-adique du conducteur de $\mathbb{Z}[\pi]$ et $\mathcal{F}(\ell)$ est le temps nécessaire pour trouver trois racines du polynôme modulaire.

5.4 Méthode par les idéaux

Soit E une courbe elliptique ordinaire définie sur un corps fini $\mathbb{K}$ et $\mathcal{O}$ son anneau d'endomorphismes. Soit E' une courbe elliptique définie sur $\mathbb{K}$. On dit que E' est dans la classe d'endomorphismes de E si E et E' sont isogènes mais non isomorphes et ont le même anneau d'endomorphismes $\mathcal{O}$. Cette nouvelle classe d'équivalence, que l'on notera $\mathcal{C}(E)$, va nous permettre de déterminer si le conducteur de notre ordre a même valuation ℓ-adique que le conducteur de $\mathbb{Z}[\pi]$ dans le cas où le conducteur a un grand diviseur premier. En effet, on a une bijection entre $\mathcal{C}(E)$ et $C(\mathcal{O})$.

Théorème 5.4.1 *Soit E une courbe elliptique ordinaire définie sur un corps fini et soit $\mathcal{O}$ l'anneau d'endomorphismes de E. Il existe alors une bijection entre $C(\mathcal{O})$ et la classe d'endomorphismes $\mathcal{C}(E)$ de E.*

Démonstration: À l'aide des théorèmes de Deuring, on va travailler sur des courbes elliptiques définies sur $\mathbb{C}$ qui ont $\mathcal{O}$ comme anneau d'endomorphismes. Une courbe elliptique définie sur $\mathbb{C}$ est déterminée par le réseau par lequel on la définit. Grâce au théorème 2.3.1, on sait qu'il y a une bijection entre la classe d'homothéties de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$ et le groupe de classe d'idéaux $C(\mathcal{O})$. Or, dans $\mathbb{C}$, deux courbes sont isomorphes si et seulement si elles ont le même j-invariant, donc si et seulement si les deux réseaux sur lesquelles elles sont respectivement définies sont homothétiques. Par conséquent, les classes d'endomorphismes de E sont en bijection avec les classes d'homothéties de réseaux Λ tels que $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$. Par suite, il existe bien une bijection entre $C(\mathcal{O})$ et les classes d'endomorphismes de E. □

Ce théorème suggère deux approches à notre problème. La première est d'énumérer l'ensemble des $h(\mathcal{O})$ courbes elliptiques dans la classe d'endomorphismes de E, ce qui implique le choix d'un ensemble de petits générateurs premiers du groupe de classes d'idéaux et de s'en servir pour construire des isogénies dans la classe d'endomorphismes de E. La seconde approche consiste en le calcul d'idéaux principaux de norme lisse dans un possible anneau d'endomorphismes $\mathcal{O}$, et ensuite en la détermination de l'isogénie correspondante pour voir si l'image de la courbe E est isomorphe à E.

Première approche : L'énumération

Le problème d'une telle approche réside dans le fait que le nombre de classes de $\mathbb{Z}[\pi]$ et des ordres qui le contiennent peut être extrêmement grand. Quoiqu'il en soit, si ℓ un grand nombre premier divisant l'ordre de $\mathbb{Z}[\pi]$, on considère

$$\mathcal{O}_1 = \mathbb{Z}\left[\frac{\pi - a}{\ell}\right].$$

Si on a l'inclusion suivante : $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subset \mathcal{O}_1$, on a alors $h(\mathcal{O}_1) < h(\mathcal{O})$ et même $h(\mathcal{O}_1) \mid h(\mathcal{O})$. Donc si l'on peut énumérer plus de $h(\mathcal{O}_1)$ courbes dans la classe d'endomorphismes de E, alors on peut en conclure que le conducteur de $\mathrm{End}(E)$ a même valuation ℓ-adique que le conducteur de $\mathbb{Z}[\pi]$.

Une telle énumération suppose que l'on ait déterminé $h(\mathcal{O}_1)$ et que l'on ait des idéaux premiers petits décomposables dans $\mathcal{O}_1$ à partir desquels on peut construire des isogènies de degré petit.

Deuxième approche : Passage par le groupe de classes d'idéaux

La première méthode n'exploite à aucun moment les connaissances que nous avons sur le groupe de classes d'idéaux. Cette méthode va se servir des algorithmes sur les groupes de classes d'idéaux pour trouver des relations du groupe de classes d'idéaux sur des idéaux premiers petits décomposables $\mathfrak{r}_1, \ldots, \mathfrak{r}_c$ dans l'ordre $\mathcal{O}_1$. En se servant de l'algorithme de McCurley (1.3.2), on obtient un idéal principal $(\beta) = \mathfrak{r}_1^{s_1} \ldots \mathfrak{r}_c^{s_c} \subseteq \mathcal{O}_1$; on pose $u = s_1 + \cdots + s_c$. Soit $\mathfrak{b} = \beta\mathcal{O} \cap \mathcal{O}$. On construit la suite d'isogénies :

$$E_0 = E \to E_1 = E/E[\mathfrak{r}_1] \to E_2 = E/E[\mathfrak{r}_1^2] \to \cdots \to E_u = E/E[\mathfrak{b}],$$

chacune de degré petit. On obtient une courbe $E_u = E/E[\mathfrak{b}]$ qui est isomorphe à E si et seulement si $\mathfrak{b}$ est principal. Typiquement, on trouve β dans $\mathcal{O}_1$ contenant $\mathbb{Z}[\pi]$ avec un grand indice, et on s'attend à ce que $\mathfrak{b}$ soit non principal. Dans le cas où $\mathcal{O} \supseteq \mathcal{O}_1$, on a construit un nouvel endomorphisme $E \to E' \cong E$.

Dans la suite, on va récapituler la méthode de construction d'une isogénie dont l'idéal du noyau est $\mathfrak{r}$. On remarque que tout idéal premier $\mathfrak{r}$ de $\mathcal{O}$ qui ne divise pas le discriminant de $\mathbb{Z}[\pi]$ peut être écrit de la forme $(r, \pi - b)$ pour $r = N(\mathfrak{r})$ et $b \in \mathbb{Z}$. Soit $F_E(x,y)$ une équation de Weierstrass de E et soit $\psi_r(x,y)$, $\psi_b(x,y)$ et $\phi_b(x,y)$ les polynômes de division de E. Le noyau de l'isogénie $E \to E' = E/E[\mathfrak{r}]$ est déterminé par l'idéal

$$I = (\psi_r(x,y), x^q\psi_b(x,y)^2 - \phi_b(x)) \subseteq \frac{\mathbb{K}[x,y]}{(F_E(x,y))}.$$

En posant $\psi(x)$ le générateur de $I \cap \mathbb{K}[x]$, on construit l'isogénie en se servant des formules de Vélu (4.1.1).
Complexité : En supposant l'hypothèse généralisée de Riemann, on peut trouver l'élément β de $\mathcal{O}_1$ cherché en un temps $O(h(\mathcal{O}_1)\log|D_1|)$.

5.5 Conclusions

Après l'exposé des trois méthodes, il est clair que le deuxième algorithme est celui qui sera utilisé effectivement. En effet la taille des polynômes de divisions utilisés dans la première méthode est rapidement un frein à son utilisation. Dans le cas de la troisième méthode, il faut soit énumérer un certain nombre de courbes elliptiques ce qui va nécessiter le calcul d'un nombre de classes et des constructions d'isogénies de degré petit soit construire un anneau principal. En plus de calculer l'anneau d'endomorphismes, on voit la relation entre les courbes isogènes et leurs anneaux d'endomorphisme. Dans le chapitre suivant, on va s'attarder à construire une structure qui va permettre de classer les courbes selon leur anneau d'endomorphismes et les courbes qui leur sont isogènes.

Chapitre 6

Volcans d'isogénies

Le travail de Kohel sur le calcul de l'anneau d'endomorphismes d'une courbe elliptique ordinaire est fortement lié aux courbes isogènes à la courbe de départ. La méthode 5.3 de calcul nous permet aussi, une fois le calcul effectué, de déduire l'anneau d'endomorphismes d'une courbe isogène à notre courbe de départ. On peut donc construire un arbre de courbes elliptiques ℓ-isogènes qui va caractériser l'anneau d'endomorphismes de l'une en fonction de celui d'autres. Cette structure si elle est bien orientée donne naissance aux *volcans d'isogénies*. On va grâce à eux pouvoir décrire la classe d'endomorphismes de E. Il faut remarquer que Couveignes, Dewaghe et Morain dans [CDM96] avaient construit un arbre de ℓ-isogénies dans le cas où ℓ est un nombre premier divisant d_π mais n'avaient pas vu la structure sous-jacente à cet arbre.

6.1 Extension du théorème de Kohel

Le tableau 6.1 résumant le théorème de Kohel 6.1 nous donne la clé pour comprendre la relation entre les anneaux d'endomorphismes de courbes isogènes. On déduit tout d'abord la relation entre une isogénie α et sa duale notée $\hat{\alpha}$.

Lemme 6.1.1 *Soit $\alpha : E \to E'$ une ℓ-isogénie et $\hat{\alpha}$ sa duale. Alors*
- *α est une ℓ-isogénie montante si et seulement si $\hat{\alpha}$ est une ℓ-isogénie descendante ;*
- *α est une ℓ-isogénie horizontale si et seulement si $\hat{\alpha}$ est une ℓ-isogénie horizontale.*

Démonstration: Si α est une isogénie montante, then $[\mathcal{O}' : \mathcal{O}] = \ell$. Puisque $\hat{\alpha} : E' \to E$, alors, par définition, $\hat{\alpha}$ est une ℓ-isogénie descendante.

Si α est une ℓ-isogénie horizontale, alors $\mathcal{O} \simeq \mathcal{O}'$. De manière immédiate, $\hat{\alpha}$ est une ℓ-isogénie horizontale. □

Cas		Type	Nombre total
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D}{\ell}\right) \ \rightarrow$	$1 + \left(\frac{D}{\ell}\right)$
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \rightarrow \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell + 1$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 \ \uparrow$	1
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell + 1$

TAB. 6.1 – Nombre et type des ℓ-isogénies en fonction de $[\mathcal{O}_K : \mathcal{O}]$ et de $[\mathcal{O} : \mathbb{Z}[\pi]]$.

À partir de ces résultats, on peut déduire quelques propriétés des anneaux d'endomorphismes $\mathcal{O}$ et $\mathcal{O}'$ tels que $\alpha : E \to E'$ soit une ℓ-isogénie. On distingue deux cas pour les anneaux d'endomorphismes par rapport à ℓ : le cas où $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ ou pas.

Le lemme suivant nous assure que si $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ, la courbe E ne peut avoir que des ℓ-isogénies horizontales.

Lemme 6.1.2 *Soit E une courbe elliptique telle que $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ. S'il existe une ℓ-isogénie de E, alors cette ℓ-isogénie est une ℓ-isogénie horizontale.*

Démonstration: Puisque $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ et que $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$, $\mathcal{O}$ est maximal par rapport à ℓ, i.e. $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$. En se rapportant au tableau 6.1, on en déduit que si E admet une ℓ-isogénie alors elle est horizontale. $\square$

On suppose maintenant que $\mathbb{Z}[\pi]$ n'est pas maximal par rapport à ℓ. On donne deux lemmes sur les ℓ-isogénies de E pour distinguer les deux cas possibles pour les anneaux d'endomorphismes des courbes ℓ-isogènes à E. Ces deux situations différents sont résumées dans les graphes suivants. On notera $\mathcal{O}'$ l'anneau d'endomorphismes d'une courbe ℓ-isogène à E.

$$\begin{tikzcd} \mathcal{O}_K \arrow[d, dash, "\ell^r \| f"] \arrow[dd, dash, bend right=60, "\ell^{r'}=\ell^{r+1}\|f'"'] \\ \mathcal{O} \arrow[d, dash, "\ell"] \\ \mathcal{O}' \arrow[d, dash, "\ell^{n-(r+1)}\|g/f'"] \\ \mathbb{Z}[\pi] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{O}_K \arrow[d, dash, "\ell^{r'}=\ell^{r-1}\|f'"] \arrow[dd, dash, bend right=60, "\ell^{r}\|f"'] \\ \mathcal{O}' \arrow[d, dash, "\ell"] \\ \mathcal{O} \arrow[d, dash, "\ell^{n-r}\|g/f'"] \\ \mathbb{Z}[\pi] \end{tikzcd}$$

On étudie tout d'abord le cas où $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, ensuite nous considérerons un cas plus général.

Lemme 6.1.3 *Si $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, alors l'unique ℓ-isogénie $\alpha : E \to E'$ de E est telle que $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$, i.e. $v_\ell(f') = n - 1$ où $n \geqslant 1$ est tel que $v_\ell(g) = n$.*

Démonstration: En se reportant au tableau 6.1, l'unique ℓ-isogénie de E notée α est une ℓ-isogénie montante. Alors on sait que $[\mathcal{O}' : \mathcal{O}] = \ell$, i.e. $f/f' = \ell$. Mais l'hypothèse $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ nous dit que si n est tel que $v_\ell(g) = n$ alors $v_\ell(f) = n$. Par conséquent, $\ell \mid (g/f')$, donc $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$ et $f' = f/\ell$ donc $v_\ell(f') = n - 1$. $\square$

Lemme 6.1.4 *Si $\alpha : E_1 \to E_2$ est une ℓ-isogénie descendante et $\ell \mid [\mathcal{O}_2 : \mathbb{Z}[\pi]]$, alors pour toute ℓ-isogénie $\beta : E_2 \to E_3$ telle que $\mathcal{O}_3 \not\simeq \mathcal{O}_1$, β est une ℓ-isogénie descendante. De plus, il y a ℓ ℓ-isogénie de la sorte.*

Démonstration: Tout d'abord puisque α est une isogénie descendante, on a $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, i.e. $f_2/f_1 = \ell$, donc $\ell \mid [\mathcal{O}_K : \mathcal{O}_2]$. En se reportant au tableau 6.1, on voit que E_2 a une ℓ-isogénie montante et ℓ ℓ-isogénies descendantes.

Soit $\gamma : E_2 \to E_3$ la ℓ-isogénie montante. Puisque γ est une ℓ-isogénie montante, $[\mathcal{O}_3 : \mathcal{O}_2] = \ell$, i.e. $f_2/f_3 = \ell$. Mais on a vu que $f_2/f_1 = \ell$, donc $f_3 = f_1$. Par conséquent, $\mathcal{O}_3 \simeq \mathcal{O}_1$, ce qui contredit notre hypothèse.

Soit $\beta : E_2 \to E_3$ l'une des ℓ-isogénies descendantes. Puisque β est descendante, $[\mathcal{O}_2 : \mathcal{O}_3] = \ell$, i.e. $f_3/f_2 = \ell$. Mais on a vu que $f_2/f_1 = \ell$, donc $f_3 = \ell^2 f_1$ et $\mathcal{O}_3 \not\simeq \mathcal{O}_1$. Par conséquent, toute ℓ-isogénie satisfaisant les hypothèses du lemme est une ℓ-isogénie descendante et il y en a ℓ. $\square$

En d'autres mots, si $\beta \neq \hat{\alpha}$, alors β est une ℓ-isogénie descendante. En effet, puisque E_2 a $\ell + 1$ ℓ-isogénies et que $\hat{\alpha}$ est une ℓ-isogénie montante d'après le Lemme 6.1.1, toute ℓ-isogénie différente de $\hat{\alpha}$ est une ℓ-isogénie descendante.

On va décrire maintenant un cas très particulier.

Lemme 6.1.5 *S'il existe deux ℓ-isogénies différentes à isomorphismes près d'une courbe E vers une courbe E', alors ce sont toutes les deux des ℓ-isogénies horizontales. On peut aussi conclure que ℓ se scinde dans $\mathcal{O}$.*

Démonstration: Tout d'abord, on va montrer que si $\mathcal{O}$ n'est pas maximal par rapport à ℓ, on ne peut avoir de telles ℓ-isogénies. Si $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, c'est évident puique E n'admet qu'une seule ℓ-isogénie à isomorphismes près (cf. Tableau 6.1). Si $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$, alors ces deux ℓ-isogénies doivent être descendantes. Autrement, puisque E n'admet qu'une seule ℓ-isogénie montante (cf. Tableau 6.1), il faudrait que l'une d'elles soit montante et l'autre descendante, i.e. $[\mathcal{O}' : \mathcal{O}] = \ell$ et $[\mathcal{O} : \mathcal{O}'] = \ell$: ce qui est impossible. On suppose donc que ces deux ℓ-isogénies sont descendantes. Si on regarde $\mathcal{O}'$ on sait que $[\mathcal{O} : \mathcal{O}'] = \ell$, donc $\mathcal{O}'$ n'est pas maximal par rapport à ℓ. Par conséquent, E' admet exactement une ℓ-isogénie montante et selon si $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$ ou pas, ℓ ℓ-isogénies descendantes. Mais les duales de nos deux ℓ-isogénies sont montantes d'après le Lemme 6.1.1 et elles sont différentes à isomorphismes près, ce qui contredit le fait que E' n'admet qu'une seule ℓ-isogénie montante. Donc il est impossible que $\ell \mid [\mathcal{O}_K : \mathcal{O}]$.

On suppose maintenant que $\mathcal{O}$ est maximal par rapport à ℓ. En se reportant au Tableau 6.1, E admet $1 + \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies horizontales et $\ell - \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies descendantes puisque l'on a supposé que $\mathbb{Z}[\pi]$ n'est pas maximal par rapport à ℓ (on peut néanmoins prouver le même résultat dans le cas où $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ de manière assez évidente). On prouve de manière similaire à ce qui vient d'être fait pour $\mathcal{O}$ non maximal par rapport à ℓ que les deux ℓ-isogénies ne peuvent être ni toutes les deux descendantes, ni une horizontale et l'autre descendante. Par conséquent elles doivent être toutes les deux horizontales. De plus $\left(\frac{d_K}{\ell}\right) = 1$, c'est à dire ℓ se scinde dans $\mathcal{O}_K$ et comme $\mathcal{O}$ est maximal par rapport à ℓ, ℓ se scinde dans $\mathcal{O}$. □

Ce cas particulier nous donne des informations sur le corps quadratique imaginaire dans lequel se trouve l'anneau d'endomorphismes de la courbe.

Théorème 6.1.1 *[Sch95] On suppose qu'il existe deux ℓ-isogénies α et β différentes à isomorphismes près de E vers la même courbe E'. Alors le discriminant D de l'anneau d'endomorphismes de E est tel que $|D| \leqslant 4\ell^2$.*

Démonstration: L'isogénie $\hat{\alpha}\beta$ est un endomorphisme de E et est cyclique de degré ℓ^2 différente de ℓ fois un automorphisme. Par conséquent, il existe un entier algébrique de $\mathcal{O}$ de norme ℓ^2 ou de manière équivalente $4\ell^2 = x^2 + |D|y^2$ est résoluble avec des entiers x et y. On a donc bien le résultat voulu. □

Cet ensemble de lemmes nous donne une idée du graphe des ℓ-isogénies des courbes elliptiques ayant le même Frobenius. Il a la structure d'un volcan tronqué au niveau de $\mathbb{Z}[\pi]$. La formation du cratère provient des ℓ-isogénies horizontales que l'on peut trouver quand $\mathcal{O}$ est maximal par rapport à ℓ en se servant du tableau 6.1 et le reste de la structure du volcan provient du fait que par les lemmes 6.1.3 et 6.1.4, si $\mathcal{O}$ n'est pas maximal par rapport à ℓ alors E n'admet pas de ℓ-isogénies horizontales. Le cas où ℓ est inerte ou se scinde dans $\mathbb{Z}[\pi]$ nous donne un cas de volcan dégénéré, puisqu'on ne peut avoir que des ℓ-isogénies horizontales d'après le Lemme 6.1.2. Pour résumer ces idées, on donne la Figure 6.1 dans le cas général.

Le niveau d'une courbe elliptique dans le volcan est l'étage auquel se trouve cette courbe dans le volcan tout en sachant que le niveau 0 correspond à l'étage du cratère. La hauteur du volcan est égale au niveau d'une courbe au niveau de $\mathbb{Z}[\pi]$.

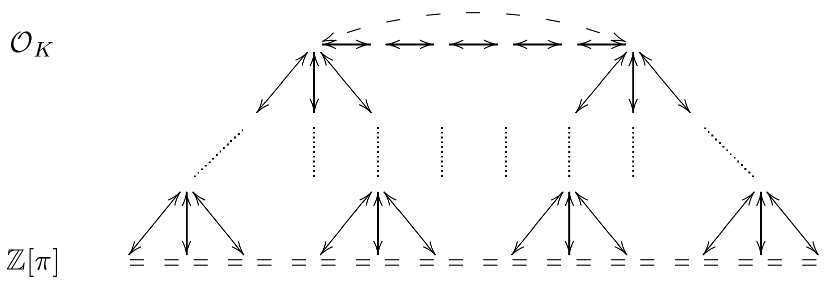


FIG. 6.1 – Volcan d'isogénies.

6.2 Construction du volcan

Dans la suite, on supposera que l'on a une procédure COURBESISOGÈNES(E, ℓ) qui nous donne la liste des courbes ℓ-isogènes à une courbe donnée E quand E n'est pas particulière. Cette procédure est dérivée du paragraphe 4.1.3.

Afin de se servir de l'algorithme 5.3 pour calculer l'anneau d'endomorphismes d'une courbe elliptique ordinaire, Kohel supposait qu'il connaissait la cardinalité de la courbe elliptique et savait la factoriser. On va maintenant essayer de construire le volcan des ℓ-isogénies sans connaitre la valeur du Frobenius. Il va donc falloir placer $\mathbb{Z}[\pi]$ par rapport à $\mathcal{O}_K$ c'est à dire trouver le "haut" et le "bas" du volcan.

6.2.1 Inversion du théorème de Kohel

Soit ℓ un nombre premier différent de la caractéristique p et soit $\mathcal{N}_\ell(E)$ le nombre de racines de $\Phi_\ell(X, j(E))$ dans $\mathbb{F}_q$. En fonction de $\mathcal{N}_\ell(E)$, on peut déterminer des propriétés de l'anneau d'endomorphismes $\mathcal{O}$ de E en se servant du Théorème 5.3.1. On résume ces propriétés dans le Tableau 6.2.

$\mathcal{N}_\ell(E)$	Type des ℓ-isogénies		$\left(\frac{D}{\ell}\right)$	$\left(\frac{d_\pi}{\ell}\right)$
0	aucune	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	-1	-1
2	$\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$+1$	$+1$
1	cas 1 : $\rightarrow$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	0	0
	cas 2 : $\uparrow$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \mid [\mathcal{O}_K : \mathcal{O}]$	0	0
$\ell + 1$	cas 1' : $\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \rightarrow \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	inconnu	0
	cas 2' : $\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \mid [\mathcal{O}_K : \mathcal{O}]$	0	0

TAB. 6.2 – Propriétés de $\mathcal{O}$ en fonction du nombre et du type des ℓ-isogénies de E.

À partir de ces propriétés on va construire le volcan des ℓ-isogénies. Nous donnons tout d'abord le squelette de l'algorithme et ensuite détaillons chacune de ses étapes.

6.2.2 But de l'algorithme

L'algorithme présenté ici a pour but non pas de dessiner l'intégralité du volcan mais de déterminer la forme du volcan, i.e. la hauteur du volcan ainsi que la forme du cratère, i.e. s'il est réduit à un point, à un 2-cycle ou encore si c'est un cycle de taille supérieure à 2. La hauteur du volcan sera donnée par une suite de courbes ℓ-isogènes dont la première se trouve dans le cratère et la dernière est à la base du volcan.

Une fois que l'on est muni de ces données, il est facile en se servant des algorithmes intermédiaires de se promener dans le volcan et donc de récupérer les données que l'on pourrait désirer sur le volcan.

6.2.3 Squelette de l'algorithme

L'algorithme est divisé en deux parties. En premier on détermine si $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ ou pas. Si tel n'est pas le cas, alors on recherche une courbe E_s qui va être dans le cratère du volcans de ℓ-isogénies (Figure 6.1) et ensuite on détermine la largeur du cratère, i.e. s'il est réduit à un point, à deux ou à plus selon si ℓ est inerte, se ramifie ou se scinde dans $\mathcal{O}_K$ et on situe la base du volcan par rapport à son cratère en utilisant ce que l'on appellera *un parcours descendant complet*. Puisque les courbes particulières nécessite un traitement particulier, on les signale par EXIT dans l'algorithme pour simplifier.

Procédure CALCULVOLCANPARTIEL
Entrée : Une courbe elliptique $\mathcal{E}$ et un nombre premier ℓ, $\ell \neq p$.
Sortie : Un parcours descendant complet dans le volcan et $\epsilon = \left(\frac{d_K}{\ell}\right)$.

1. SI $\mathcal{E}$ est particulière ALORS EXIT ;
2. $F \leftarrow$COURBESISOGÈNES$(\mathcal{E}, \ell)$;
3. SI $(\#F = 0)$ ALORS $\{\mathcal{F} = \{\mathcal{E}\}\,;\, \epsilon = -1\,;$ GOTO 5$\}$
   SINON
   SI $(\#F = 2)$ ALORS $\{\mathcal{F} = \{\mathcal{E}\}\,;\, \epsilon = +1\,;$ GOTO 5$\}$
   SINON
   SI $(\#F = 1)$ ALORS
   – $E' \leftarrow F[1]$;
   – SI E' est particulière ALORS EXIT ;
     SINON
     SI $\mathcal{N}_\ell(E') = 1$ ALORS $\{\mathcal{F} = \{\mathcal{E}\}\,;\, \epsilon = 0\,;$ GOTO 5$\}$
     SINON GOTO 4 ;
   SINON
   SI $(\#F = \ell + 1)$ ALORS GOTO 4 ;
4. $(E_s, \epsilon, n, \mathcal{F}) \leftarrow$CALCULPARCOURSDESCENDANTSCOMPLETS$(\mathcal{E}, \ell)$.
5. RETURN $\{\mathcal{F}; \epsilon\}$.

6.2.4 Courbes particulières : le cas $j \in \{0, 1728\}$.

Si notre courbe de départ $\mathcal{E}$ a 0 ou 1728 comme j-invariant, alors on ne sait construire aucune partie du volcan. En effet, on ne sait pas distinguer les courbes isogènes à $\mathcal{E}$ sur $\mathbb{F}_q$ à celles qui lui sont uniquement isogènes sur une clôture algébrique de $\mathbb{F}_q$. Par contre, si l'on rencontre une courbe avec un tel j-invariant au cours de la construction du volcan, on sait alors que cette courbe est dans le cratère et on peut en déduire un parcours descendant complet et aussi la valeur de ϵ. Par contre, nous ne savons pas construire le volcan dans son intégralité.

6.2.5 Les cas $\mathcal{N}_\ell(E) \neq \ell + 1$.

Ces cas sont traités en premier parce que l'on peut aisément en se servant du Lemme 6.1.2 voir si on se trouve dans le cas où $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ ou alors en utilisant le Lemme 6.1.3 revenir au cas général.

$\mathcal{N}_\ell(E) = 0$.

Dans ce cas, si on se rapporte au Tableau 6.2, on voit que E n'admet pas de ℓ-isogénie et que ℓ est inerte dans $\mathbb{Z}[\pi]$. On peut aussi en déduire que $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ. Par conséquent le volcan est réduit à un point unique : la courbe E.

$\mathcal{N}_\ell(E) = 2$.

En se reportant au Tableau 6.2, on voit que ℓ se scinde dans $\mathbb{Z}[\pi]$. Ce cas a déjà été traité par Couveignes, Dewaghe et Morain ([CM94], [CDM96]) qui construisent le cycle de ℓ-isogénies qui forment le cratère du volcan. En se servant du Lemme 6.1.2, on voit que toute ℓ-isogénie sera dans ce cas horizontale donc le volcan sera réduit à son cratère. En d'autres termes, $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ.

$\mathcal{N}_\ell(E) = 1$.

Dans ce cas, on voit que ℓ se ramifie dans $\mathbb{Z}[\pi]$. Dans le Tableau 6.2, on remarque que deux solutions sont possibles pour ce cas : soit $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ soit non. Il nous faut distinguer ces deux cas. Pour se faire il nous faut la courbe ℓ-isogène E' à E et $\mathcal{N}_\ell(E')$.

Cas 1 : $\mathcal{N}_\ell(E') = 1$. Supposons que $\mathbb{Z}[\pi]$ ne soit pas maximal par rapport à ℓ. En se reportant au Tableau 6.2, on en déduit que $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ et la ℓ-isogénie de E vers E' est une ℓ-isogénie montante. Par conséquent d'après le Lemme 6.1.3 on obtient $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$. Donc en se servant du Tableau 6.1, $\mathcal{N}_\ell(E') = \ell + 1$ ce qui contredit la valeur de $\mathcal{N}_\ell(E')$ que l'on a trouvé. Par conséquent, $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ. On peut aussi en déduire que le volcan se réduit à deux points : les courbes E et E'.

Cas 2 : $\mathcal{N}_\ell(E') = \ell + 1$. Supposons que $\mathbb{Z}[\pi]$ est maximal par rapport à ℓ, i.e. $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. En se reportant au Tableau 6.2, on sait que la ℓ-isogénie de E vers E' est une ℓ-isogénie horizontale et $(D/\ell) = 0$. Par conséquent $\mathcal{O}'$ a le même conducteur que $\mathcal{O}$, i.e. $\ell \nmid [\mathcal{O}' : \mathbb{Z}[\pi]]$, $\ell \nmid [\mathcal{O}_K : \mathcal{O}']$ et $(D'/\ell) = 0$. En se reportant au Tableau 6.1, on voit qu'alors $\mathcal{N}_\ell(E') = 1 + \left(\frac{D'}{\ell}\right) = 1$ ce qui contredit la valeur de $\mathcal{N}_\ell(E')$ que l'on a trouvé. Par conséquent, $\mathbb{Z}[\pi]$ n'est pas maximal par rapport à ℓ. On peut aussi en déduire que la courbe E se trouve à la base du volcan.

6.2.6 Le cas général $\mathcal{N}_\ell(E) = \ell + 1$.

Au vu du squelette de l'algorithme, ce cas est celui sur lequel on s'attarde le plus.

À partir de maintenant on suppose que la courbe E est au niveau r pour ℓ, $r \in \mathbb{N}$ et que $\mathcal{N}_\ell(E)$ est égal à $\ell+1$. En fait, on a l'egalité $\mathcal{N}_\ell(E_i) = \ell+1$ jusqu'à ce que l'on trouve la condition d'arrêt de notre récurrence que l'on reconnaît par $\mathcal{N}_\ell(E_i) = 1$.

Le but de l'algorithme est en particulier de trouver une courbe E_s qui sera dans le cratère du volcan. Pour cela on va se servir de *parcours descendants*. On va tout d'abord préciser cette notion.

Parcours descendants.

Définition 6.2.1 *Un* parcours descendant *d'une courbe elliptique E est un parcours $E = E_0 \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$ de courbes elliptiques tel que l'application $E_i \to E_{i+1}$ pour tout $i \in [0, \ldots, m[$ soit une ℓ-isogénie descendante et que $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$.*

On dira que l'on a un parcours descendant complet *si E est dans le cratère du volcan.*

La taille d'un parcours descendant est définie comme étant le nombre de courbes du parcours.

Lemme 6.2.1 *En se servant des notations de la définition 6.2.1, si E est au niveau r alors E_i est au niveau $r + i$.*

Démonstration: On prouve ce lemme par induction. $E_0 = E$ est au niveau r. On suppose que le résultat est vrai pour E_j où $0 \leqslant j < m$. On sait que l'application $E_j \to E_{j+1}$ est une ℓ-isogénie descendante. Par conséquent, puisque le niveau de E_j est $r + j$, i.e. $\ell^{r+j} \parallel [\mathcal{O}_K : \mathcal{O}_j]$ et par définition d'une ℓ-isogénie descendante alors $\ell^{r+j+1} \parallel [\mathcal{O}_K : \mathcal{O}_{j+1}]$. Donc E_{j+1} est au niveau $r + (j + 1)$. □

Le but principal à la recherche d'un parcours descendant à partir d'une courbe E est de localiser l'anneau d'endomorphisme de E dans la structure volcanique (cf. Figure 6.1) par rapport à son cratère et à sa base.

Lemme 6.2.2 *Soit $\mathcal{P}$ un parcours descendant partant de E et soit $m = \#\mathcal{P} - 1$. Alors E est au niveau $(n - m)$ où n est la hauteur du volcan.*

Démonstration: À partir de la définition, $\mathcal{P}$ est un parcours $E = E_0 \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$. Soit E une courbe au niveau r. Par conséquent d'après le Lemme 6.2.1, E_m est au niveau $r + m$. On sait aussi que $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$, i.e. que si la hauteur du volcan est n alors la courbe E_m est au niveau n. Par conséquent $n = r + m$ donc $r = n - m$. □

Maintenant que l'on a défini cette notion et son intérêt, on va montrer comment calculer un parcours descendant. On donne tout d'abord l'algorithme et ensuite on prouve sa validité.

Procédure CALCULPARCOURSDESCENDANT
Entrée : Une courbe elliptique non particulière E telle que $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
Sortie : Un parcours descendant partant de E.

1. $F \leftarrow$COURBESISOGÈNES(E, ℓ) ;
2. SI $\#F = 1$ ALORS $\{P[1] \leftarrow \{E\}$; $i_0 \leftarrow 1$; GOTO 6$\}$;
3. POUR $i := 1$ À 3 FAIRE
   (a) $P[i] \leftarrow \{E\} \cup \{F[i]\}$;
   (b) $G[i] \leftarrow E$;
   (c) $G'[i] \leftarrow F[i]$;
   (d) SI $G'[i]$ est particulière ALORS $S[i] \leftarrow \emptyset$ SINON $S[i] \leftarrow$COURBESISOGÈNES$(G'[i], \ell)$;
4. $i_0 \leftarrow -1$
5. TANT QUE $(i_0 = -1)$ FAIRE
   POUR $i := 1$ À 3 FAIRE
   (à ce stade, $G'[i]$ est l'une des courbes ℓ-isogènes de $G[i]$ et $S[i]$ contient une liste de courbes ℓ-isogènes à $G'[i]$)
   – SI $S[i] = \emptyset$ ALORS utiliser le i suivant ;
   – SI $\#S[i] = 1$ ALORS $\{i_0 \leftarrow i$; (on a trouvé la base du volcan)$\}$
   – SINON

(a) SI $(j(S[i][1]) = j(G[i]))$ ALORS {(on ne veut pas revenir sur la courbe précédente) $G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][2]$;} ;
SINON $\{G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][1]$;$\}$;
(b) $P[i] \leftarrow P[i] \cup \{G'[i]\}$;
(c) SI $G'[i]$ est particulière ALORS $S[i] \leftarrow \emptyset$ SINON $S[i] \leftarrow$COURBESISOGÈNES$(G'[i], \ell)$;

6. RETURN $P[i_0]$.

Le lemme 6.1.4 nous assure que dès que l'on trouve une ℓ-isogénie $\alpha : E \to E'$ telle que α soit une ℓ-isogénie descendante, toute ℓ-isogénie $\beta : E' \to E''$ telle que $E'' \not\simeq E$, i.e. $\beta \neq \hat{\alpha}$, est une ℓ-isogénie descendante. Par conséquent, de manière inductive, si l'on commence un parcours de courbes ℓ-isogénes par une ℓ-isogénie descendante, on obtient un parcours descendant.

Afin de trouver une telle ℓ-isogénie, on calcule parallèlement trois parcours de courbes ℓ-isogènes partant de trois courbes différentes ℓ-isogènes à E quelconques. Il nous en faut trois parce que si $\mathcal{O}$ est maximal par rapport à ℓ, on peut avoir deux ℓ-isogénies horizontales (voir le Tableau 6.1) et si par hasard nos parcours commencent par ces deux là, alors les parcours ne débuteront pas par une ℓ-isogénie descendante. Le troisième parcours nous assure le fait d'avoir un parcours qui commence par une ℓ-isogénie descendante et cela nous assure aussi d'avoir un parcours non-vide. Dans le cas où $\mathcal{O}$ n'est pas maximal par rapport à ℓ, il n'y a qu'une seule ℓ-isogénie montante (voir le Tableau 6.1), par conséquent au moins deux de nos parcours débuteront par une ℓ-isogénie descendante et cela nous assure d'avoir un parcours non-vide. Puisqu'un parcours non-descendant est composé d'un parcours de courbes ℓ-isogènes reliées par des ℓ-isogénies non-descendantes et d'un parcours descendant, un parcours non-descendant est plus long qu'un parcours descendant. C'est pourquoi, le premier parcours qui s'arrêtera sera un parcours descendant.

Lemme 6.2.3 *La complexité de l'algorithme* CALCULPARCOURSDESCENDANT *est* $O((n-r)\mathcal{F}(\ell))$, *où* n *est la hauteur du volcan,* r *le niveau de la courbe et* $\mathcal{F}(\ell)$ *le temps de trouver trois racines du polynôme modulaire.*

Démonstration: Pour calculer chacun des trois parcours, il faut $\#\mathcal{P} = m + 1$ factorisations partielles de l'équation modulaire. D'après le lemme 6.2.2 le niveau de la courbe est alors $n - m$. □

Pourquoi nous faut-il une courbe qui se trouve dans le cratère ?

Si l'on a une courbe E_s dans le cratère et un parcours descendant complet $E_s \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$, alors on peut situer le cratère et la base du volcan et on peut après se déplacer dans le volcan facilement. Pour trouver une telle courbe E_s, il nous faut savoir reconnaître le fait d'être dans le cratère.

Détecter le cratère et donc déterminer ϵ.

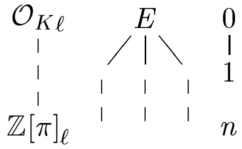
En se servant du tableau 6.2, on voit qu'il y a trois types différents de cratère qui vont chacun être détecté d'une manière différente. En fait, ces trois cas obéissent à la même équation en ce qui concerne les ℓ-isogénies de la courbe :

$$\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \ell\text{-isogénies horizontales,} \\ \ell - \left(\frac{D}{\ell}\right) & \ell\text{-isogénies descendantes.} \end{cases} \tag{6.1}$$

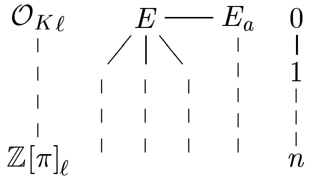
Pour simplifier les notations, on notera n la hauteur du volcan.

Supposons que la courbe E soit dans le cratère. Alors elle satisfera l'une des conditions suivantes.

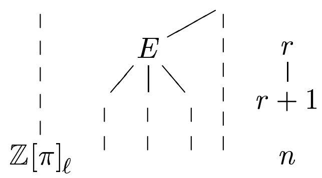
- Cas a : Il n'y a pas de ℓ-isogénie horizontale. En considérant le fait que nous sommes dans le cratère, on a $\ell+1$ ℓ-isogénies descendantes d'après (6.1). Alors tous les parcours descendants partant des $\ell+1$ courbes ℓ-isogènes de E sont de même taille. Le graphe suivant caractérise cette situation.

  La taille des parcours descendants est $(n-1)$ puisque toutes les courbes correspondant aux $\ell+1$ racines de $\Phi_\ell(X,j)$ sont au niveau 1. On peut aussi en déduire que ℓ est inerte dans $\mathcal{O}_K$ et donc $\epsilon=-1$.
- Cas b : Il y a exactement une ℓ-isogénie horizontale. Il y a donc aussi ℓ ℓ-isogénies descendantes d'après (6.1). Alors l'un des parcours descendants partant des $\ell+1$ courbes ℓ-isogènes à E est de taille n (disons que ce parcours descendant parte de la courbe E_a) et les ℓ autres sont de taille $(n-1)$. Le graphe suivant caractérise cette situation et fait le parallèle avec la situation "normale" i.e. que l'on retrouve au cœur du volcan.

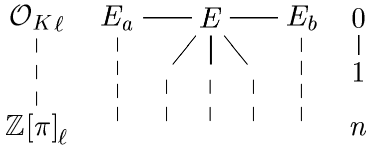
  

  Cas horizontal

  Cas "normal"

  On ne peut confondre ce cas avec le cas "normal" qui a une ℓ-isogénie ascendante et ℓ ℓ-isogénies descendantes, puisque dans le cas horizontal, la différence entre la taille du parcours descendant partant de E_a et la taille des autres parcours descendants est de 1 alors que dans le cas "normal" cette différence est de 2. Dans ce cas, on sait aussi que ℓ se ramifie dans $\mathcal{O}_K$ et donc $\epsilon=0$.
- Cas c : Il y a deux ℓ-isogénies horizontales. Il y a aussi $\ell-1$ ℓ-isogénies descendantes d'après (6.1). Alors deux des parcours descendants partant des $\ell+1$ courbes ℓ-isogènes sont de taille n (disons que ces parcours descendants partent des courbes E_a et E_b) et les $\ell-1$ autres sont de taille $(n-1)$. Le graphe suivant caractérise cette situation.

  La différence avec les cas précédents est que l'on trouve deux parcours descendants plus longs que les autres au lieu de n'en avoir qu'un. Donc aucune confusion avec le cas "normal" n'est possible. On sait aussi que ℓ se scinde dans $\mathcal{O}_K$ et donc $\epsilon=1$.

Comment trouver une courbe dans le cratère.

L'algorithme qui trouve une courbe dans le cratère du volcan est exactement l'inverse de celui qui recherche un parcours descendant. On cherche à construire maintenant un *parcours ascendant* partant de $\mathcal{E}$.

Définition 6.2.2 *Un* parcours ascendant *d'une courbe elliptique E est un parcours $E=E_0\to$*

$E_{-1} \to E_{-2} \to \cdots \to E_{-(s-1)} \to E_{-s}$ de courbes elliptiques tel que l'application $E_{-i} \to E_{-(i+1)}$, pour $i \in [0, \ldots, s-1[$, est une ℓ-isogénie ascendante et $\mathcal{O}_{-s}$ est maximal par rapport à ℓ.

On dira que nous avons un parcours ascendant complet *si* $\mathrm{End}(E)_\ell \simeq \mathbb{Z}[\pi]_\ell$.

Lemme 6.2.4 *En utilisant les mêmes notations que dans la définition 6.2.2, si E est au niveau r alors E_{-i} est au niveau $(r-i)$.*

Démonstration: La preuve est similaire à la preuve du lemme 6.2.1. □

Corollaire 6.2.1 *Si la taille du parcours ascendant partant de E est $r+1$, alors E est au niveau $r+1$.*

À chaque pas dans cet algorithme, on recherche une courbe à un niveau inférieur que celle que nous considérons. Dans ce cas, il nous faut considérer les $\ell+1$ ℓ-isogénies de E et déterminer laquelle est une ℓ-isogénie ascendante. Pour se faire, on va calculer un parcours descendant pour chacune des courbes ℓ-isogènes de E et le plus long parcours descendant sera celui qui débute par la courbe issue de la ℓ-isogénie ascendante. On réitère cette opération jusqu'à ce que l'on détecte une courbe dans le cratère.

Avant de donner l'algorithme qui recherche une courbe dans le cratère, il nous faut tout d'abord donner un algorithme qui détecte si la courbe que l'on considère n'est pas déjà dans le cratère et si tel n'est pas le cas, qui donne alors une courbe à un niveau inférieur.

Procédure DÉTECTIONCRATÈRE
Entrée : Une liste de parcours descendants $\mathfrak{P}$ et la courbe E_{cour}.
Sortie : $(\epsilon, i_{max}, \lambda, \mathcal{F})$ tel que

- $\epsilon = 0$, i_{max} tel que $\#\mathfrak{P}[i_{max}]$ est maximal et λ la taille de $\mathfrak{P}[i_{max}]$
- OU $\epsilon = (d_K/\ell)$, $i_{max} = -1$ et λ la hauteur du volcan si l'on détecte une courbe dans le cratère ;
- $\mathcal{F}$ est une liste de (quelques) parcours descendants.

1. $\epsilon \leftarrow 0$; $\mathcal{F} \leftarrow \emptyset$;
2. Trouver i_{max} tel que $\#\mathfrak{P}[i]$ est maximal ;
3. $I \leftarrow \{i \text{ t.q. } i \neq i_{max} \text{ et } \#\mathfrak{P}[i] = \#\mathfrak{P}[i_{max}]\}$;
4. /* Cas où l'on détecte le niveau du cratère et $\left(\frac{d_K}{\ell}\right) = -1$ (cas a) */
   SI $\#I = \ell$ ALORS $\{\epsilon \leftarrow -1$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}]$; $i_{max} \leftarrow -1$; $\mathcal{F} \leftarrow \{\{E_{cour}, \mathfrak{P}[1]\}\}$; $\}$
5. /* Cas où l'on détecte le niveau du cratère et $\left(\frac{d_K}{\ell}\right) = +1$ (cas c)*/
   SI $\#I = 1$ ALORS $\{$ $i_{max2} \leftarrow I[1]$; $\epsilon \leftarrow 1$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $i_0 \leftarrow$ un indice différent de i_{max} et i_{max2} ; $\mathcal{F} \leftarrow \{\{E_{cour}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}], \mathfrak{P}[i_{max2}]\}$; $i_{max} \leftarrow -1$; $\}$
6. SI $\#I = 0$ ALORS
   (a) SI $i_{max} = 1$ ALORS $i_0 \leftarrow 2$; SINON $i_0 \leftarrow 1$;
   (b) SI $\#\mathfrak{P}[i_{max}] - \#\mathfrak{P}[i_0] = 1$ /* Cas où l'on détecte le niveau du cratère et $\left(\frac{d_K}{\ell}\right) = 0$ (cas b) */
   ALORS $\{\epsilon \leftarrow 0$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $\mathcal{F} \leftarrow \{\{E_{cur}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}]\}$; $i_{max} \leftarrow -1$; $\}$
   SINON $\{\lambda \leftarrow \#\mathfrak{P}[i_{max}]$;$\}$
7. RETURN $(\epsilon, i_{max}, \lambda, \mathcal{F})$.

L'algorithme suivant calcule un parcours ascendant partant de E en utilisant l'algorithme précédent et retourne une courbe isogène à E qui se trouve dans le cratère.

Procédure CALCULPARCOURSDESCENDANTSCOMPLETS
Entrée : Une courbe elliptique non-particulière E telle que $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
Sortie : $(E_s, \epsilon, n, \mathcal{F})$ tel que E_s est dans le cratère, isogène à E, $\epsilon = (d_K/\ell)$, n la hauteur du volcan et $\mathcal{F}$ est une liste de (quelques) parcours descendants complets.

1. $E_{cour} \leftarrow E$;
2. $F \leftarrow$COURBESISOGÈNES(E_{cour}, ℓ) ;
3. $P \leftarrow \{E_{cour}\}$;
4. SI $\#F = 1$ ALORS $\{E_{cour} \leftarrow F[1]$; SI E_{cour} est particulière ALORS EXIT ; SINON $\{P \leftarrow P \cup \{F[1]\}$;$\}\}$
5. $i_0 \leftarrow 0$;
6. TANT QUE $i_0 \neq -1$ FAIRE
   (a) $F \leftarrow$COURBESISOGÈNES(E_{cour}, ℓ) ;
   (b) POUR $i := 1$ À $\ell + 1$ FAIRE
   SI $F[i]$ est particulière ALORS EXIT ;
   $\mathfrak{P}[i] \leftarrow$ CALCULPARCOURSDESCENDANT$(F[i])$;
   (c) $(\epsilon, i_0, \lambda, \mathcal{F}) \leftarrow$DÉTECTIONCRATÈRE$(\mathfrak{P})$;
   (d) SI $i_0 \neq -1$ ALORS $\{E_{cour} \leftarrow F[i_0]$; $P \leftarrow P \cup \{E_{cour}\}$;$\}$
7. $E_s \leftarrow E_{cour}$;
8. RETURN $(E_s, \epsilon, \lambda, \mathcal{F})$;

Lemme 6.2.5 *La complexité de l'algorithme* CALCULPARCOURSDESCENDANTSCOMPLETS *est* $O(n^2\ell\mathcal{F}(\ell))$, *où* $\mathcal{F}(\ell)$ *est le temps nécessaire pour calculer toutes les racines d'un polynôme modulaire et* n *est la hauteur du volcan.*

Démonstration: Pour passer du niveau μ au niveau $\mu - 1$, il nous faut calculer $\ell + 1$ parcours descendants. Cela nécessite $O(\mu\ell\mathcal{F}(\ell))$ opérations. Donc en tout cela nécessite $\Sigma_{\mu=1}^{n}\mu\mathcal{F}(\ell) = \frac{n(n+1)}{2}\mathcal{F}(\ell)$ opérations. Donc il faut $O(n^2\ell\mathcal{F}(\ell))$ opérations pour calculer un parcours ascendant. □

Le théorème suivant donne la complexité de l'algorithme qui calcule un volcan partiel.

Théorème 6.2.1 *Il faut* $O(n^2\ell\mathcal{F}(\ell))$ *opérations pour calculer un volcan partiel de* ℓ*-isogénies, où* $n \leqslant \log_\ell(|d_K|)$ *et* $\mathcal{F}(\ell)$ *est le temps nécessaire pour calculer toutes les racines d'un polynôme modulaire.*

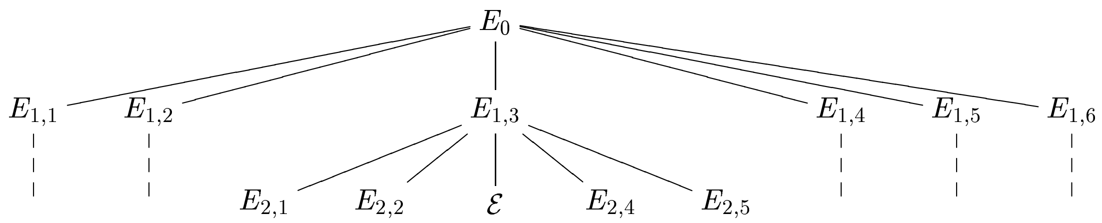
Démonstration: L'algorithme est fondé sur le calcul d'un parcours ascendant partant de $\mathcal{E}$. □

6.3 Exemples numériques

Dans ces exemples on donne l'ensemble des courbes parcourues lorsque l'on exécute l'algorithme CALCULVOLCANPARTIEL avec la courbe $\mathcal{E}$. Ces résultats ont été obtenus avec notre implantation de ces algorithmes en MAGMA.

Notation : On pose $E = [a, b]$ pour la courbe E d'équation $y^2 = x^3 + ax + b$.

Exemple 1 (Cas normal, ℓ est inerte dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = -1$) : Soient $p = 5081$ et $\mathcal{E} = [3290, 3887]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 1765$. Pour $\ell = 5$, on trouve :



où

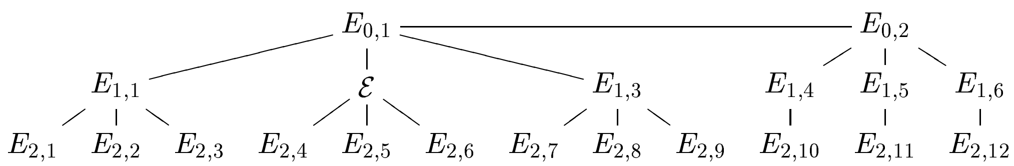
courbe	équation	courbe	équation	courbe	équation	courbe	équation
E_0	$[1355, 2505]$	$E_{1,3}$	$[3688, 3542]$	$E_{1,6}$	$[3211, 3432]$	$E_{2,4}$	$[1282, 1856]$
$E_{1,1}$	$[3623, 3418]$	$E_{1,4}$	$[2104, 4311]$	$E_{2,1}$	$[4192, 3469]$	$E_{2,5}$	$[2979, 436]$
$E_{1,2}$	$[2761, 2991]$	$E_{1,5}$	$[279, 3638]$	$E_{2,2}$	$[3332, 4679]$		

Dans ce cas, on obtient le parcours descendant complet suivant :

$$E_0 \to E_{1,3} \to \mathcal{E}$$

et on sait aussi que $\epsilon = -1$.

Exemple 2 (Cas normal, ℓ se ramifie dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = 0$) : Soient $p = 5059$ et $\mathcal{E} = [4646, 1411]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 1790$. Pour $\ell = 3$, on a :



où

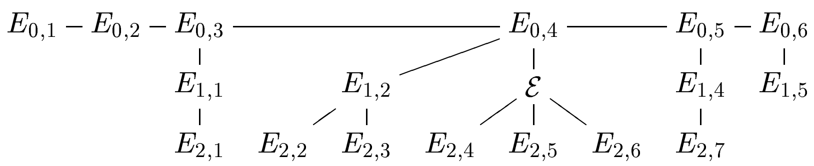
courbe	équation	courbe	équation	courbe	équation	courbe	équation
$E_{0,1}$	$[4307, 2079]$	$E_{1,5}$	$[1701, 548]$	$E_{2,4}$	$[4770, 1483]$	$E_{2,9}$	$[1724, 4275]$
$E_{0,2}$	$[2746, 1513]$	$E_{1,6}$	$[1105, 3273]$	$E_{2,5}$	$[3968, 2595]$	$E_{2,10}$	$[3571, 1957]$
$E_{1,1}$	$[2072, 3214]$	$E_{2,1}$	$[4021, 3717]$	$E_{2,6}$	$[2853, 4777]$	$E_{2,11}$	$[2543, 1941]$
$E_{1,3}$	$[880, 2818]$	$E_{2,2}$	$[3348, 2041]$	$E_{2,7}$	$[1273, 1362]$	$E_{2,12}$	$[2544, 3362]$
$E_{1,4}$	$[407, 2942]$	$E_{2,3}$	$[4995, 1623]$	$E_{2,8}$	$[301, 235]$		

Dans ce cas on obtient les deux parcours descendants complets suivants :

$$E_{0,1} \to \mathcal{E} \to E_{2,4} \quad \text{et} \quad E_{0,2} \to E_{1,4} \to E_{2,10}$$

et on en déduit $\epsilon = 0$.

Exemple 3 (Cas normal, ℓ se scinde dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = +1$) : Soient $p = 10009$ et $\mathcal{E} = [7478, 1649]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 83$. Avec $\ell = 3$, on trouve



où

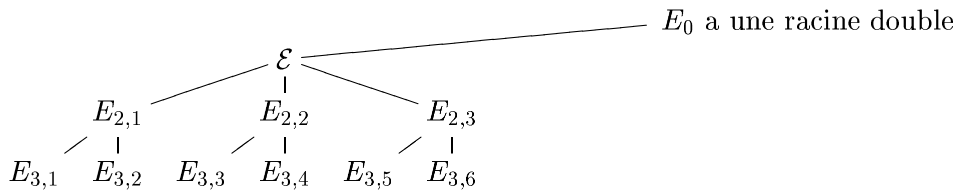
courbe	équation	courbe	équation	courbe	équation	courbe	équation
$E_{0,1}$	$[1336, 8702]$	$E_{0,6}$	$[352, 4401]$	$E_{2,1}$	$[5412, 9972]$	$E_{2,6}$	$[6203, 3741]$
$E_{0,2}$	$[56, 8167]$	$E_{1,1}$	$[9166, 9156]$	$E_{2,2}$	$[9899, 274]$	$E_{2,7}$	$[2728, 8215]$
$E_{0,3}$	$[7418, 8055]$	$E_{1,2}$	$[5138, 6736]$	$E_{2,3}$	$[6796, 2230]$		
$E_{0,4}$	$[7778, 9421]$	$E_{1,4}$	$[6435, 570]$	$E_{2,4}$	$[8899, 8303]$		
$E_{0,5}$	$[5051, 4157]$	$E_{1,5}$	$[3659, 6441]$	$E_{2,5}$	$[4732, 4541]$		

On obtient alors les trois parcours descendants complets suivants :

$$E_{0,3} \to E_{1,1} \to E_{2,1}$$
$$E_{0,4} \to \mathcal{E} \to E_{2,5}$$
$$E_{0,5} \to E_{1,4} \to E_{2,7}$$

et on saît aussi que $\epsilon = +1$.

Exemple 4 (Cas de racines doubles, ℓ se scinde dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = +1$) : Soient $p = 10039$ et $\mathcal{E} = [7372, 8261]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 102$. Si on calcule le volcan pour $\ell = 3$, on obtient :

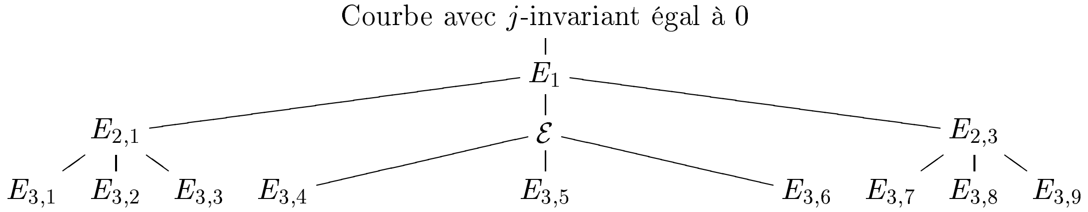


où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
E_0	$[3273, 8056]$	$E_{2,3}$	$[7337, 5253]$	$E_{3,3}$	$[7330, 392]$	$E_{3,6}$	$[3853, 5654]$
$E_{2,1}$	$[8850, 7741]$	$E_{3,1}$	$[9062, 3199]$	$E_{3,4}$	$[3523, 8744]$		
$E_{2,2}$	$[7787, 2602]$	$E_{3,2}$	$[4544, 8271]$	$E_{3,5}$	$[4370, 7215]$		

Dès que l'on détecte une courbe qui a une racine double, on arrête les calculs puisque l'on sait que E_0 est dans le cratère et que $\epsilon = +1$ d'après le lemme 6.1.5.

Exemple 5 (Cas où le j-invariant de la courbe E_s est égal à 0) : Soient $p = 1009$ et $\mathcal{E} = [363, 690]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 433$. En prenant $\ell = 3$, on obtient :

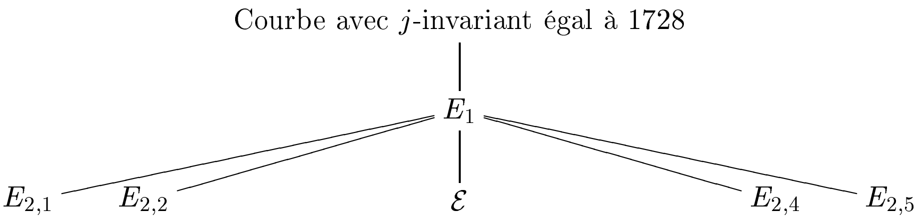


où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
E_1	$[45, 30]$	$E_{3,1}$	$[677, 347]$	$E_{3,4}$	$[917, 182]$	$E_{3,7}$	$[901, 228]$
$E_{2,1}$	$[178, 159]$	$E_{3,2}$	$[608, 155]$	$E_{3,5}$	$[595, 887]$	$E_{3,8}$	$[155, 198]$
$E_{2,3}$	$[212, 23]$	$E_{3,3}$	$[941, 179]$	$E_{3,6}$	$[110, 848]$	$E_{3,9}$	$[999, 594]$

Dans ce cas on ne peut trouver l'équation de la courbe de j-invariant 0, donc on ne peut obtenir de parcours descendants complets.

Exemple 6 (Cas où le j-invariant de la courbe E_s est égal à 1728) : Soient $p = 7349$ et $\mathcal{E} = [6871, 2131]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 331$. Pour $\ell = 5$, on obtient :



où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
E_1	$[4255, 5418]$	$E_{2,2}$	$[3272, 6926]$	$E_{2,4}$	$[7104, 2664]$	$E_{2,5}$	$[329, 4771]$
$E_{2,1}$	$[1316, 2594]$						

Là aussi, on ne peut obtenir de parcours descendants complets.

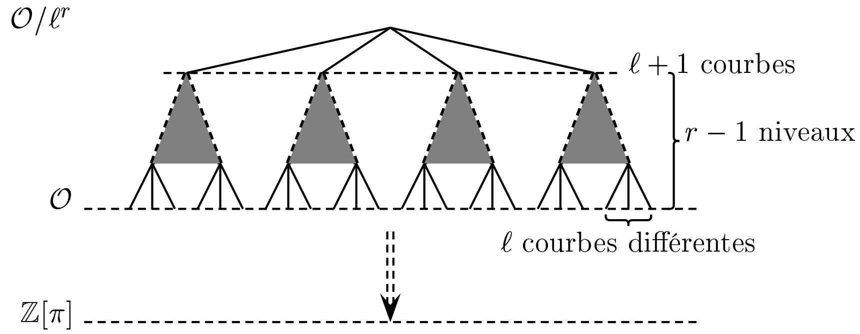
6.4 Nombre de volcans d'isogénies

On a vu comment construire un volcan de ℓ-isogénies, mais est-il possible que dans la même classe d'endomorphismes on puisse en calculer plusieurs, i.e. soit E et E' deux courbes elliptiques ayant le même anneau d'endomorphismes appartiennent-elles au même volcan de ℓ-isogénies ?

Soit E une courbe elliptique ordinaire définie sur $\mathbb{K} = \mathbb{F}_q$ (de caractéristique p). Soit $D < 0$ le discriminant fondamental tel que $\mathcal{O} = \mathrm{End}(E)$ soit un ordre dans le corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{D})$. On note g le conducteur de l'ordre $\mathbb{Z}[\pi]$ et f le conducteur de $\mathcal{O}$.

Si dans tous les cas on ne pouvait construire qu'un unique volcan de ℓ-isogénies alors on pourrait dénombrer grâce à ce volcan l'ensemble des $h(\mathcal{O})$ courbes elliptiques qui appartiennent à $\mathcal{C}(E)$. La méthode de dénombrement proposée des volcans de ℓ-isogénies est fondée sur le calcul de $h(\mathcal{O})$. Avant de dénombrer le nombre de volcans, il faut remarquer que si E et E' sont deux courbes qui sont ℓ^k-isogènes où $k \geqslant 1$ alors on construit le même volcan de ℓ-isogénies que l'on se serve de E ou de E' comme point de départ à l'algorithme.

Cas où $\left(\frac{d_K}{\ell}\right) = -1$. Dans cette situation, tout volcan de ℓ-isogénies admet la forme suivante :



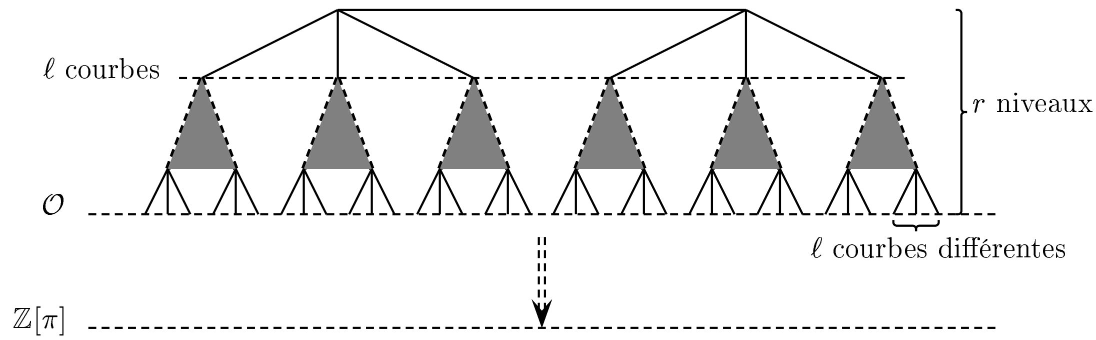
Comme il y a $h(\mathcal{O})$ courbes isogènes à E qui ont le même anneau d'endomorphismes que E, alors dans un volcan de ce type on en trouve $\ell^r + \ell^{r-1}$ (à chaque niveau descendu, on en a ℓ fois plus sauf pour le premier où là il y en a $\ell + 1$). Comme $h(m^2D) = \frac{h(D)m}{[\mathcal{O}_1^* : \mathcal{O}_2^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)$ où $\mathcal{O}_1$ et $\mathcal{O}_2$ sont les ordres de discriminant D et m^2D (voir [Cox89, p.148 Cor 7.28]), si l'on considère que D est différent de -4 et de -3 le dénominateur est alors égal à 1. On s'intéresse à

$m = \ell^r$ avec r la valuation ℓ-adique de f. On pose $f = f'\ell^r$. On a :

$$\begin{aligned} h(f^2 d_K) &= h(f'^2 D)\ell^r \left(1 - \left(\frac{D}{\ell}\right)\frac{1}{\ell}\right) \\ &= h(f'^2 D)\ell^r (1 + 1/\ell) \\ &= h(f'^2 D)(\ell^r + \ell^{r-1}) \end{aligned}$$

On voit donc qu'il y a $h(f'^2 D)$ volcans de cette forme et qui sont disjoints deux à deux.

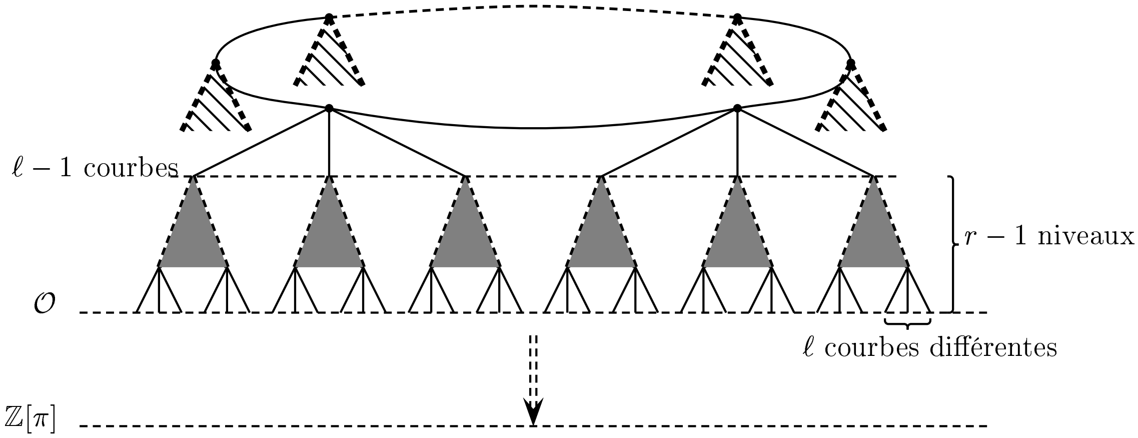
Cas où $\left(\frac{d_K}{\ell}\right) = 0$. Dans ce cas, tout volcan de ℓ-isogénies admet la forme suivante :



Dans un volcan de ce type, nous trouvons $2\ell^r$ courbes dans $\mathcal{C}(E)$. Dans ce cas il est aussi évident que le nombre de volcans est $h(f'^2 D_K)/2$ (en reprenant les notations décrites précédemment).

Cas où $\left(\frac{d_K}{\ell}\right) = 1$. C'est le cas le plus intéressant parce qu'au sommet du volcan il y a un cycle non réduit à un aller-retour (mis à part le cas où il y a deux ℓ-isogénies différentes de E vers E')

On obtient un volcan de la forme suivante :



Pour chacun des graphes sous le cratère, on trouve $(\ell - 1)\ell^{r-1}$ courbes dans $\mathcal{C}(E)$. Le tout maintenant est de savoir combien de sous-graphes construit-on i.e. combien de courbes vont se trouver dans le cratère du volcan ? La réponse est l'ordre de l'idéal premier $\mathfrak{l}$ de norme ℓ de $\mathcal{O}_K$. En effet, si l'on considère l'ensemble des courbes du cratère relevées dans $\mathbb{C}$, on obtient alors un cycle $\mathcal{E}_0 \to \mathcal{E}_1 \to \cdots \mathcal{E}_{s-1} \to \mathcal{E}_s \simeq \mathcal{E}_0$ où $\mathcal{E}_i \simeq \mathbb{C}/\mathfrak{a}_i$ et comme ce sont des ℓ-isogénies on a $\mathfrak{a}_i = \mathfrak{a}_{i+1}\mathfrak{l}$. Par conséquent, $\mathfrak{a}_0 = \mathfrak{a}_s = \mathfrak{l}^s \mathfrak{a}_0$ i.e. $\mathfrak{l}^s$ est un idéal principal de $\mathcal{O}_K$ et donc s est l'ordre de $\mathfrak{l}$ dans $\mathcal{O}_K$. Le nombre de volcans distincts que l'on peut construire dans ce cas est donc

$$h(f'^2 d_K)/\mathrm{ord}(\mathfrak{l}) \tag{6.2}$$

où $\mathrm{ord}(\mathfrak{l})$ est l'ordre de l'idéal $\mathfrak{l}$ qui est lui-même un idéal premier de norme ℓ.

En fait les trois cas reviennent à calculer la formule (6.2) d'après la proposition 1.2.1.

6.5 Extension de corps et extension du volcan

Une fois la création du volcan faite, l'une des questions naturelles est : qu'en est-il des courbes ℓ-isogènes qui n'apparaissent pas (i.e. celles qui sont sous $\mathbb{Z}[\pi]$) ? Nous allons chercher dans quelle extension de corps elles sont définies et surtout quelles sont les répercussions sur le volcan.

Tout d'abord regardons dans quelle extension de corps ces ℓ-isogénies sont définies. Lorsque nous sommes à la base du volcan (i.e. au niveau de $\mathbb{Z}[\pi]_\ell$), le modèle de factorisation de $\Phi_\ell(X, j)$ où j est le j-invariant d'une courbe E telle que $\mathrm{End}(E)_\ell = \mathbb{Z}[\pi]_\ell$ est un facteur de degré 1 et un facteur irréductible de degré ℓ. Il nous faut un résultat de factorisation dans les corps finis afin de déterminer l'extension qui nous intéresse.

Proposition 6.5.1 *Soit f un polynôme irréductible de $\mathbb{F}_q[X]$ de degré m alors le corps de décomposition de f sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$.*

Démonstration: Voir [LN83, Cor. 2.15.] □

On déduit de cette proposition que si l'on considère les isogénies et donc les courbes dans $\mathbb{F}_{q^\ell}$ alors on obtient les courbes que l'on recherchait, c'est à dire celles sous la base du volcan.

Maintenant que l'on sait dans quel corps regarder, on va étudier l'incidence que cela peut avoir sur le volcan.

$\mathbb{Z}[\pi]$ étant un ordre de K, nous pouvons aussi l'exprimer sous la forme $[1, g\omega_K]$ où g est le conducteur de $\mathbb{Z}[\pi]$ et donc π s'écrit aussi $a + g\omega_K$ où $a \in \mathbb{Z}$. On peut en savoir un peu plus sur les diviseurs de a en fonction des diviseurs de g.

Lemme 6.5.1 *Soit $\pi = a + g\omega_K$ le Frobenius. Soit $\ell \neq p$ un nombre premier tel que $\ell | g$, alors $\ell \nmid a$.*

Démonstration: Supposons qu'il existe un nombre premier ℓ tel que $\ell | a$ et $\ell | g$. Alors $\pi = \ell(a' + g'\omega_K)$ où $a' = a/\ell$ et $g' = g/\ell$ et donc le Frobenius est la composition de la multiplication par ℓ et d'un autre endomorphisme défini par $\alpha = a' + g'\omega_K$ i.e. $\pi = [\ell] \circ \alpha$. Si on considère la duale du Frobenius, on obtient $\hat{\pi} = \widehat{[\ell] \circ \alpha} = \hat{\alpha} \circ [\ell]$ et donc $q = \deg(\pi) = \hat{\pi} \circ \pi = \ell^2 \times \deg(\alpha)$ donc $\ell | q$ ce qui impossible par hypothèse. □

On peut prouver de manière similaire que tout diviseur de a ne peut être un diviseur de g. En définitive, a et g sont premiers entre eux. Maintenant il nous est possible de prouver que si l'on considère le même volcan de ℓ-isogenies dans $\mathbb{F}_{q^\ell}$ pour $\ell \neq 2$ alors il n'augmente que d'un niveau.

Lemme 6.5.2 *Soit $\ell \neq p$ un nombre premier tel que $\ell | g$ et $\ell \neq 2$ et soit n la valuation ℓ-adique de g. Alors la valuation ℓ-adique du conducteur de $\mathbb{Z}[\pi^\ell]$ est $n + 1$.*

Démonstration: En reprenant la notation précédente, on a $\pi = a + g\omega_K$. Dans le corps $\mathbb{F}_{q^\ell}$, le Frobenius qui nous intéresse est l'application qui pour tout $x \in \mathbb{F}_{q^\ell}$ associe x^{q^ℓ}. On peut l'étendre aux courbes elliptiques, i.e. à tout $P = (X, Y)$ point de la courbe on associe le point de coordonnées (X^{q^ℓ}, Y^{q^ℓ}). Cette application est égale à π^ℓ. On va donc regarder ce que vaut π^ℓ à partir des données sur π.

$$\begin{aligned}\pi^\ell &= (a + g\omega_K)^\ell \\ &= \sum_{k=0}^{\ell} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k} \\ &= a^\ell + \sum_{k=0}^{\ell-1} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k} \\ &= a^\ell + g\omega_K \sum_{k=0}^{\ell-1} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1}.\end{aligned}$$

On pose $\tau = \sum_{k=0}^{\ell-1} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1}$:

$$\begin{aligned}\tau &= \binom{\ell}{\ell-1} a^{\ell-1} + \sum_{k=1}^{\ell-2} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1} + (g\omega_K)^{\ell-1} \\ &= \ell a^{\ell-1} + \sum_{k=1}^{\ell-2} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1} + (g\omega_K)^{\ell-1}.\end{aligned}$$

D'après le lemme 6.5.1, $\ell \nmid a$ donc $\ell \parallel \ell a^{\ell-1}$. Pour tout $1 \leqslant k \leqslant \ell - 1$ et pour tout nombre ℓ premier, $\ell | \binom{\ell}{k}$. De plus comme $g | \sum_{k=1}^{\ell-2} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1}$ et que $\ell | g$ par hypothèse, alors

$$\ell^2 | \sum_{k=1}^{\ell-2} \binom{\ell}{k} a^k (g\omega_K)^{\ell-k-1}.$$

Enfin, comme $\ell | g$ et $\ell \neq 2$, $\ell^2 | (g\omega_K)^{\ell-1}$. On a donc $\ell \parallel \tau$ et la valuation ℓ-adique du conducteur de $\mathbb{Z}[\pi^\ell]$ est $n + 1$.
□

Le cas où $\ell = 2$ pose un problème lorsque $2 \parallel g$. Autrement pour les autres cas, la croissance du volcan n'est que d'un seul niveau.

Chapitre 7

Applications des volcans d'isogénies

Toutes les améliorations de l'algorithme de Schoof présentées en 4.2 ne sont valables que lorsque le Frobenius modulo ℓ a deux valeurs propres distinctes. Couveignes, Morain et Dewaghe ont déjà essayé de traiter le cas où le Frobenius admet une unique valeur propre double. Ils ont construit des arbres d'isogénies mais n'avaient pas d'explications pour ces graphes. On se propose ici de résoudre enfin ce cas. En effet, les volcans d'isogénies vont nous permettre de comprendre ces arbres. On va tout d'abord supposer que ℓ est différent de 2. Ce cas est très similaire aux autres cas, mais demande de petites modifications qui seront décrites en 7.6.

7.1 Le discriminant d_π

Le discriminant d_π est égal à t^2-4q, mais il est aussi égal à $g^2 d_K$ où g est le conducteur de $\mathbb{Z}[\pi]$ et d_K le discriminant du corps quadratique imaginaire qui contient l'anneau d'endomorphismes de la courbe. Si l'on sait que le Frobenius modulo ℓ admet une racine double unique, on sait alors que $d_\pi \equiv 0 \bmod \ell$ et donc que $t^2 \equiv 4q \bmod \ell$. La construction du volcan d'isogénies de la courbe pour ℓ tel que $d_\pi \equiv 0 \bmod \ell$ va nous donner la valuation ℓ-adique ν_ℓ de d_π.

En effet, la construction même du volcan nous montre qu'en partant du cratère chaque niveau vertical parcouru correspond à des courbes dont le conducteur de l'anneau d'endomorphismes a une puissance de ℓ en plus. Ainsi connaître le niveau des courbes dont l'anneau d'endomorphismes est isomorphe à $\mathbb{Z}[\pi]$ localement par rapport à ℓ nous donne la valuation ℓ-adique de g. Le type de cratère auquel nous avons à faire nous indique si (d_K/ℓ) est égal à $+1$, 0 ou -1 et donc si $d_K \equiv 0 \bmod \ell$ ou pas. Si on note n la valuation ℓ-adique de g et δ celle de d_K, on obtient $\nu_\ell = 2n + \delta$ et donc que $t^2 \equiv 4q \bmod \ell^{2n+\delta}$.

7.2 Algorithme

Comme on vient de le décrire, connaître le volcan nous donne tous les renseignements nécessaires. Ainsi l'algorithme est tout simplement fondé sur un calcul de volcan partiel.

Procédure CalculValuation
Entrée : Une courbe elliptique $\mathcal{E}$ et un nombre premier ℓ, $\ell \neq p$.
Sortie : La valuation ℓ-adique de d_π.

1. $\{pdc, \epsilon\} \leftarrow$ CalculVolcanPartiel$(\mathcal{E}, \ell)$;
2. $n \leftarrow \#pdc - 1$;
3. SI $\epsilon = 0$ ALORS $\delta \leftarrow 1$ SINON $\delta \leftarrow 0$;

4. RETURN $2n+\delta$.

7.3 Trouver t mod ℓ^ν

En général (c'est à dire excepté dans les cas particuliers, voir 7.5), notre algorithme nous donne $t^2 \equiv 4q \bmod \ell^\nu$, il nous faut maintenant obtenir $t \bmod \ell^\nu$. On suppose encore dans ce cas que $\ell \neq 2$. Alors il y a seulement deux racines carrées de $4q$ modulo ℓ^ν. Pour trouver le signe de t, il suffit de trouver le signe de $t_1 \equiv t \bmod \ell$: une seule des racines de l'equation modulo ℓ^ν se réduira à t_1 modulo ℓ. Trouver t_1 est réalisé via la détermination d'un espace propre de π et le facteur associé du polynôme de ℓ-division f_ℓ à la Elkies. On va ainsi déterminer la valeur propre, qui est égal en fait à $t_1/2 \bmod \ell$ dans notre cas.

7.4 Trouver t mod $\ell^{\nu+1}$

Une fois que l'on a trouvé $t \bmod \ell^\nu$, est-il possible de trouver $t \bmod \ell^{\nu+1}$? Quand $(d_K/\ell) \neq +1$, on ne peut rien faire puisque l'on a déjà exploré toutes les isogénies possibles. Dans le cas où $(d_K/\ell) = +1$, le cratère du volcan est un cycle d'isogénies et les idées de [CM94] s'appliquent ici aussi. Dans ce cas, on a trouvé trois courbes : la courbe E_s dans le cratère et deux autres courbes E_1 et E_1^* qui sont reliées à E_s par des ℓ-isogénies horizontales. En commençant par exemple à partir de $I_1 : E_s \to E_1$, on peut trouver l'unique ℓ-isogénie horizontale $I_2 : E_1 \to E_2$ qui ne soit pas la duale de I_1 (et par conséquent E_2 n'est pas isomorphe à E_s) en utilisant la procédure CalculParcoursDescendantsComplets. De cette manière, on construit une suite de courbes isogènes, à partir duquel on peut déduire les facteurs de $f_{\ell^d}(E_s)$ ou d'un $f_{\ell^d}(E)$, selon si on calcule les isogénies en avançant dans le cycle comme proposé originalement dans [CM94] ou alors à l'envers ce qui est bien plus efficace (voir [CDM96]). Voir l'exemple 3 ci dessous.

7.5 Cas particuliers

7.5.1 Cas des courbes de j-invariant égal à 0 ou 1728.

Si notre courbe originale E a l'un de ces invariants, alors il est facile de calculer sa cardinalité, cf. par exemple [Kat85]. Si on rencontre une telle courbe en construisant le volcan d'isogénie, alors on peut tout de même connaitre la hauteur du volcan et donc la valuation ℓ-adique du conducteur g de $\mathbb{Z}[\pi]$. On sait aussi que $j = 0$ (resp. $j = 1728$) correspond à $\#E = q + 1 - t$ où $4q = t^2 + 3v^2$ (resp. $4q = t^2 + 4v^2$). Il y a 6 (resp. 4)solutions pour (t, v), mais seulement une telle que $\ell \mid v$ (sauf dans le cas où $\ell = 2$).

7.5.2 Cas où pour l'un des j du volcan, $\Phi_\ell(X, j)$ a une racine double.

Soit E notre courbe initiale, d'anneau d'endomorphismes $\mathrm{End}(E)$ de conducteur f et soit E_s telle que $\Phi_\ell(X, j(E_s))$ a une racine double. Ceci ne peut arriver que lorsque l'on calcule un chemin ascendant partant de E. Par le lemme 6.1.5 on sait que E_s est dans le cratère du volcan. L'anneau d'endomorphismes $\mathrm{End}(E_s)$ de E_s a pour conducteur f_s qui n'est pas divisible par ℓ. En calculant un parcours descendant à partir de E_s, on trouve la valuation ℓ-adique n de g.

Nous savons aussi, d'après le théorème 6.1.1 qu'un entier de $\mathrm{End}(E_s)$ a pour norme ℓ^2, i.e., l'équation $4\ell^2 = x^2 + (|d_K|f_s^2)y^2$ a une solution entière non-triviale (x, y). Si ℓ est petit, ce qui est généralement le cas en pratique, on peut tester l'ensemble des d_K et des f_s premiers à ℓ satisfaisant l'équation de la norme, et on trouve l'ensemble des anneaux d'endomorphismes possibles. On peut éliminer des candidats, puisque l'on sait aussi que q doit satisfaire $4q = t^2 + (|d_K|(\ell^n f_s)^2)v^2$ pour des entiers rationnels t et v.

7.6 Remarques sur le cas $\ell = 2$.

Quelques modifications mineures sont nécessaires. Tout d'abord, si ℓ se ramifie dans $\mathcal{O}_K$, cela signifie que $\ell \mid d_K$. Quand $\ell = 2$, par définition du discriminant d'un corps quadratique, alors on a $4 \mid d_K$. Par conséquent, quand 2 se ramifie dans $\mathcal{O}_K$, δ est égal à 2. Cette remarque s'applique aussi lorsque $\mathcal{O}_{K_\ell} \simeq \mathbb{Z}[\pi]_\ell$ et que $\mathcal{N}_\ell(j) = 1$, i.e. on sait alors directement que $t^2 \equiv 4q \pmod 4$.

Il se pourrait aussi que la valuation 2-adique de d_π soit égale à $2n + \delta + 1$, puisque par définition du discriminant d'un corps quadratique $d_K/4$ peut être divisible par 2. Mais nous ne savons pas comment récupérer ce facteur de d_K et dans ce cas, on n'obtiendra peut-être qu'un résultat partiel.

Trouver $t \bmod 2^\nu$ est pour ainsi dire sans espoir. D'un côté, l'équation $t^2 \equiv 4q \bmod 2^\nu$ nous donne $t \bmod 2^{\nu-1}$. De l'autre côté, il y a quatre valeurs possibles de t (au moins quand $\nu > 2$) que l'on ne peut distinguer sans avoir à calculer le facteur correspondant de $f_{2^{\nu-1}}$.

7.7 Relations avec les arbres d'isogénies

Dans [CDM96], les auteurs ont essayé de décrire la situation via un arbre où le Frobenius a une valeur propre double. Cette arbre correspond à des appels répétitifs à la routine qui construit des courbes isogènes. Cet arbre est en fait une vue particulière du volcan. Une fois le cratère du volcan détecté dans l'arbre d'isogénies, on l'équilibre et on retrouve le volcan (voir l'exemple 5).

7.8 Résolution d'un problème de Lercier

Dans sa thèse [Ler97a, p. 137], Lercier a besoin de trouver une courbe elliptique E' isogène à une courbe donnée E qui a trois points de 2-torsion, avec la propriété que E' a seulement un point de 2-torsion. Une telle courbe peut exister, puisque deux courbes isogènes peuvent ne pas avoir la même structure de groupe (voir [Len96]). En utilisant notre approche, ce phénomène peut être expliqué et nous pouvons donner un algorithme pour trouver E'.

Tout d'abord on remarque que les points de 2-torsion de E correspondent exactement à des isogénies de degré 2. Par exemple, quand $p > 2$, la courbe $E : Y^2 = (X - x_0)(X^2 + aX + b)$ d'invariant

$$j = 256\frac{(w + a^2 - 4b)^3}{w^2(a^2 - 4b)}$$

(avec $w = x_0^2 + ax_0 + b$) a $(x_0, 0)$ comme point de 2-torsion et un simple calcul montre que

$$j^* = 16\frac{(16w + a^2 - 4b)^3}{w(a^2 - 4b)^2}$$

est l'invariant d'une courbe 2-isogène.

Par conséquent, le nombre de points de 2-torsion est égal au nombre de 2-isogénies rationnelles de la courbe, c'est à dire $\mathcal{N}_2(E)$. D'après notre algorithme, on sait que les courbes dont l'anneau d'endomorphismes est isomorphe à $\mathbb{Z}[\pi]$ localement par rapport à ℓ satisfont $\mathcal{N}_2 = 1$. Pour trouver l'une de ces courbes, il suffit donc de calculer un chemin descendant partant de E, et ceci est un sous-produit du calcul de ν_2. La complexité des calculs est bornée par la hauteur du volcan d'isogénies, qui est polynomial en $\log |d_K|$. De plus, en moyenne, ν_2 est petit, et donc la recherche de E' est assez rapide.

7.9 Exemples numériques

On reprend dans cette section les exemples donnés en 6.3 et on en déduit la valuation ℓ-adique de d_π. On ne va pas redessiner les volcans mais juste s'y réferer.

Exemple 1 (ℓ est inerte dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = -1$) : Soient $p = 5081$ et $\mathcal{E} = [3290, 3887]$. Le j-invariant de $\mathcal{E}$ est $j_\mathcal{E} = 1765$. Pour $\ell = 5$, on trouve que $n = 2$ et que $\left(\frac{d_K}{\ell}\right) = -1$. On en déduit que $\delta = 0$ et donc que $t^2 \equiv 4p \pmod{5^4}$. On utilise la ℓ-isogénie $E_0 \to E_{1,1}$ pour trouver le facteur $X^2 + 1448X + 1478$ de $f_5(E_0)$ qui est associé à la valeur propre 1 du Frobenius modulo 5. Nous en déduisons que $t \equiv 607 \equiv -18 \bmod 5^4$. En fait, $t = -18$.

Exemple 2 (ℓ se ramifie dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = 0$) : Soient $p = 5059$ et $\mathcal{E} = [4646, 1411]$. Le j-invariant de $\mathcal{E}$ est $j_\mathcal{E} = 1790$. Pour $\ell = 3$, on trouve que $n = 2$ et que $\left(\frac{d_K}{\ell}\right) = 0$. On en déduit que $\delta = 1$ et donc que $t^2 \equiv 4p \pmod{3^5}$. En fait, $t = -124$.

Exemple 3 (ℓ se scinde dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = +1$) : Soient $p = 10009$ et $\mathcal{E} = [7478, 1649]$. Le j-invariant de $\mathcal{E}$ est $j_\mathcal{E} = 83$. Pour $\ell = 3$, on trouve que $n = 2$ et que $\left(\frac{d_K}{\ell}\right) = +1$. On en déduit que $\delta = 0$ et $t^2 \equiv 4p \pmod{3^4}$. En fait, $t \equiv 34 \bmod 3^4$.

De plus dans ce cas, nous pouvons construire dans le cratère du volcan un cycle de ℓ-isogénie. On obtient le graphe suivant :

$$\begin{tikzcd}
& E_6 \arrow[dl] & E_5 \arrow[l] & E_4 \arrow[l] & \\
E_0 \arrow[dr] & & & & E_3 \arrow[ul] \\
& E_1 \arrow[rr] & & E_2 \arrow[ur] &
\end{tikzcd}$$

où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
E_0	$[7778, 9421]$	E_2	$[56, 8167]$	E_4	$[616, 274]$	E_6	$[5051, 4157]$
E_1	$[7418, 8055]$	E_3	$[1336, 8702]$	E_5	$[352, 4401]$		

En utilisant ce cycle on trouve que $t \equiv -47 \bmod 3^5$. En fait, $t = -47$.

Exemple 4 (Cas de racines doubles, ℓ se scinde dans $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = +1$) : Soient $p = 10039$ et $\mathcal{E} = [7372, 8261]$. Le j-invariant de $\mathcal{E}$ est $j_\mathcal{E} = 102$. Pour $\ell = 3$, on trouve que $n = 3$ et $\left(\frac{d_K}{\ell}\right) = 1$ donc $\delta = 0$ et $t^2 \equiv 4p \pmod{3^6}$. De plus, on observe que la courbe que l'on trouve dans le cratère a une racine double. On en déduit donc que $\mathcal{E}$ est à multiplication complexe par un ordre de conducteur $3^3 f_s$ dans un corps quadratique $K = \mathbb{Q}(\sqrt{d_K})$ tel que les deux équations

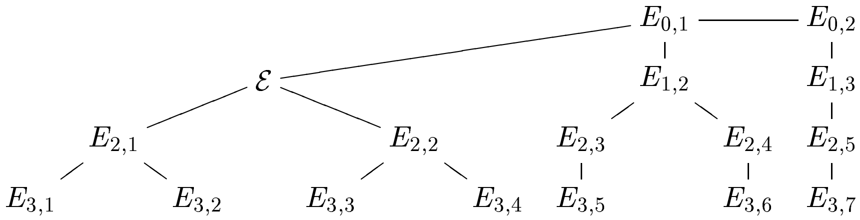
$$4 \times 3^2 = x^2 + (|d_K| f_s^2) y^2, \quad 4p = t^2 + (|d_K|(3^3 f_s)^2) v^2$$

admettent une solution en entiers rationnels x, y, t, v. L'unique solution possible est $d_K = -35$ et $f_s = 1$. On en déduit que $|t| = 121$ et en fait, $t = 121$.

Exemple 5 (Cas où la courbe E_s a j-invariant égal à 0) : Soient $p = 1009$ et $\mathcal{E} = [363, 690]$. Le j-invariant de $\mathcal{E}$ est $j_\mathcal{E} = 433$. On trouve que $n = 3$, $\left(\frac{d_K}{\ell}\right) = 0$ donc $\delta = 1$ et $t^2 \equiv 4p \pmod{3^7}$. En réalité, $t = 43$.

Exemple 6 (Cas où la courbe E_s a j-invariant égal à 1728) : Soient $p = 7349$ et $\mathcal{E} = [6871, 2131]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 331$. On trouve que $n = 2$, $\left(\frac{d_K}{\ell}\right) = +1$ donc $\delta = 0$ et $t^2 \equiv 4p \pmod{5^4}$. En réalité, $t = 164$.

Exemple 7 (Cas incomplet pour $\ell = 2$ de [CDM96]) : Soient $p = 1009$ et $\mathcal{E} = [1, 3]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 269$. Pour $\ell = 2$, on obtient



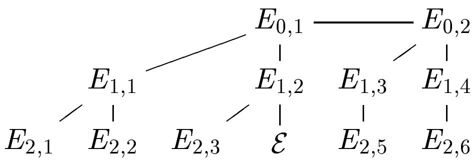
où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
$E_{0,1}$	$[241, 990]$	$E_{2,1}$	$[502, 692]$	$E_{2,5}$	$[763, 476]$	$E_{3,4}$	$[65, 785]$
$E_{0,2}$	$[481, 611]$	$E_{2,2}$	$[284, 534]$	$E_{3,1}$	$[978, 971]$	$E_{3,5}$	$[917, 988]$
$E_{1,2}$	$[814, 970]$	$E_{2,3}$	$[309, 338]$	$E_{3,2}$	$[979, 113]$	$E_{3,6}$	$[46, 408]$
$E_{1,3}$	$[427, 373]$	$E_{2,4}$	$[397, 322]$	$E_{3,3}$	$[995, 970]$	$E_{3,7}$	$[1000, 782]$

Par conséquent, $n = 3$, $\left(\frac{d_K}{\ell}\right) = 0$ et donc $\delta = 2$ et $t^2 \equiv 4p \pmod{2^8}$.

En réalité, $t = -50$, donc $d_K = -24$, $g = 2^3$ et $(-50)^2 \equiv 4 \times 1009 \pmod{2^9}$. Dans ce cas, on n'obtient donc qu'une borne inférieure de la valuation 2-adique de d_π.

Exemple 8 (Cas complet pour $\ell = 2$) : Soient $p = 10009$ et $\mathcal{E} = [7171, 8117]$. Le j-invariant de $\mathcal{E}$ est $j_{\mathcal{E}} = 14$. Pour $\ell = 2$, on obtient :



où

courbe	équation	courbe	équation	courbe	équation	courbe	équation
$E_{0,1}$	$[2275, 6698]$	$E_{1,2}$	$[201, 7055]$	$E_{2,1}$	$[3135, 4043]$	$E_{2,5}$	$[6160, 1295]$
$E_{0,2}$	$[932, 23]$	$E_{1,3}$	$[654, 573]$	$E_{2,2}$	$[2343, 2889]$	$E_{2,6}$	$[7890, 2646]$
$E_{1,1}$	$[6775, 534]$	$E_{1,4}$	$[9749, 2660]$	$E_{2,3}$	$[4637, 9029]$		

Par conséquent, $n = 2$, $\left(\frac{d_K}{\ell}\right) = 0$ donc $\delta = 2$ et $t^2 \equiv 4p \pmod{2^6}$.

En réalité, $t = 70$, donc $d_K = -2^2 \times 61$, $g = 2^2 \times 3$ et $(-70)^2 \equiv 4 \times 10009 \pmod{2^6}$. Dans ce cas, on obtient la bonne valuation.

7.10 Calcul de l'équation de classe

Dans leur article [CNST98] Chao et al. proposent une nouvelle méthode pour déterminer l'équation de classe d'un ordre $\mathcal{O}$ dans un corps quadratique imaginaire. Leur algorithme consiste en le calcul de cette équation modulo un ensemble de nombres premiers p_i et de finalement retrouver $H_{\mathcal{O}}(X)$ en utilisant le théorème du reste chinois.

Soit d le discriminant de l'ordre $\mathcal{O}$. On peut écrire d sous la forme $c^2 D$ où D est un discriminant fondamental. Comme l'on ne va s'attarder que sur le calcul de $H_{\mathcal{O}}(X)$ modulo un nombre premier, on note p ce nombre premier. Soit $\mathbb{F}_q$ le corps résiduel de $\mathbb{Q}(j(\mathcal{O}))$ modulo l'idéal premier $\mathfrak{P}$ au dessus de p.

Pour calculer $H_{\mathcal{O}}(X) \bmod p$, ils suggèrent de calculer $h(d)$ courbes E_s isogènes mais non-isomorphes telles que

$$\#E_s(F_q) = q + 1 - t \text{ où } 4q = t^2 - c'^2 D \tag{7.1}$$

alors

$$H_{\mathcal{O}}(X) \bmod p \equiv \prod_{s=1}^{h(d)} (X - j(E_s)).$$

Cependant ces calculs ne sont valides que si les courbes E_s considérées ont pour anneau d'endomorphismes $\mathcal{O}$. Or la condition 7.1 n'impose pas que $\mathrm{End}(E_s) = \mathcal{O}$. Pour assurer la validité de cet algorithme, il faudrait donc que pour chaque courbe calculée on vérifie la valeur de son anneau d'endomorphismes à l'aide de l'une des méthodes de Kohel.

Nous proposons de modifier légèrement cette méthode afin de ne pas avoir à utiliser les algorithmes de Kohel à chaque calcul de courbes. Au lieu de calculer les $h(d)$ courbes, nous ne calculons qu'une seule courbe satisfaisant 7.1 et nous allons alors calculer à l'aide des volcans d'isogénies un ensemble de courbes E_i telles que $\mathrm{End}(E_i) = \mathcal{O}$. Pour cela il faut pouvoir déterminer des courbes dont le conducteur de l'anneau d'endomorphisme a une valuation ℓ-adique donnée.

Procédure CalculCourbesÀValuationDonnée
Entrée : Une courbe elliptique E satisfaisant la condition 7.1, un nombre premier ℓ et la valuation ℓ-adique e recherchée.
Sortie : Une courbe E' isogène à E telle que si f est le conducteur de $\mathrm{End}(E)$ alors $\ell^e \parallel f$.

1. $\{\mathcal{F}, \epsilon\} \leftarrow$CalculVolcanPartiel (E, ℓ) ;
2. $E' \leftarrow$ la $e+1$-ème courbe de $\mathcal{F}$;
3. RETURN E'.

D'après le lemme 6.2.2, la $e+1$-ème courbe d'un parcours descendant complet est au niveau e et donc la valuation ℓ-adique du conducteur de $\mathrm{End}(E')$ est e.

Maintenant il nous faut pouvoir trouver un ensemble de courbes E_i qui satisfont $\mathrm{End}(E_i) = \mathcal{O}$. On rappelle tout d'abord que les conducteurs des anneaux d'endomorphismes de deux courbes dans le même volcan de ℓ-isogénies ne diffèrent que d'une puissance de ℓ. On va donc considérer l'ensemble des nombres premiers ℓ_i divisant c et leur valuation e_i correspondante.

Procédure CalculCourbesAvecConducteurDonné
Entrée : Une courbe elliptique E satisfaisant la condition 7.1 et un conducteur c.
Sortie : Un ensemble de courbes E_i isogènes mais non-isomorphes telles que $\mathrm{End}(E_i) = \mathcal{O}$.

1. Déterminer les couples (ℓ_i, e_i) tels que $\prod_{i=1}^n \ell_i^{e_i}$ soit la factorisation en nombres premiers distincts de c ;
2. POUR $j = 1$ À $n-1$ FAIRE $E \leftarrow$ CalculCourbeÀValuationDonnée(E, ℓ_j, e_j) ;
3. Construire dans son intégralité le volcan de ℓ_n-isogénies de E ;
4. RETURN l'ensemble des courbes au niveau e_n.

Cela nous donne un ensemble de courbes qui satisfont les conditions nécessaires pour être utilisées dans le calcul de $H_{\mathcal{O}}(X) \bmod p$. Pour calculer les $h(d)$ courbes dont nous avons besoin, il suffit de recommencer cette manœuvre autant de fois que nécessaire avec une nouvelle courbe satisfaisant 7.1 à chaque fois.

Troisième partie

Algorithmes p-adiques

Chapitre 8

Anneaux locaux

Les récents algorithmes de calcul de la cardinalité d'une courbe elliptique ordinaire définie sur un corps à p^d éléments utilisent un relèvement de la courbe dans un anneau local ou plus exactement dans l'extension non ramifiée de degré d de l'anneau des entiers p-adiques. Ainsi avant de décrire ces algorithmes, nous décrivons cet objet et expliquons quelle représentation nous utilisons pour les calculs. Pour de plus amples détails sur les anneaux locaux, voir [Ser68].

8.1 L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Avant de pouvoir introduire cet objet mathématique, il nous faut tout d'abord faire quelques rappels sur l'anneau des entiers p-adiques. Ces rappels ne se veulent pas du tout exhaustif et nous renvoyons le lecteur au livre de Serre [Ser70] et à celui d'Amice [Ami75] pour une approche plus complète.

8.1.1 Définitions

Soit π_n la projection de $\mathbb{Z}/p^{n+1}\mathbb{Z}$ dans $\mathbb{Z}/p^n\mathbb{Z}$. Cette projection est un homomorphisme d'anneau. On est amené alors à considérer la suite :

$$\ldots \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

On peut donner une définition constructive des entiers p-adiques de la manière suivante.

Définition 8.1.1 *Un entier p-adique est une suite $x = (x_1, x_2, \ldots, x_n, \ldots)$, avec $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ et tel que $\pi_n(x_{n+1}) = x_n$ pour $n \geqslant 1$. L'anneau des entiers p-adiques est noté par $\mathbb{Z}_p$.*

De manière plus formelle, on peut aussi définir l'anneau des entiers p-adiques comme étant la limite projective du système $(\mathbb{Z}/p^n\mathbb{Z}, \pi_n)$.

La somme et le produit dans $\mathbb{Z}_p$ sont définis coordonnées par coordonnées de manière naturelle. On remarque que $\mathbb{Z}_p$ est un anneau de valuation discrete non-ramifié. Son unique idéal premier non nul est $p\mathbb{Z}_p$ et le corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p$ est isomorphe à $\mathbb{F}_p$.

On étend la définition de π_n afin d'inclure la projection de $\mathbb{Z}_p$ sur $\mathbb{Z}/p^n\mathbb{Z}$ i.e. $x \mapsto x_n$. Il est clair que si l'on connait x_n, on peut retrouver la valeur de x_k pour $k \leqslant n$ facilement en se servant des projections sur $\mathbb{Z}/p^k\mathbb{Z}$. On pose $\pi = \pi_1$. On remarque que π peut être considéré comme la projection sur $\mathbb{F}_p$.

8.1.2 Les unités p-adiques et la valuation p-adique

Proposition 8.1.1 *1. Pour qu'un élément de $\mathbb{Z}_p$ soit inversible, il faut et il suffit qu'il ne soit pas divisible par p.*

2. Si U désigne le groupe des éléments inversibles de $\mathbb{Z}_p$, tout élément de $\mathbb{Z}_p$ différent de 0 s'écrit de façon unique sous la forme $p^n u$ avec $u \in U$ et $n \geqslant 0$.

(Un élément de U est appelé une unité p-adique.*)*

Démonstration:

1. On va prouver cette assertion pour tous les $\mathbb{Z}/p^n\mathbb{Z}$, après déduire le résultat sur $\mathbb{Z}_p$ est évident. Soit $x \in \mathbb{Z}/p^n\mathbb{Z}$ tel que $x \notin p\mathbb{Z}/p^n\mathbb{Z}$, alors son image dans $\mathbb{Z}/p\mathbb{Z}$ est non nulle et donc inversible. Il existe donc y et z éléments de $\mathbb{Z}/p^n\mathbb{Z}$ tel que $xy = 1 - pz$ et donc $xy(1 + pz + p^2z^2 + \ldots + p^{n-1}z^{n-1}) = 1 - p^n z^n = 1 \in \mathbb{Z}/p^n\mathbb{Z}$. Par suite, x est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$. De manière évidente si $x \in p\mathbb{Z}/p^n\mathbb{Z}$ alors x est un diviseur de 0 et donc n'est pas inversible.
2. Soit $x \in \mathbb{Z}_p$ non nul. Alors par définition, il existe un plus grand n tel que $\pi_n(x) = 0$. On a alors $x = p^n u$ où u n'est pas divisible par p donc $u \in U$.

□

C'est à dire que les éléments inversibles de $\mathbb{Z}_p$ sont les entiers p-adiques qui ne se trouvent pas dans $p\mathbb{Z}_p$ i.e., ceux tels que $\pi(x) \neq 0$.

Définition 8.1.2 *Soit $x \in \mathbb{Z}_p$, non-nul. Alors x s'écrit sous la forme $p^n u$ où $u \in U$. L'entier n est appelé la* valuation p-adique *de x, et est noté $v_p(x)$.*

Par convention, on pose $v_p(0) = +\infty$. On a :

$$\begin{aligned} v_p(xy) &= v_p(x) + v_p(y) \\ v_p(x+y) &\geqslant \mathrm{Inf}(v_p(x), v_p(y)) \end{aligned}$$

On peut à partir de la valuation p-adique définir une *distance ultramétrique* : soient x et y dans $\mathbb{Z}_p$,

$$d(x, y) = e^{-v_p(x-y)}. \tag{8.1}$$

8.1.3 Le corps $\mathbb{Q}_p$

Définition 8.1.3 *On appelle corps des nombres p-adiques, et on note $\mathbb{Q}_p$, le corps des fractions de l'anneau $\mathbb{Z}_p$.*

On voit tout de suite que $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. Tout élément de $\mathbb{Q}_p^*$ s'écrit de façon unique sous la forme $p^n u$ avec $n \in \mathbb{Z}$ et $u \in U$; ici encore, n s'appelle la valuation p-adique de x et se note $v_p(x)$. On a $v_p(x) \geqslant 0$ si et seulement si $x \in \mathbb{Z}_p$. La distance ultramétrique d est aussi définie dans ce cas.

8.2 L'anneau $\mathbb{Z}_q$

L'anneau $\mathbb{Z}_p$ des entiers p-adiques est pour ainsi dire "au-dessus" de $\mathbb{F}_p$. En effet, on a vu dans la section précédente que si l'on considère la projection π de $\mathbb{Z}_p$ on se retrouve dans $\mathbb{F}_p$. L'anneau dans lequel nous cherchons à relever notre courbe a pour sa part $\mathbb{F}_q$ comme corps résiduel. La réponse mathématique est l'*anneau des vecteurs de Witt.*

8.2.1 Vecteurs de Witt

Soit p un nombre premier, soit $(X_0, \ldots, X_n, \ldots)$ une suite d'indéterminées, et considérons les polynômes suivants appelés *polynômes de Witt* :

$$\begin{aligned} W_0 &= X_0 \\ W_1 &= X_0^p + pX_1 \\ &\cdots \\ W_n &= \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n \text{ pour } n \geqslant 1 \end{aligned}$$

On remarque tout d'abord que $W_n(X_0, \ldots, X_n) = W_{n-1}(X_0^p, \ldots, X_{n-1}^p) + p^n X_n$.

Si l'on note $\mathbb{Z}'$ l'anneau $\mathbb{Z}[p^{-1}]$, il est clair que l'on peut exprimer les X_i comme des polynômes par rapport aux W_j à coefficients dans $\mathbb{Z}'$:

$$X_0 = W_0,\ X_1 = p^{-1}(W_1 - W_0^p), \ldots$$

Soit maintenant $(Y_0, \ldots, Y_n, \ldots)$ une autre suite d'indéterminées.

Théorème 8.2.1 *Pour tout $\Phi \in \mathbb{Z}[X, Y]$, il existe une suite $(\varphi_0, \ldots, \varphi_n, \ldots)$ d'éléments de $\mathbb{Z}[X_0, \ldots, X_n, \ldots; Y_0, \ldots, Y_n, \ldots]$ et une seule telle que l'on ait :*

$$\Phi(W_n(X_0, \ldots), W_n(Y_0, \ldots)) = W_n(\varphi_0, \ldots, \varphi_n, \ldots), \text{ pour tout } n \geqslant 0.$$

Démonstration: Serre [Ser68, Chap. II §6] □

Notons maintenant $S_0, \ldots, S_n, \ldots$ (resp. $P_0, \ldots, P_n, \ldots$) les polynômes $\varphi_0, \ldots, \varphi_n, \ldots$ associés par le théorème 8.2.1 aux polynômes

$$\Phi(X, Y) = X + Y \text{ (resp. } \Phi(X, Y) = X.Y).$$

Soit A un anneau commutatif. Soient $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ et $\mathfrak{b} = (b_0, \ldots, b_n, \ldots)$ deux éléments de $A^{\mathbb{N}}$. On pose :

$$\mathfrak{a} + \mathfrak{b} = (S_0(\mathfrak{a}, \mathfrak{b}), \ldots, S_n(\mathfrak{a}, \mathfrak{b}), \ldots) \tag{8.2}$$
$$\mathfrak{a}.\mathfrak{b} = (P_0(\mathfrak{a}, \mathfrak{b}), \ldots, P_n(\mathfrak{a}, \mathfrak{b}), \ldots) \tag{8.3}$$

Théorème 8.2.2 *Les lois de compositions définies en (8.2) et (8.3) font de $A^{\mathbb{N}}$ un anneau commutatif à élément unité, appelé l'anneau des* vecteurs de Witt *à coefficients dans A, et noté $W(A)$.*

Démonstration: Serre [Ser68, Chap. 6 §6] □

Soient $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ et $\mathfrak{b} = (b_0, \ldots, b_n, \ldots)$ deux éléments de $W(A)$. On a alors par exemple :

$$S_0(\mathfrak{a}, \mathfrak{b}) = a_0 + b_0 \qquad S_1(\mathfrak{a}, \mathfrak{b}) = a_1 + b_1 + \tfrac{a_0^p + b_0^p - (a_0 + b_0)^p}{p}, \tag{8.4}$$
$$P_0(\mathfrak{a}, \mathfrak{b}) = a_0.b_0 \qquad P_1(\mathfrak{a}, \mathfrak{b}) = b_0^p a_1 + b_1 a_0^p + p a_1 b_1. \tag{8.5}$$

On peut aussi définir la multiplication par un scalaire m comme étant l'application qui à un élément $\mathfrak{a}$ de $W(A)$ associe l'élément $[m]\mathfrak{a} = \underbrace{\mathfrak{a} + \cdots + \mathfrak{a}}_{m \text{ fois}}$.

De cette construction de $W(A)$, on tire le théorème suivant.

Théorème 8.2.3 *Si K est un corps parfait de caractéristique p, $W(K)$ est un anneau de valuation discrète non ramifié.*

Démonstration: Serre [Ser68, Chap. 6 §6] □

Le Frobenius dans $W(\mathbb{F}_q)$

Soit p la caractéristique de $\mathbb{F}_q$. Alors on appelle le *petit Frobenius* de $\mathbb{F}_q$ l'application qui à un élément $x \in \mathbb{F}_q$ associe l'élément x^p. Cette application définit alors une application Σ sur $W(\mathbb{F}_q)$ qui à tout élément $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ associe l'élément $(a_0^p, \ldots, a_n^p, \ldots)$ et qui est un homomorphisme d'anneaux.

Définition 8.2.1 *Σ défini comme précédemment est appelé le* petit Frobenius de $W(\mathbb{F}_q)$.

On remarque que Σ fixe les éléments de $W(\mathbb{F}_p)$.

On définit aussi l'application V appelée *décalage de $W(F_q)$* qui à tout élément $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$ associe l'élément $(0, a_0, \ldots, a_n, \ldots)$. Nous avons alors l'identité $\Sigma V = V\Sigma = [p]$.

8.2.2 L'anneau $\mathbb{Z}_q$

Algorithmiquement la réponse mathématique n'est pas satisfaisante. On va alors définir l'anneau “au-dessus” de $\mathbb{F}_q$ différemment. On verra par la suite que ces deux représentations sont en définitive isomorphes.

Définitions.

Soit $q = p^d$ où p premier. Soit $f(t)$ un polynôme unitaire dans $\mathbb{Z}_p[t]$ de degré d tel que le polynome $\pi(t)$ obtenu en projetant les coefficients de $f(t)$ est irréductible dans $\mathbb{F}_p[t]$.

Définition 8.2.2 *L'anneau $\mathbb{Z}_q$ est $\mathbb{Z}_p[t]$ modulo l'idéal engendré par $f(t)$.*

Un élément a de $\mathbb{Z}_q$ peut être représenté par un polynome $a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$ où $a_i \in \mathbb{Z}_p$. La somme et le produit dans $\mathbb{Z}_q$ sont définis comme une somme et un produit ordinaires de polynômes pris modulo $f(t)$. On remarque que $\mathbb{Z}_q$ contient $\mathbb{Z}_p$ comme sous-anneau (il suffit de poser $a_{d-1} = \ldots = a_2 = a_1 = 0$).

De plus, $\mathbb{Z}_q$ est un anneau de valuation discrète non ramifié. Son unique idéal premier non nul est $p\mathbb{Z}_q$ et le corps résiduel $\mathbb{Z}_q/p\mathbb{Z}_q$ est isomorphe à $\mathbb{F}_q$.

On étend la définition de π_n et de π à $\mathbb{Z}_q$ naturellement. À nouveau on peut considérer π comme étant la projection sur $\mathbb{F}_q$. Dans la suite, on utilisera la notation “mod p^n” à la place d'écrire explicitement modulo l'idéal $p^n\mathbb{Z}_q$. Les éléments inversibles de $\mathbb{Z}_q$ sont ceux tels que $\pi(x) \neq 0$. Pour de plus amples détails sur le sujet, voir [Ser68, Chapitre I et II].

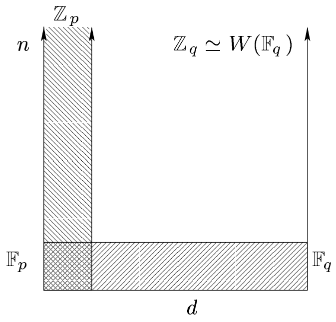
8.2.3 Relation entre $\mathbb{Z}_q$ et les vecteurs de Witt $W(\mathbb{F}_q)$.

Dans le paragraphe précédent, on faisait remarquer que $\mathbb{Z}_q$ est un anneau de valuation discrète non ramifié de corps résiduel $\mathbb{Z}_q/p\mathbb{Z}_q$ isomorphe à $\mathbb{F}_q$. En fait ces conditions caractérisent $\mathbb{Z}_q$; en particulier il est isomorphe à l'anneau $W(\mathbb{F}_q)$ des vecteurs de Witt. En effet, on a le théorème suivant :

Théorème 8.2.4 *Pour tout corps parfait K de caractéristique p, il existe un anneau de valuation discrète complet et un seul (à isomorphisme près) qui est non ramifié et admet K pour corps résiduel.*

En particulier, on a $W(\mathbb{F}_p) = \mathbb{Z}_p$.

On peut montrer cet isomorphisme à l'aide de la figure suivante.



Lorsque l'on se place dans $\mathbb{Z}_q$ on regarde les colonnes de cette figure alors que dans $W(\mathbb{F}_q)$, on considère cette fois-ci les lignes modulo certaines transformations.

Cependant la représentation des vecteurs de Witt n'est pas très pratique pour faire nos calculs. Il suffit de regarder la forme de l'addition 8.4 et celle de la multiplication 8.5 pour voir que les calculs dans $W(\mathbb{F}_q)$ sont bien plus compliqués que dans $\mathbb{Z}_q$.

8.3 Le Frobenius de $\mathbb{Z}_q$

Afin de pouvoir caractériser le petit Frobenius relevé $\Sigma : \mathbb{Z}_q \to \mathbb{Z}_q$, il nous faut rappeler quelques unes de ces propriétés. Tout d'abord Σ est un homomorphisme d'anneaux, de plus il fixe les éléments de $\mathbb{Z}_p$. La méthode suivante permet de le construire, mais s'en servir donne des calculs assez lents en pratique.

Soit $x \in \mathbb{Z}_q$ donc on peut écrire $x = \sum_{i=0}^{d-1} x_i t^i$. Alors

$$\begin{aligned}\Sigma(x) &= \Sigma(\sum_{i=0}^{d-1} x_i t^i)\\ &= \sum_{i=0}^{d-1} \Sigma(x_i t^i)\\ &= \sum_{i=0}^{d-1} x_i \Sigma(t)^i.\end{aligned}$$

D'après les propriétés du Frobenius, $\Sigma(t)$ est l'unique élément de $\mathbb{Z}_q$ tel que $\Sigma(t) \equiv t^p \bmod p$ et $\Sigma(t)$ est une racine de $f(X) \in \mathbb{Z}_p[X]$ où $f(X)$ est le polynôme irréductible qui nous permet de définir $\mathbb{Z}_q$.

8.4 Itération de Newton

De nombreux algorithmes décrits dans cette partie sont fondés sur l'itération de Newton. Il paraît donc nécessaire de la présenter ici.

Soit R un anneau p-adique arbitraire. L'*itération de Newton* suivante nous permet d'améliorer une approximation d'une racine d'un polynôme. Intuitivement, étant donnée une bonne approximation d'une racine on peut calculer de manière efficace une approximation meilleure, avec environ une précision doublée.

Il est nécessaire d'être très prudent lorsque l'on parle de précision. On écrit que $p^k \mid x$ lorsque $x \equiv 0 \bmod p^k$. Dans ce cas, $p^{-k}x$ est un élément de R. De même on écrit $p^k \parallel x$ quand $p^k \mid x$ mais $p^{k+1} \nmid x$. Dans ce cas, $p^{-k}x$ est un élément inversible de R.

Soit $x \in R$ et $f \in R[t]$. Soit k tel que $p^k \parallel f'(x)$ et supposons que $p^{n+k} \mid f(x)$ pour un $n > k$. Sous ces conditions, on dira que x est une racine approximée de f connue à la précision n, c'est à dire qu'il existe une racine exacte y de f dans R telle que $x \equiv y \bmod p^n$.

On va tout d'abord démontrer un lemme qui montre comment une itération de Newton améliore une racine connue à une précision n en une racine connue à une précision $2n - k$.

Lemme 8.4.1 *(Convergence quadratique d'une itération de Newton) Soit $x \in R$ et $f \in R[t]$. Soit k tel que $p^k \parallel f'(x)$ et on suppose que $p^{n+k} \mid f(x)$ pour un $n > k$. Soit :*

$$\Delta = \frac{p^{-k}f(x)}{p^{-k}f'(x)}$$

et $y = x - \Delta$. Alors $y \equiv x \bmod p^n$, $p^{2n} \mid f(y)$ et $p^k \parallel f'(y)$.

Démonstration: Il est clair que $p^n \mid \Delta$ donc $y \equiv x \bmod p^n$. Par le théorème des développements de Taylor,

$$f(y) = f(x) - \Delta f'(x) + \Delta^2\Psi(x),$$

où $\Psi(x)$ est un polynôme à coefficients dans R. Comme $p^{2n} \mid \Delta^2$, on a $f(y) \equiv f(x) - \Delta f'(x) \equiv 0 \bmod p^{2n}$.

Enfin comme $y \equiv x \bmod p^n$, on a $f'(x) \equiv f'(x) \bmod p^n$. Comme $p^k \parallel f'(x)$ et $n > k$ on a $p^k \parallel f'(y)$. □

En utilisant ce lemme de manière répétée, on obtient un algorithme qui permet de calculer une racine d'un polynôme quelle que soit la précision désirée.

Procédure ITERATIONSDENEWTON
Entrées :
- Un polynôme $f \in R[t]$,
- Une approximation initiale $x_0 \in R$ et un entier k où $p^k \parallel f'(x_0)$ et $p^{2k+1} \mid f(x_0)$.
- La précision désirée n.

Sortie : Une racine approximée $x \in R$ où $x \equiv x_0 \mod p^{k+1}$ et $p^{n+k} \mid f(x)$.

1. SI $n \leqslant k+1$ ALORS $y \leftarrow x_0$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n+k}{2} \rceil$;
3. $x \leftarrow$ ITERATIONSDENEWTON(f, x_0, k, n') ;
4. $y \leftarrow x - \frac{p^{-k}f(x)}{p^{-k}f'(x)}$;
5. RETURN y.

Pour une implantation efficace, il est important de travailler avec la plus petite précision possible à chaque étape de l'algorithme. En particulier, il faudrait réduire la précision de l'itération de Newton à chaque appel récursif. La profondeur de la récursion nécessaire pour atteindre la précision désirée n est $\log n$, donc si toutes les opérations étaient réalisées à précision n alors le temps total nécessaire serait de $O(M(n).\log(n))$ où $M(n)$ est le temps nécessaire pour effectuer une multiplication. Si l'on fait la première itération à précision n, le premier appel récursif à, à peu près, la moitie de la précision, le deuxième appel recursif à un quart de la précision et ainsi de suite le temps nécessaire total est réduit à $O(M(n))$.

De plus, quand on calcule la racine améliorée $y = x - f/f'$ dans une itération de Newton, il est possible de réduire la précision de certains calculs à peu près de moitié. Les précisions les plus faibles nécessaires sont indiquées dans la suite. On écrit $x + O(p^n)$ pour parler de tout $y \equiv x \bmod p^n$. Par exemple $xy + O(p^n)$ peut être compris comme étant le produit xy calculé à la précision n.

Quand un élément $a \in R$ est connu à la précision n alors le produit $p^k a$ est connu à la précision $n+k$, dans le sens que $p^k(a+O(p^n)) = p^k a + O(p^{n+k})$. Inversement quand a est connu à la précision n et satisfait $p^k \mid a$, où $k \leqslant n$, alors $p^{-k}a$ est connu à la précision $n-k$. En pratique, la division et la multiplication par p^k sont des opérations rapides, e.g. des décallages à droite et à gauche quand $p=2$.

On peut maintenant calculer l'itération de Newton comme $y = x - \Delta + O(p^{2n-k})$ où :

$$\Delta = \left(\frac{(f(x)+O(p^{2n})) \cdot p^{-n-k} + O(p^{n-k})}{(f'(x)+O(p^n)) \cdot p^{-k} + O(p^{n-k})} + O(p^{n-k}) \right) \cdot p^n + O(p^{2n-k}).$$

8.5 Calculs dans $\mathbb{Z}_p$ et dans $\mathbb{Z}_q$

Pour effectuer des calculs on considère les entiers p-adiques à une certaine précision n. Ce qui est équivalent à dire qu'on représente un élément $a \in \mathbb{Z}_p$ par une approximation $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ et les opérations dans l'anneau sont calculées modulo p^n.

L'inverse d'un élément inversible $a \in \mathbb{Z}_p$ peut être calculé par une itération de Newton simple $x \leftarrow x - x(ax-1)$, initialisé par l'inverse $1/\pi(a)$ pris dans $\mathbb{F}_p$.

De manière similaire, pour représenter $a = a_{d-1}t^{d-1} + \cdots + a_0 \in \mathbb{Z}_q$ à une précision n donnée, on peut garder en mémoire la suite $(\pi_n(a_{d-1}), \ldots, \pi_n(a_0))$. L'espace mémoire requis est $s = O(nd\log p)$ et le temps nécessaire pour effectuer une addition ou une soustraction de deux éléments est en $O(s)$. Le polynôme $f(t)$ peut être choisi creux et avec des coefficients simples, ainsi la réduction modulo $f(t)$ ne coûtera que quelques additions et quelques soustractions. Une multiplication utilisant une arithmétique polynomiale naïve prendrait $O(s^2)$ alors que si l'on se sert de l'algorithme de Karatsuba, pour la dimension p-adique et pour la dimension polynomiale, le coût d'une multiplication est réduit à $O(s^{\log 3/\log 2})$.

On peut aussi utiliser les algorithmes de multiplication rapide mais plutôt que de les utiliser indépendamment pour chaque dimension, une meilleure méthode asymptotique est de mettre tous les coefficients dans un grand entier et après d'utiliser un algorithme rapide pour la multiplication d'entiers. Chaque coefficient devrait être intercalé avec des bits zéros afin de remplir un champs de taille $\lceil 2n\log_2 p + \log_2 d \rceil$ bits, ainsi les coefficients du polynôme produit peuvent être récupérés à partir de certains champs dans l'entier produit. L'arithmétique avec une précision moindre que $O(\log d)$ prend un temps négligeable donc on peut supposer que la taille ℓ des entiers résultant est $\Theta(nd\log p)$. L'algorithme le plus rapide pour multiplier de grands entiers est celui de Schönhage [SS71] qui a pour complexité de temps $O(\ell.\log \ell.\log\log \ell)$ pour ℓ bits. Par la suite $n = O(d)$ donc la multiplication peut être faite en $O(nd\log d\log\log d)$ pour p fixé.

Comme on l'a vu précédemment dans le cas de $\mathbb{Z}_p$, on peut obtenir l'inverse d'un élément inversible $a \in \mathbb{Z}_q$ par une simple itération de Newton initialisée par $1/\pi(a)$ calculé dans $\mathbb{F}_q$. En variant la précision comme décrit dans la section suivante, une division prend un temps proportionnel à celui d'une multiplication.

Pour calculer le Frobenius tel que décrit il faut (après précalcul de $\Sigma(t)$) effectuer une évaluation de Hörner i.e. $O(d)$ multiplications dans $\mathbb{Z}_q$. Le précalcul est fondé sur un relèvement de Newton d'un polynôme de degré d donc dans ce cas aussi on nécessite $O(d)$ multiplications dans $\mathbb{Z}_q$.

Chapitre 9

Algorithme de Satoh et améliorations

Le calcul du nombre de points d'une courbe E jusqu'en 1999 était entièrement fondé sur l'idée initiale de Schoof [Sch85]. Ces travaux avaient été par la suite améliorés, on trouve une courte description de ces changements en 4.2. On travaillait toujours dans les sous-groupes de ℓ^n-division de notre courbe de départ où ℓ est un entier premier différent de la caractéristique du corps sur lequel on travaille. Satoh [Sat00] propose en 1999 une nouvelle approche qui travaille dans $E[p]$ où p est la caractéristique du corps et relève notre courbe dans Z_q.

Ce chapitre retranscrit les travaux réalisés en collaboration avec Pierrick Gaudry et Robert Harley [FGH00].

9.1 Les morphismes de Frobenius et le relèvement canonique

9.1.1 Les morphismes de Frobenius sur les courbes

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, où $q = p^d$. Pour déterminer la cardinalité de la courbe E, il suffit de déterminer la trace t de l'endomorphisme de Frobenius sur cette courbe. Le nombre de points de la courbe est alors donné par la formule $q+1-t$. D'après la borne de Hasse-Weil on a $|t| \leqslant 2\sqrt{q}$.

Le petit Frobenius σ sur $\mathbb{F}_q$ peut clairement être étendu à l'application pour laquelle l'image d'un point (x, y) de E est un point $(\sigma(x), \sigma(y))$ de la courbe conjuguée E^σ obtenue en appliquant σ aux coefficients de E et en fait cette application est une isogénie purement inséparable que nous appelerons aussi le petit Frobenius. De plus cette construction peut être réitérée ce qui donne une isogénie de E^σ à E^{σ^2} et ainsi de suite. En répétant cette construction d fois on obtient un cycle d'isogénies qui revient sur la courbe initiale E. Si l'on note E_0 la courbe E, E_{d-1} la courbe E^σ, σ_{d-1} l'isogénie entre ces deux courbees et ainsi de suite on peut dessiner le graphe suivant :

$$E_0 \xrightarrow{\sigma_{d-1}} E_{d-1} \xrightarrow{\sigma_{d-2}} \cdots \xrightarrow{\sigma_1} E_1 \xrightarrow{\sigma_0} E_0$$

En composant toutes ces isogénies on obtient :

Définition 9.1.1 *Le morphisme de Frobenius sur E* [4] *est l'endomorphisme $F = \sigma_0 \circ \sigma_1 \circ \ldots \circ \sigma_{d-1}$.*

Bien sûr l'action de F est trivial sur $\mathbb{F}_q$ mais ne l'est plus dans les extensions de corps.

De manière similaire, si l'on a une courbe $\mathcal{E}$ sur $\mathbb{Z}_q$, le petit Frobenius Σ sur $\mathbb{Z}_q$ peut être étendu à une application entre $\mathcal{E}$ et sa ccourbe conjuguée $\mathcal{E}^\Sigma$. En réitérant cette opération d fois on revient à la courbe initiale et cela nous donne un autre cycle d'isogénies.

[4] Pour des raisons d'uniformité avec les différents travaux concernant cet algorithme, dans toute cette partie nous noterons F le Frobenius au lieu de le noter π comme précédemment.

9.1.2 Relèvement canonique de courbes

Le théorème suivant dû à Lubin, Serre et Tate [LST64] nous permet de relever une courbe E sur $\mathbb{F}_q$ en une courbe $\mathcal{E}$ sur $\mathbb{Z}_q$ canoniquement en relevant son j-invariant. La courbe $\mathcal{E}$ est l'unique relèvement de E qui conserve son anneau d'endomorphismes.

Théorème 9.1.1 *Soit E une courbe sur $\mathbb{F}_q$ qui a pour j-invariant $j \in \mathbb{F}_q/\mathbb{F}_{p^2}$, alors il existe un unique J dans $\mathbb{Z}_q$ tel que*

$$\Phi_p(J, \Sigma(J)) = 0 \text{ et } J \equiv j \mod p.$$

et J est le j-invariant du relèvement canonique $\mathcal{E}$ de E (défini à isomorphisme près).

Il est possible d'implanter ce théorème directement mais l'algorithme qui en résulte est plutôt lent à cause des calculs de Σ. Une méthode bien plus rapide est donné dans les sections suivantes. Dans tous les cas on obtient :

$$\begin{tikzcd}
\mathcal{E}_0 \arrow[r, "\Sigma_{d-1}"] \arrow[d, "\pi"] & \mathcal{E}_{d-1} \arrow[r, "\Sigma_{d-2}"] \arrow[d, "\pi"] & \cdots \arrow[r, "\Sigma_1"] & \mathcal{E}_1 \arrow[r, "\Sigma_0"] \arrow[d, "\pi"] & \mathcal{E}_0 \\
E_0 \arrow[r, "\sigma_{d-1}"] & E_{d-1} \arrow[r, "\sigma_{d-2}"] & \cdots \arrow[r, "\sigma_1"] & E_1 \arrow[r, "\sigma_0"] & E_0
\end{tikzcd}$$

Si l'on considère le cycle entièrement on obtient l'endomorphisme $\mathcal{F}$ qui est le relèvement de F :

$$\begin{tikzcd}
\mathcal{E} \arrow[r, "\mathcal{F}"] \arrow[d, "\pi"] & \mathcal{E} \arrow[d, "\pi"] \\
E \arrow[r, "F"] & E
\end{tikzcd}$$

L'isogénie duale du petit Frobenius σ est une isogénie séparable $\hat{\sigma}$ appelée le *Verschiebung*. En suivant l'idée de Satoh on va travailler avec les isogénies duales puisque, étant séparables, on peut les manipuler facilement via leur noyau. En considérant les isogénies duales, on parcourt le même cycle mais dans le sens inverse :

$$\begin{tikzcd}
\mathcal{E}_0 \arrow[r, "\hat{\Sigma}_0"] \arrow[d, "\pi"] & \mathcal{E}_1 \arrow[r, "\hat{\Sigma}_1"] \arrow[d, "\pi"] & \cdots \arrow[r, "\hat{\Sigma}_{d-2}"] & \mathcal{E}_{d-1} \arrow[r, "\hat{\Sigma}_{d-1}"] \arrow[d, "\pi"] & \mathcal{E}_0 \\
E_0 \arrow[r, "\hat{\sigma}_0"] & E_1 \arrow[r, "\hat{\sigma}_1"] & \cdots \arrow[r, "\hat{\sigma}_{d-2}"] & E_{d-1} \arrow[r, "\hat{\sigma}_{d-1}"] & E_0
\end{tikzcd}$$

On obtient ainsi aussi le dual de l'endomorphisme de Frobenius $\hat{F} = \hat{\sigma}_{d-1} \circ \hat{\sigma}_{d-2} \circ \cdots \circ \hat{\sigma}_0$ et son relèvement $\hat{\mathcal{F}}$.

$$\begin{tikzcd}
\mathcal{E} \arrow[r, "\hat{\mathcal{F}}"] \arrow[d, "\pi"] & \mathcal{E} \arrow[d, "\pi"] \\
E \arrow[r, "\hat{F}"] & E
\end{tikzcd}$$

9.1.3 L'algorithme de Satoh

L'algorithme de Satoh se décompose en deux phases : la première consiste au relèvement du cycle d'isogénies et de courbes sur $\mathbb{Z}_q$ à une précision suffisante et la seconde est le calcul de la trace du Frobenius à l'aide de toutes ces données. On présente ici une idée d'ensemble de tout l'algorithme.

Procédure AlgorithmeDeSatoh
Entrée : Une courbe elliptique E définie sur $\mathbb{F}_q$ qui a pour j-invariant $j \notin \mathbb{F}_{p^2}$.
Sortie : La trace du Frobenius sur E.

1. Calcul du cycle des d courbes E_i et leurs j-invariants j_i ;
2. Relèvement des j-invariants, des coefficients des courbes et de leurs sous-groupes de p-torsion ;
3. Calcul de la trace dans $\mathbb{Z}_q$.

Relèvement

En suivant l'idée de Satoh, on va construire un cycle de j-invariants, en se servant du petit Frobenius σ dans $\mathbb{F}_q$, et après les relever tous simultanément en utilisant une itération multivariée de Newton. De cette manière on obtient tous les j-invariants conjugués J dans $\mathbb{Z}_q$ sans avoir à calculer à aucun moment le Frobenius Σ dans $\mathbb{Z}_q$. Une fois fait, on peut relever les courbes une par une en relevant leurs coefficients en utilisant une itération (univariée) de Newton.

Les isogénies $\hat{\sigma}_i$ et $\hat{\Sigma}_i$ sont séparable de degré p, elles sont donc déterminées par leurs noyaux qui sont d'ordre p. Par conséquent relever $\hat{\sigma}_i$ vers $\hat{\Sigma}_i$ s'effectue en relevant un sous-groupe de p-torsion de la courbe.

On peut relever chaque sous-groupe de p-torsion soit en relevant un unique point en utilisant une itération de Newton quand $p = 2$ et $p = 3$ soit en relevant un facteur du polynôme de p-division à l'aide d'un relèvement de Hensel quand $p \geqslant 5$.

Le squelette de la première phase est :

Procédure RELÈVEMENTDESATOH

Entrée : Un cycle de courbes elliptique E_i définies sur $\mathbb{F}_q$.

Sortie : Un cycle de courbes elliptiques définies sur $\mathbb{Z}_q$: $\mathcal{E}_0 \to \mathcal{E}_1 \to \cdots \to \mathcal{E}_{d-1} \to \mathcal{E}_0$ et leur sous-groupe de p-torsion.

1. Calcul du cycle de d courbes E_i et de leur j-invariant j_i ;
2. Relèvement de tous les j_i simultanément, ce qui nous donnee les J_i ;
3. Relèvement de chaque courbe en relevant ses coefficients ;
4. Relèvement d'un sous-groupe de p-torsion pour chaque courbe.

Calcul de la trace

Le but de cet algorithme est de calculer la trace de l'endomorphisme de Frobenius $F : E \to E$. On suppose que l'on a calculé (une bonne approximation de) la courbe $\mathcal{E}$ qui est le relèvement canonique de E et qui a la propriété $\operatorname{Tr} F = \operatorname{Tr} \mathcal{F}$ où $\mathcal{F}$ est le Frobenius sur $\mathbb{Z}_q$. La trace d'un endomorphisme est égale à celle de l'endomorphisme dual. Donc au lieu de travailler avec le Frobenius, on peut se permettre d'étudier sa duale $\hat{F}$:

$$\operatorname{Tr} F = \operatorname{Tr} \mathcal{F} = \operatorname{Tr} \hat{\mathcal{F}}.$$

D'après la définition 9.1.1, on peut décomposer le Frobenius F en un produit de petits Frobenius qui parcourt le cycle de d courbes conjuguées à E, cette décomposition est similaire pour les duaux. Donc

$$\operatorname{Tr} F = \operatorname{Tr} \left(\hat{\Sigma}_{d-1} \circ \hat{\Sigma}_{d-2} \circ \cdots \circ \hat{\Sigma}_0 \right).$$

L'étape suivante est de passer dans les groupes formelles de la courbe $\mathcal{E}$ et de ses conjugués. On note τ le paramètre local $-X/Y$ de $\mathcal{E}$ et τ_i le paramètre local de $\mathcal{E}_i$. En exprimant l'action de $\hat{\mathcal{F}}$ sur ce paramètre, on obtient la forme

$$\hat{\mathcal{F}}(\tau) = \sum_{k \geqslant 1} c_k \tau^k,$$

et la proposition 4.1. de [Sat00] prouve que

$$\operatorname{Tr} F = \operatorname{Tr}(\hat{\mathcal{F}}(\tau)) = c_1 + \frac{q}{c_1}.$$

Par conséquent le calcul du premier coefficient c_1 est suffisant pour résoudre le problème. L'idée clé de l'algorithme du calcul de la trace réside dans le fait que, puisque $\hat{\mathcal{F}}$ est une composition de morphismes, il est possible de calculer c_1 comme le produit des premiers coefficients des développements des facteurs de $\hat{\mathcal{F}}$ dans les groupes formels. Plus précisément, on peut écrire $\hat{\Sigma}_i : \mathcal{E}_i \to \mathcal{E}_{i+1}$ sur les groupes formels comme

$$\hat{\Sigma}_i(\tau_i) = g_i\tau_i + O(\tau_i^2).$$

On a alors

$$c_1 = \prod_{0 \leqslant i < d} g_i,$$

et

$$\operatorname{Tr} F \equiv \prod_{0 \leqslant i < d} g_i \mod q. \tag{9.1}$$

Remarquez que le produit des g_i est une expression de la norme de $\mathbb{Z}_q$ sur $\mathbb{Z}_p$ de g_0 (et donc c'est certainement dans $\mathbb{Z}_p$). En plus c'est la trace de F à la précision $O(p^d)$, si l'on avait besoin d'une précision supérieure il serait nécessaire d'ajouter le terme $\frac{q}{c_1}$.

L'étape finale est de calculer les g_i à partir des courbes $\mathcal{E}_i$ et $\mathcal{E}_{i+1}$ et du noyau de $\hat{\Sigma}_i$. On obtient le résultat désiré en se servant des formules de Vélu. Finalement, g_i peut être exprimé comme une fraction rationnelle en fonction des données que nous avons relevées, et en les multipliant nous donne le résultat.

Complexité

Pour le corps $\mathbb{F}_q$, on travaille avec une extension algébrique de degré d à la précision p-adique $O(p^{O(d)})$ ainsi chaque élément de $\mathbb{Z}_q$ occupe $O(d^2 \log p)$ en mémoire. Pour chaque courbe on a besoin de conserver $O(1)$ tels éléments et il y a d courbes conjuguées ; donc l'espace mémoire total requis est $O(d^3 \log p)$. De manière remarquable la complexité en temps est juste $O(d^{3+\epsilon})$ avec une arithmétique rapide (ou $O(d^5)$ avec une arithmétique naïve), pour p fixé. L'algorithme est aussi bien plus simple à implanter qu'une version optimisée de l'algorithme SEA et même avec une arithmétique simple de Karatsuba, l'exposant de la complexité en temps est un respectable $1 + 2\frac{\log 3}{\log 2} \simeq 4.17$.

Satoh a prouvé le théorème suivant pour $p \geqslant 5$ et nous l'avons étendu au cas où $p = 2$ et $p = 3$.

Théorème 9.1.2 (Satoh) *Soit E une courbe elliptique définie sur le corps fini à $q = p^d$ éléments. Supposons que que $j(E) \notin \mathbb{F}_{p^2}$. Alors il existe un algorithme déterministe pour calculer l'ordre de E qui, pour p fixé, nécessite $O(d^3)$ espace mémoire et $O(d^{3+\epsilon})$ bits-opérations.*

On remarque que la restriction $j \notin \mathbb{F}_{p^2}$ n'est pas essentiel étant donné que on peut s'occuper du cas où $j \in \mathbb{F}_{p^2}$ si p est petit en un temps polynômial en utilisant un algorithme naïf.

9.2 Algorithmes de relèvement

9.2.1 Relèvement du cycle de courbes

Le théorème de Lubin, Serre et Tate nous assure que le cycle que l'on désire construire est caractérisé par $\Phi_p(J_i, J_{i+1}) = 0$ pour tou $0 \leqslant i < d$ (pour faciliter la notation, les indices sont compris comme étant pris modulo d). L'algorithme pour calculer ce cycle à partir du cycle des j_i est une itération de Newton fondé sur la fonction suivante qui agit sur un vecteur de taille d :

$$\Theta(x_0, \dots, x_{d-1}) = (\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \cdots, \Phi_p(x_{d-1}, x_0)) .$$

L'algorithme de Newton présenté à la section 8.4 peut être adapté à ce cas multivarié assez facilement. Au lieu de considérer la dérivée de la fonction, il est maintenant nécessaire de travailler avec la matrice Jacobienne

$$D\Theta(x_0, \dots, x_{d-1}) = \begin{pmatrix} \Phi'_p(x_0, x_1) & \Phi'_p(x_1, x_0) & 0 & \dots & 0 \\ 0 & \Phi'_p(x_1, x_2) & \Phi'_p(x_2, x_1) & & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \Phi'_p(x_{d-1}, x_{d-2}) \\ \Phi'_p(x_0, x_{d-1}) & 0 & 0 & \dots & \Phi'_p(x_{d-1}, x_0) \end{pmatrix}$$

où $\Phi'_p(X, Y)$ est la dérivée partielle de $\Phi_p(X, Y)$ par rapport à X et l'itération est essentiellement

$$(x_0, \dots, x_{d-1}) \leftarrow (x_0, \dots, x_{d-1}) - \left((D\Theta)^{-1}\Theta\right)(x_0, \dots, x_{d-1}).$$

Nous présentons ici un algorithme détaillé (prêt à l'implantation) qui fait attention à deux choses importantes : les problèmes liés à la précision que nous voulons au final et l'inversion de la matrice Jacobienne.

Si les calculs sont bien organisés, l'inversion peut être faite en un nombre linéaire (en d) d'opérations arithmétiques. Les éléments de la diagonale sont tous inversibles donc nous pouvons faire l'élimination sans avoir à chercher un pivot. De plus tous les éléments en dehors de la diagonale sont tous divisibles par p.

En faisant des opérations sur les lignes sur la matrice dérivée (et simultanément sur Θ) on déplace l'élément en bas à gauche $\Phi'_p(x_0, x_{d-1})$ vers la droite. À la n-ième étape il est divisible par p^n, il devient ainsi rapidement zéro en fonction de la précision. Ensuite la matrice a une forme simple facilement résoluble.

Procédure RELEVERJINVARIANTS
Entrées : Une précision désirée n et un cycle $j_i \in \mathbb{F}_q \setminus \mathbb{F}_{p^2}$ tel que $\Phi_p(j_i, j_{i+1}) \equiv 0 \mod p$ pour tout $i \in \mathbb{Z}$ tel que $0 \leqslant i < d$.
Sortie : Un cycle $J_i \in \mathbb{Z}_q$ tel que $\pi(J_i) = j_i$ et $\Phi_p(J_i, J_{i+1}) \equiv 0 \mod p^n$ pour tout $0 \leqslant i < d$.

1. SI $n = 1$ ALORS on choisit arbitrairement J_i t.q. $\pi(J_i) = j_i$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n}{2} \rceil$;
3. $(J_0, J_1, \dots, J_{d-1}) \leftarrow$ RELEVERJINVARIANTS$((j_0, j_1, \dots, j_{d-1}), n')$;
4. $(J_0, J_1, \dots, J_{d-1}) \leftarrow$ METTREAJOURJS$((J_0, J_1, \dots, J_{d-1}), n)$;
5. RETURN $(J_0, J_1, \dots, J_{d-1})$.

Procédure METTREAJOURJS
Entrées : Une précision désirée n et un cycle $J_i \in \mathbb{Z}_q$ tel que $\Phi_p(J_i, J_{i+1}) \equiv 0 \mod p^{\lceil n/2 \rceil}$ pour

tout $0 \leqslant i < d$.

Sortie : Un cycle $\mathfrak{J}_i \in \mathbb{Z}_q$ tel que $\Phi_p(\mathfrak{J}_i, \mathfrak{J}_{i+1}) \equiv 0 \mod p^n$ et $\mathfrak{J}_i \equiv J_i \mod p^{\lceil n/2 \rceil}$ pour tout $0 \leqslant i < d$.

1. Allouer des tableaux $D[0..d-2]$, $P[0..d-2]$ et $\mathfrak{J}[0..d-1]$ d'éléments de $\mathbb{Z}_q$;
2. POUR $i = 0$ À $d-2$ FAIRE
   - $t \leftarrow 1/\Phi'(J_i, J_{i+1})$;
   - $D_i \leftarrow t \cdot \Phi'(J_{i+1}, J_i)$;
   - $P_i \leftarrow t \cdot \Phi(J_i, J_{i+1})$;
3. $m \leftarrow \Phi'(J_0, J_{d-1})$;
   $f \leftarrow \Phi(J_{d-1}, J_0)$;
4. POUR $i = 0$ À $d-2$
   - $f \leftarrow f - m \cdot P_i$;
   - $m \leftarrow -m \cdot D_i$;
   - IF $m \equiv 0 \mod p^n$ ALORS STOP ;
5. $m \leftarrow m + \Phi'(J_{d-1}, J_0)$;
6. $f \leftarrow f/m$;
7. POUR $i = 0$ À $d-2$ FAIRE
   - $P_i \leftarrow P_i - D_i \cdot P_{i+1}$;
8. POUR $i = 0$ À $d-2$ FAIRE
   - $\mathfrak{J}_i \leftarrow J_i - P_i$;
9. $\mathfrak{J}_{d-1} \leftarrow J_{d-1} - f$;
10. Liberer les tableaux D et P ;
11. RETURN $(\mathfrak{J}_0, \mathfrak{J}_1, \ldots, \mathfrak{J}_{d-1})$.

Dans la procédure MettreAJourJs il est possible de réduire de manière signifiquante l'espace mémoire utilisée. En effet, les tableaux P et D peuvent être évités en calculant leurs valeurs à la volée ; cela implique par contre que certains calculs soient répétés. Pour se faire la boucle 2 de l'algorithme doit être retirée et les valeurs D_i et P_i doivent être calculées à la volée dans la boucle 4. Les boucles 7 et 8 doivent être fusionnées et là aussi les valeurs D_i et P_i sont calculées à la volée. Quelques unes de ces valeurs auront déjà été calculées dans la boucle 4 mais on remarque que le test $m \equiv 0$ arrête la boucle après à peu près n itérations. En fait si l'on travaille à la moitié de la précision, comme décrit à la fin de la section 8.4 environ $n/2$ itérations seront suffisantes. Comme $n \approx d/2$, il n'y pas beaucoup de recalculs à faire.

9.2.2 Cas de la caractéristique $p \geqslant 5$ (Algorithme original de Satoh)

Relèvement de l'équation de courbe

Quand la caractéristique du corps fini considéré est au moins 5 (le cas de la caractéristique 2 est traité dans la section 9.2.3 et celui de la caractéristique 3 dans la section 9.2.4), on considère que la courbe elliptique E définie sur $\mathbb{F}_q$ a une équation de la forme $E : y^2 = x^3 + ax + b$. Dans ce cas, on veut relever E vers une courbe $\mathcal{E} : y^2 = x^3 + Ax + B$ sur $\mathbb{Z}_q$ ayant pour j-invariant celui déjà calculé précédemment. Pour se faire, on relève arbitrairement l'un des coefficients et on relève le second avec une itération de Newton fondé sur l'équation $J = -1728(4A)^3/\Delta$ où $\Delta = -16(4A^3 + 27B^2)$. Remarquez que les hypothèses $p \geqslant 5$ et $J \notin \mathbb{F}_{p^2}$ nous assurent que le dénominateur dans l'itération est non nul, la précision double exactement à chaque itération.

Procédure RELEVERAETB
Entrées : Un j-invariant J dans $\mathbb{Z}_q$, les coefficients a et b d'une courbe E sur $\mathbb{F}_q$ ayant pour j-invariant $\pi(J)$, et une précision désirée n.
Sortie : Les coefficients A et B dans $\mathbb{Z}_q$ d'une courbe $\mathcal{E}$ ayant pour j-invariant J, relevés à la précision n.

1. Choisir arbitrairement A tel que $\pi(A) = a$;
2. $B \leftarrow$RELEVERBSUIVANTA(J, A, b, n) ;
3. RETURN A, B.

Procédure RELEVERBSUIVANTA
Entrées : Un j-invariant J et un coefficient A dans $\mathbb{Z}_q$, un coefficient b dans $\mathbb{F}_q$, une précision désirée n.
Sortie : Un coefficient B dans $\mathbb{Z}_q$, relevé à la précision n.

1. SI $n = 1$ ALORS choisir un quelconque B tel que $\pi(B) = b$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n}{2} \rceil$;
3. $B \leftarrow$ RELEVERBSUIVANTA(J, A, b, n') ;
4. $B \leftarrow B - \frac{J(4A^3+27B^2)-6912A^3}{54\,J\,B}$; *(À la précision n)*
5. RETURN B.

Relèvement de la p-torsion

Relever le sous-groupe de p-torsion est l'étape la plus délicate de l'algorithme de Satoh. L'idée est de relever un facteur du polynôme de p-division $\Psi_p(x)$ de E_i par une sorte de relèvement quadratique de Hensel (ce qui ressemble à une itération de Newton). Cependant deux problèmes surgissent :

- Relever un facteur d'un polynôme n'est pas aussi simple que d'en relever une racine,
- La dérivée de $\Psi_p(x)$ est nul modulo p, il faut donc faire particulièrement attention aux précisions. En particulier c'est très important pour trouver la précision initiale requise.

L'algorithme qui effectue le relèvement de ce facteur est essentiellement donné dans le Lemme 2.1. de l'article de Satoh. Ce lemme est très technique et on ne donnera pas ici sa démonstration. On reformule uniquement le résultat avec nos notations.

Théorème 9.2.1 (Satoh) *Soit $\Psi(x)$ un polynôme sur un corps p-adique tel que $p \parallel \Psi'(x)$. Soit $h(x)$ un polynôme unitaire connu à la précision n tel que*
- *$\pi(h(x))$ n'a pas de carré et est premier à $\pi(p^{-1}\Psi'(x))$,*
- *$h(x)$ divise $\Psi(x)$ à la précision $n+1$.*

On définit un nouveau polynôme

$$\mathfrak{h}(x) = h(x) + \left(\frac{\Psi(x)}{\Psi'(x)}h'(x) \mod h(x)\right).$$

Alors $\mathfrak{h}(x)$ a les propriétés suivantes
- *$\mathfrak{h}(x) \equiv h(x)$ modulo p^n,*
- *$\mathfrak{h}(x)$ divise $\Psi(x)$ à la précision $2n+1$.*

On remarque de plus que si $n \geqslant 1$, alors $\pi(h(x)) = \pi(\mathfrak{h}(x))$, et la méthode peut être répétée.

Pour transformer ce théorème en un algorithme, il ne nous reste plus qu'à initialiser l'itération. Pour cela, on a besoin d'une manière de construire la première approximation pour le facteur $H(x)$ de $\Psi_p(x)$. Satoh propose de prendre la racine p-ième du polynôme de p-division de la courbe E_i, ce qui est facile à obtenir puisque toutes les informations nécessaires sont le polynôme de p-division de la courbe E_{i+1}.

On obtient l'algorithme suivant :

Procédure RELEVERH
Entrées : Une courbe elliptique E_{i+1} sur $\mathbb{F}_q$, une courbe elliptique $\mathcal{E}_i$ sur $\mathbb{Z}_q$ et une précision désirée n.
Sortie : Un facteur unitaire $H(x)$ du polynôme de p-division de $\mathcal{E}_i$, représentant le noyau de $\hat{\Sigma}_i$.

1. $\Psi(x) \leftarrow$ le polynôme de p-division de $\mathcal{E}_i$; *(Car. 0 : son degré est $\frac{p^2-1}{2}$.)*
2. $\psi(x) \leftarrow$ le polynôme de p-division de E_{i+1} ;
   (Car. p : c'est la puissance p-ième d'un polynôme $h(x)$ de degré $\frac{p-1}{2}$.)
3. $H(x) \leftarrow 0$;
4. POUR $k = 0$ À $\frac{p-1}{2}$ FAIRE
   – $h(x) \leftarrow h(x) + \frac{u_k}{u_{(p-1)/2}} x^k$, où u_k est le coefficient de x^{pk} dans $\psi(x)$;
5. $H(x) \leftarrow$ RELEVERHBIS$(\Psi(x), h(x), n)$;
6. RETURN $H(x)$.

Procédure RELEVERHBIS
Entrées : Un polynôme $\Psi(x)$, une approximation $h(x)$, et une précision désirée n.
Sortie : Un facteur unitaire $H(x)$ de $\Psi(x)$ à la précision n.

1. SI $n = 1$ ALORS $H(x) \leftarrow h(x)$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n-1}{2} \rceil$;
3. $H(x) \leftarrow$ ReleverHbis$(\Psi(x), h(x), n')$;
4. $H(x) \leftarrow H(x) + \left(\frac{\Psi(x)}{\Psi'(x)} H'(x) \mod H(x) \right)$; *(À la précision n)*
5. RETURN H(x).

9.2.3 Cas de la caractéristique 2

Dans cette sous-section on traite en détail le cas de la caractéristique deux qui était juste suggéré dans [Sat00]. Satoh proposait une méthode avec un algorithme probabiliste de factorisation. On donnera ici une méthode déterministe.

Avant tout, étant donnée une courbe elliptique ordinaire E définie sur un corps fini de caractéristique deux, il est toujours possible de trouver une équation pour E ou pour sa tordue de la forme :

$$y^2 + xy = x^3 + a.$$

Nous pouvons nous restreindre à ce cas.

Relèvement de l'équation de la courbe

Notre algorithme pour relever l'équation de la courbe consiste en le relèvement de son coefficient a en utilisant une itération de Newton, afin d'obtenir le coefficient A dans l'équation

$y^2+xy = x^3+A$ de la courbe relevée $\mathcal{E}$. Comme $J = \frac{1}{\Delta}$, où $\Delta = -A-432A^2$ est le discriminant de la courbe, le polynôme dont nous voulons calculer la racine est $f(x) = 1 + J(x + 432x^2)$. L'approximation initiale de la racine est $-1/J \mod 16$.

Dans ce cas, la précision augmente à chaque pas de l'algorithme de n à $2n+4$. Soit x la racine approchée à la précision n. Soit e le terme d'erreur à la précision n i.e., $e = f(x)$. Soit y la valeur de l'approximation au pas suivant i.e., $y = x - e/e'$, où $e' = J(1+864x)$. Alors le terme d'erreur à ce pas est

$$\begin{aligned} f(y) &= 1 + J(y+432y^2) \\ &= 432J\frac{e^2}{e'^2} \end{aligned}$$

On a $e = O(2^n)$, $2 \nmid e'$ et $2^4 \parallel 432$. Par conséquent $f(y) = O(2^{2n+4})$.

Procédure RELEVERA
Entrées : Le j-invariant J d'une courbe $\mathcal{E}$ dans $\mathbb{Z}_q$ et une précision désirée n.
Sortie : Le coefficient A de la courbe relevée $\mathcal{E}$ dans $\mathbb{Z}_q$ à la précision n.

1. SI $n \leqslant 4$ ALORS $A \leftarrow -1/J$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n-4}{2} \rceil$;
3. $A \leftarrow$ RELEVERA$(J,\ n')$;
4. $A \leftarrow A - \frac{1+J(A+432A^2)}{J(1+864A)}$; *(À la précision n)*
5. RETURN A.

Une alternative possible à cet algorithme serait de relever les conjugués du coefficient a directement en se servant d'un polynôme modulaire pour a au lieu de l'habituel pour j.

Relèvement de la 2-torsion

Notre algorithme pour relever la 2-torsion est similaire. Dans ce cas, la fonction $f(x)$ provient de l'équation satisfaite par les abscisses des points de 2-torsion non triviaux sur la courbe $\mathcal{E}$, c'est à dire le polynôme de 2-torsion $4X^3+X^2+4A$. Une racine X de ce polynôme est nécessairement égale à $0 \mod 2$. En posant $X = 2Z$, on obtient le polynôme de division modifié suivant $8Z^3 + Z^2 + A$.

Dans ce cas on relève Z en se servant d'une itération de Newton fondée sur la fonction $f(x) = 8x^3 + x^2 + A$. L'approximation initiale de la racine est $1/\sqrt{J} \mod 8$. Obtenir $\sqrt{J}$ est immédiat puisque nous avons calculé le cycle des courbes relevées et puisque $J = j(\mathcal{E}_i)$, on a $\sqrt{J} = j(\mathcal{E}_{i+1})$. Cette astuce nous donne une manière de contourner le problème rencontré par Satoh puisque dans son article il proposait de factoriser le polynôme ce qui n'est pas déterministe.

Dans ce cas, la précision augmente à chaque pas de l'algorithme de n à $2n-2$. Soit x la valeur approchée à la précision n. Soit e le terme d'erreur à la précision n i.e., $e = f(x)$. Soit y la valeur approchée au pas suivant i.e., $y = x - e/e'$, où $e' = 2(12x^2+x)$. Le terme d'erreur à ce pas est alors

$$\begin{aligned} f(y) &= 8y^3 + y^2 + A \\ &= \frac{e^2}{e'^2}(24x+1) - 8\frac{e^3}{e'^3} \end{aligned}$$

On a $e = O(2^n)$ et $2 \parallel e'$. Par conséquent $f(y) = O(2^{\min(2n-2,3n)}) = O(2^{2n-2})$.

Procédure RELEVERZ
Entrées : Le j-invariant J, le coefficient A d'une courbe $\mathcal{E}$ dans $\mathbb{Z}_q$ et une précision désirée n.
Sortie : Le Z de la courbe relevée $\mathcal{E}$ dans $\mathbb{Z}_q$ à la précision n.

1. SI $n \leqslant 3$ ALORS $Z \leftarrow 1/\sqrt{J}$; GOTO 5 ;
2. $n' \leftarrow \lceil \frac{n+2}{2} \rceil$;
3. $Z \leftarrow$ RELEVERZ$(J,\ A,\ n')$;
4. $Z \leftarrow Z - \frac{8Z^3+Z^2+A}{2(12Z^2+Z)}$; *(À la précision n)*
5. RETURN Z.

9.2.4 Cas de la caractéristique trois

Les courbes en caractéristique trois, comme les courbes en caractéristique deux, ont une forme particulière qui amène certaines différences dans l'algorithme de Satoh. L'équation d'une courbe elliptique ordinaire en caractéristique trois est de la forme $y^2 = x^3 + a_2x^2 + a_6$ si son j-invariant est non nul et dans ce cas il est égal à $j = -a_2^3/a_6$.

Relèvement de l'équation de la courbe

La courbe relevée $\mathcal{E}$ est de la forme $y^2 = x^3 + A_2x^2 + A_6$ et son j-invariant est égal à $J = -256A_2^6/(4A_2^3A_6 + 27A_6^2)$.

Par conséquent, pour relever les coefficients de la courbe, on utilise presque les mêmes algorithmes que dans le cas de la caractéristique $p \geqslant 5$. C'est-à-dire, on relève d'abord le coefficient A_2 de manière arbitraire et ensuite on relève A_6 en utilisant une itération de Newton fondée sur $f(x) = J(A_2^3x + 27/4x^2) + 64A_2^6$ et en prenant comme approximation initiale de la racine $x_0 = a_6$.

Relèvement de la 3-torsion

Le polynôme de 3-division de $\mathcal{E}$ est $\Psi_3(x) = 3x^4+4A_2x^3+12A_6x+4A_2A_6$ alors que celui de E est $\psi_3(x) = a_2(x^3+a_6)$. On relève le sous-groupe de 3 en utilisant une itération de Newton fondée sur la fonction $\Psi_3(x)$. L'approximation initiale de la racine est $x_0 = -\sqrt[3]{A_6}$. Cette itération est valide puisque nous avons :

$$\begin{aligned}\Psi_3(x_0) &= -3A_6x_0 - 4A_2A_6 + 12A_6x_0 + 4A_2A_6 = 9A_6x_0\\ \Psi_3'(x_0) &= -12A_6 + 12A_2x_0^2 + 12A_6 = 12A_2x_0^2\end{aligned}$$

Donc $\Psi_3(x_0) \equiv 0 \mod 9$ et $\Psi_3'(x_0) \equiv 0 \mod 3$ mais pas $\mod 9$ (remarquez que $A_2 \neq 0$ et $A_6 \neq 0$).

9.3 Calcul de la trace

Les formules de Vélu nous donne des expressions simples pour le premier coefficient du petit Verschiebung entre $\mathcal{E}_i$ et $\mathcal{E}_{i+1}$. Le calcul de la trace demande juste de prendre le produit de toutes ces expressions. Dans cette section on rappelle la formule donnée par Satoh pour $p \geqslant 5$ et on en déduit de similaires pour le cas de la caractéristique deux et celui de la caractéristique trois.

9.3.1 Utilisation des formules de Vélu

Soit E une courbe elliptique, et soit F un sous-groupe fini de E. Alors E/F est isomorphe à une courbe elliptique. Comme présenté en 4.1.1, les formules données par Vélu [Vél71] donne l'équation *explicite* d'une courbe elliptique E' isomorphe à E/F, et aussi une formule *explicite* pour l'isogénie entre E et E'. De plus cette isogénie est telle que quand on l'écrit dans le groupe formel, son premier coefficient est 1.

Nous allons appliquer ces formules à notre problème. Nous avons deux courbes $\mathcal{E}_i$ et $\mathcal{E}_{i+1}$ et un sous-groupe de $\mathcal{E}_i$ et l'on cherche à connaître l'expression dans le groupe formel de l'isogénie entre $\mathcal{E}_i$ et $\mathcal{E}_{i+1}$ correspondant à ce noyau. La première étape est de calculer la courbe $\mathcal{E}_i'$ donnée par les formules de Vélu. Après on sait que $\mathcal{E}_i'$ et $\mathcal{E}_{i+1}$ sont isomorphes donc on peut calculer cet isomorphisme λ explicitement et son premier coefficient de son développement dans le groupe formel.

On a le diagramme suivant :

$$\begin{tikzcd}
\mathcal{E}_i \arrow[rr, "\hat{\Sigma}_i"] \arrow[dr] & & \mathcal{E}_{i+1} \\
& \mathcal{E}_i' \arrow[ur, "\lambda"] &
\end{tikzcd}$$

Donc g_i, le premier coefficient de l'isogénie $\hat{\Sigma}_i$ est égal au produit du premier coefficient de l'isogénie de Vélu (qui est égal à 1) et à celui de l'isomorphisme λ. Pour ce dernier il est plus simple de trouver son *carré* en fonction des équations des courbes.

9.3.2 Caractéristique $p \geqslant 5$ (Satoh)

Dans le cas de la caractéristique $p \geqslant 5$, on se reporte à l'article original de Satoh pour la preuve des formules. (Pour la caractéristique deux, cf. Section 9.3.3 et pour la caractéristique trois cf. Section 9.3.4). L'équation de $\mathcal{E}_i$ est de la forme

$$y^2 = x^3 + A_i x + B_i,$$

et celle de $\mathcal{E}_{i+1}$ est

$$y^2 = x^3 + A_{i+1} x + B_{i+1}.$$

Le noyau de $\hat{\Sigma}_i$ consiste en le point à l'infini de $\mathcal{E}_i$ et $p-1$ points finis dont les $\frac{p-1}{2}$ abscisses distinctes sont données par les racines du polynôme $H_i(x)$.

La courbe $\mathcal{E}_i'$ donnée par les formules de Vélu a pour équation $y^2 = x^3 + \alpha_i x + \beta_i$ avec

$$\begin{aligned}
\alpha_i &= (6-5p)A_i - 30(s_1^2 - 2s_2) \quad \text{et} \\
\beta_i &= (15-14p)B_i - 70(-s_1^3 + 3s_1 s_2 - 3s_3) + 42 A_i s_1,
\end{aligned}$$

où s_k est le coefficient de $x^{(p-1)/2-k}$ dans $H_i(x)$.

Une fois que l'on a l'équation de $\mathcal{E}_i'$, il est plutôt simple de calculer l'isomorphisme avec $\mathcal{E}_{i+1}$. On se rapporte au livre de Silverman [Sil86] pour la forme générale d'un isomorphisme entre deux courbes elliptiques. Dans ce cas, il a la forme $(x,y) \mapsto (g_i^2\, x,\, g_i^3\, y)$ où g_i est le terme que nous recherchons. En conséquence,

$$g_i^2 = \frac{\beta_i}{\alpha_i}\,\frac{A_{i+1}}{B_{i+1}}.$$

Donc l'algorithme pour calculer le carré de la trace est clair, et on décide entre les deux racines en vérifiant le signe de la trace en se servant de l'invariant de Hasse h_E défini comme étant la norme du coefficient de x^{p-1} dans le polynôme $(x^3+ax+b)^{(p-1)/2}$.

Procédure CalculTraceCaracP
Entrée : Une courbe elliptique E sur $\mathbb{F}_{p^d}$ donnée par son équation $y^2 = x^3+ax+b$, avec $j(E) \notin \mathbb{F}_{p^2}$.
Sortie : La trace de la courbe.

1. $n \leftarrow \lceil \log_p 4 + \frac{d}{2} \rceil$;
2. $(j_i)_{0\leqslant i<d}$, $(a_i)_{0\leqslant i<d}$, $(b_i)_{0\leqslant i<d} \leftarrow$ Conjugués de $j(E)$, de a, de b ;
3. $(J_i)_{0\leqslant i<d} \leftarrow$ ReleverJInvariants$((j_i), n)$;
4. $N \leftarrow 1$; $D \leftarrow 1$;
5. POUR $i=0$ À $d-1$ FAIRE
   - $A, B \leftarrow$ ReleverAEtB(J_i, a, b, n) ;
   - $H \leftarrow$ ReleverH$(a_{i+1}, b_{i+1}, A, B, n)$;
   - $s_1, s_2, s_3 \leftarrow$ coefficients de $x^{(p-1)/2-1}$, $x^{(p-1)/2-2}$, $x^{(p-1)/2-3}$ dans $H(x)$;
   - $\alpha \leftarrow (6-5p)A - 30(s_1^2 - 2s_2)$;
   - $\beta \leftarrow (15-14p)B - 70(-s_1^3 + 3s_1s_2 - 3s_3) + 42As_1$;
   - $N \leftarrow N\beta A$;
   - $D \leftarrow D\alpha B$;
6. $t \leftarrow \sqrt{N/D}$; *(À la précision n)*
7. $h_E \leftarrow$ invariant de Hasse de E.
8. SI $t \not\equiv h_E \mod p$ ALORS $t \leftarrow -t$;
9. Réduire t à un entier dans $0 \ldots p^n$. SI $t > 2\sqrt{q}$ ALORS $t \leftarrow t - p^n$;
10. RETURN t.

On remarque qu'au pas 6, le numérateur et le dénominateur sont dans $\mathbb{Z}_p$ et t aussi. La racine carrée p-adique peut être trouvée en utilisant une itération de Newton pour la racine carrée inverse et ensuite en multipliant par t. Il y a deux racines possibles, n'importe laquelle des deux fonctionne puisque l'étape 8 corrige son signe si nécessaire.

9.3.3 Cas de la caractéristique deux

L'équation de $\mathcal{E}_i$ est de la forme

$$y^2 + xy = x^3 + A_i,$$

et celle de $\mathcal{E}_{i+1}$ est

$$y^2 + xy = x^3 + A_{i+1}.$$

Dans le cas de la caractéristique deux, le sous-groupe de $\mathcal{E}_i$ qui est le noyau de $\hat{\Sigma}_i$ est d'ordre 2. Soit (X_i, Y_i) le point non-trivial de ce sous-groupe. Remarquez que connaître l'abscisse est suffisant puisque $Y_i = -\frac{X_i}{2}$.

La courbe $\mathcal{E}_i'$ donnée par les formules de Vélu a pour équation $y^2+xy = x^3 + \mathcal{A}_4 x + \mathcal{A}_6$ où

$$\mathcal{A}_4 = -5v \quad \text{et} \quad \mathcal{A}_6 = A_i - v - 7w,$$

avec

$$v = 3X_i^2 - Y_i \quad \text{et} \quad w = 7X_i^3 + X_i^2 - X_iY_i + 4A_i.$$

Là aussi, connaître l'équation de $\mathcal{E}'_i$ et celle de $\mathcal{E}_{i+1}$ nous permet de calculer l'isomorphisme et donc le coefficient g_i^2. Après translation des axes (ce qui n'affecte pas le premier coefficient du développement de l'isomorphisme dans le groupe formel), les équations sont les suivantes :

$$\begin{array}{lcrcl} \mathcal{E}_{i+1} & : & y^2 & = & x^3 - \frac{1}{48}x + \frac{1}{864} + A_{i+1} \\ \mathcal{E}'_i & : & y^2 & = & x^3 + \left(\mathcal{A}_4 - \frac{1}{48}\right)x + \frac{1}{864} + \mathcal{A}_6 - \frac{\mathcal{A}_4}{12}. \end{array}$$

Donc

$$g_i^2 = \frac{-\frac{1}{48}}{\frac{1}{864} + A_{i+1}} \cdot \frac{\frac{1}{864} + \mathcal{A}_6 - \frac{\mathcal{A}_4}{12}}{\mathcal{A}_4 - \frac{1}{48}},$$

ce qui se simplifie en

$$g_i^2 = -\frac{-72\mathcal{A}_4 + 1 + 864\mathcal{A}_6}{(48\mathcal{A}_4 - 1)(1 + 864A_{i+1})}.$$

On peut alors remplacer $\mathcal{A}_4$ et $\mathcal{A}_6$ par leur expression en fonction de A_i et X_i.

On obtient

$$g_i^2 = -\frac{42336X_i^3 + 10584X_i^2 + 252X_i - 1 + 23328A_i}{(720X_i^2 + 120X_i + 1)(1 + 864A_{i+1})}.$$

On peut encore simplifier cette formule en la réduisant modulo le polynôme minimal de X_i, qui est $4X_i^3 + X_i^2 + 4A_i$. On obtient

$$g_i^2 = \frac{1 - 252X_i + 19008A_i}{\left(1 + 120(X_i + 6X_i^2)\right)(1 + 864A_{i+1})}.$$

En se rappelant que nous avons relevé $Z_i = X_i/2$ au lieu de X_i et en considérant que nous avons un bit en plus de précision pour la racine carrée 2-adique, on a alors l'algorithme suivant.

Procédure CALCULTRACECARAC2
Entrée : Une courbe elliptique E sur $\mathbb{F}_{2^d}$ donnée par son coefficient a, avec $j(E) \notin \mathbb{F}_4$.
Sortie : La trace de la courbe.

1. $n \leftarrow \lceil \frac{d+6}{2} \rceil$;
2. $(j_i)_{0 \leqslant i < d} \leftarrow$ Conjugués de $j(E)$;
3. $(J_i)_{0 \leqslant i < d} \leftarrow$ RELEVERJINVARIANTS$((j_i), n)$;
4. $N \leftarrow 1$; $D \leftarrow 1$;
5. POUR $i = 0$ À $d - 1$ FAIRE
   - $A \leftarrow$ RELEVERA(J_i, n) ;
   - $Z \leftarrow$ RELEVERZ(J_i, A, n) ;
   - $A \leftarrow 864A$;
   - $N \leftarrow N(1 - 504Z + 22A)$;
   - $D \leftarrow D(1 + 240(Z + 12Z^2))(1 + A)$;
6. $t \leftarrow \sqrt{N/D}$; *(À la précision n)*
7. SI $t \not\equiv 1 \mod 4$ ALORS $t \leftarrow -t$;
8. Réduire t à un entier dans $0 \ldots 2^{n-1}$. SI $t > 2\sqrt{q}$ ALORS $t \leftarrow t - 2^{n-1}$;
9. RETURN t.

On remarque qu'à l'étape 6, le numérateur et le dénominateur sont dans $\mathbb{Z}_2$ et t aussi. La racine carrée 2-adique peut être trouvée via une itération de Newton pour l'inverse d'une racine carrée. Il y a quatre racines carrées possibles, mais seulement deux modulo 2^{n-1} et l'étape 7 corrige le signe si nécessaire.

9.3.4 Cas de la caractéristique trois

Pour le calcul de la trace, la méthode est la même que dans le cas de la caractéristique deux, mis à part le fait que l'on doit prendre en compte la forme de l'équation de la courbe et adapter les formules dde Vélu.

La courbe $\mathcal{E}_i$ a une équation de la forme

$$\mathcal{E}_i \;:\; y^2 = x^3 + A_i x^2 + B_i.$$

On note X_i l'abscisse du point de 3-torsion relevé. Les formules de Vélu nous donne alors l'équation suivante pour la courbe $\mathcal{E}_i'$:

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

où

$$a_2 = A_i, \quad a_4 = -5t, \quad a_6 = B_i - 4A_i t - 7w,$$

avec

$$t = 6X_i^2 + 4A_i X_i, \quad \text{et} \quad w = 10X_i^3 + 8A_i X_i^2 + 4B_i.$$

On transforme les équations de $\mathcal{E}_i'$ et de $\mathcal{E}_{i+1}$ par translation des axes pour obtenir

$$\begin{array}{rcrcl} \mathcal{E}_{i+1} & : & y & = & x^3 - \frac{1}{3}A_{i+1}^2 x + B_i + \frac{2}{27}A_{i+1}^3 \\ \mathcal{E}_i' & : & y & = & x^3 + \left(a_4 - \frac{1}{3}a_2^2\right)x + a_6 + \frac{2}{27}a_2^3 - \frac{1}{3}a_2 a_4 \end{array}$$

L'expression de g_i^2 suit facilement. Sa formule est :

$$g_i^2 = \frac{A_i'^2\left(-1890X_i^3 - 1890A_iX_i^2 - 252A_i^2X_i + 2A_i^3 - 729B_i\right)}{\left(2A_i'^3 + 27B_i'\right)\left(90X_i^2 + 60A_iX_i + A_i^2\right)}.$$

et finalement la trace est donnée par

$$\operatorname{Tr} F = \prod_{0 \leqslant i < d} g_i \mod q.$$

9.4 Exemples numériques

9.4.1 Un petit exemple

Dans cette partie nous donnons des valeurs intermédiaires qui sont calulées quand on lance l'algorithme de Satoh avec la courbe elliptique sur $\mathbb{F}_{2^{11}} = \mathbb{F}_2[X]/(X^{11} + X^2 + 1)$ définie par $y^2 + xy = x^3 + a$ avec $a = X^4 + X^2 + X$. Cet exemple est tiré de [LM00] où on s'en sert pour comparer les différents algorithmes pour calculer les isogénies.

Travailler à la précision $O(2^9)$ est suffisant pour calculer la trace. La première étape dans l'algorithme de Satoh est de relever le cycle de courbes. On donne ici la suite résultante des A_i relevés, à la précision $O(2^9)$.

$$\begin{array}{rcl}
A_0 & = & 158X^{10} + 140X^9 + 158X^8 + 230X^7 + 366X^6 + 116X^5 + 217X^4 + 382X^3 + 169X^2 + 391X + 108, \\
A_1 & = & 312X^{10} + 300X^9 + 71X^8 + 268X^7 + 178X^6 + 202X^5 + 19X^4 + 470X^3 + 459X^2 + 324X + 332, \\
A_2 & = & 454X^{10} + 12X^9 + 339X^8 + 113X^7 + 90X^6 + 193X^5 + 139X^4 + 402X^3 + 376X^2 + 286X + 236, \\
A_3 & = & 271X^{10} + 310X^9 + 163X^8 + 225X^7 + 454X^6 + 246X^5 + 316X^4 + 177X^3 + 144X^2 + 40X + 154, \\
A_4 & = & 322X^{10} + 75X^9 + 46X^8 + 251X^7 + 91X^6 + 358X^5 + 384X^4 + 53X^3 + 419X^2 + 52X + 241, \\
A_5 & = & 42X^{10} + 415X^9 + 90X^8 + 177X^7 + 79X^6 + 457X^5 + 491X^4 + 470X^3 + 342X^2 + 63X + 333, \\
A_6 & = & 167X^{10} + 85X^9 + 161X^8 + 43X^7 + 30X^6 + 217X^5 + 456X^4 + 290X^3 + 383X^2 + 229X + 63, \\
A_7 & = & 279X^{10} + 326X^9 + 470X^8 + 358X^7 + 402X^6 + 296X^5 + 157X^4 + 413X^3 + 226X^2 + 474X + 74, \\
A_8 & = & 120X^{10} + 365X^9 + 47X^8 + 206X^7 + 343X^6 + 370X^5 + 286X^4 + 302X^3 + 265X^2 + 336X + 199, \\
A_9 & = & 210X^{10} + 459X^9 + 378X^8 + 6X^7 + 110X^6 + 95X^5 + 17X^4 + 159X^3 + 272X^2 + 473X + 369, \\
A_{10} & = & 225X^{10} + 73X^9 + 125X^8 + 171X^7 + 417X^6 + 10X^5 + 78X^4 + 466X^3 + 17X^2 + 404X + 379.
\end{array}$$

Si nécessaire, les J_i peuvent être récupérés facilement avec la formule

$$J_i = -\frac{1}{A_i + 432A_i^2}.$$

Alors la moitié de l'abscisse des points de 2-torsion peut être relevée. On obtient les résultats suivants :

$$\begin{array}{rcl}
Z_0 & = & 359X^{10} + 263X^9 + 491X^8 + 125X^7 + 295X^6 + 6X^5 + 510X^4 + 86X^3 + 123X^2 + 352X + 117, \\
Z_1 & = & 226X^{10} + 420X^9 + 22X^8 + 170X^7 + 426X^6 + 292X^5 + 107X^4 + 330X^3 + 155X^2 + 265X + 292, \\
Z_2 & = & 240X^{10} + 100X^9 + 61X^8 + 70X^6 + 482X^5 + 369X^4 + 194X^3 + 213X^2 + 228X + 356, \\
Z_3 & = & 206X^{10} + 348X^9 + 465X^8 + 187X^7 + 174X^6 + 167X^5 + 197X^4 + 378X^3 + 232X^2 + 66X + 140, \\
Z_4 & = & 169X^{10} + 398X^9 + 133X^8 + 451X^7 + 318X^6 + 114X^5 + 100X^4 + 363X^3 + 116X^2 + 200X + 274, \\
Z_5 & = & 22X^{10} + 9X^9 + 234X^8 + 81X^7 + 313X^6 + 38X^5 + 228X^4 + 499X^3 + 133X^2 + 256X + 235, \\
Z_6 & = & 10X^{10} + 285X^9 + 82X^8 + 83X^7 + 505X^6 + 131X^5 + 21X^4 + 98X^3 + 62X^2 + 285X + 135, \\
Z_7 & = & 333X^{10} + 275X^9 + 263X^8 + 253X^7 + 26X^6 + 295X^5 + 500X^4 + 282X^3 + 345X^2 + 179X + 313, \\
Z_8 & = & 361X^{10} + 86X^9 + 62X^8 + 450X^7 + 418X^6 + 240X^5 + 75X^4 + 331X^3 + 266X^2 + 454X + 298, \\
Z_9 & = & 288X^{10} + 247X^9 + 73X^8 + 346X^7 + 273X^6 + 98X^5 + 366X^4 + 358X^3 + 439X^2 + 124X + 197, \\
Z_{10} & = & 346X^{10} + 129X^9 + 162X^8 + 414X^7 + 254X^6 + 185X^5 + 87X^4 + 153X^3 + 476X^2 + 151X + 147.
\end{array}$$

Le carré de la trace peut maintenant être calculé grâce à la formule :

$$t^2 = \frac{\prod_i (1 - 504Z_i + 19008A_i)}{\prod_i (1 + 240(Z_i + 12Z_i^2))(1 + 864A_i)} \equiv \frac{65}{129} \mod 512 \equiv 449 \mod 512.$$

Les deux racines carrées modulo 256 sont

$$t \equiv \pm 31 \mod 256,$$

et on choisit celle congruente à 1 modulo 4. Donc

$$t = -31.$$

9.4.2 De nouveaux records

Dans cette section, nous présentons les records que nous avions obtenu pour la caractéristique deux avec notre première implantation de l'algorithme. Ils ont depuis été battus par différentes implantations, mais représentent tout de même les premiers résultats obtenu avec cette méthode.

On représente les corps $\mathbb{F}_{2^d}$ pour $d = 2003$, 2503, 3001, 3511, 4001, 5003, 6007, 7001 et 8009 comme $\mathbb{F}_2[X]/(f(X))$ où f est le polynôme irréductible $X^{2003}+X^{12}+X^{10}+X^8+1$, $X^{2503}+X^{316}+1$, $X^{3001}+X^{975}+1$, $X^{3511}+X^{1141}+1$, $X^{4001}+X^{137}+1$, $X^{5003}+X^{18}+X^{16}+X^8+1$, $X^{6007}+X^{435}+1$, $X^{7001}+X^{1631}+1$ et $X^{8009}+X^{3159}+1$ respectivement.

Pour les corps de 2003 bits, 2503 bits, 3001 bits, 3511 bits et 4001 bits, soit E la courbe $y^2+xy = x^3+a$ où le coefficient a est :

`0x3F6576EA7220656A20F96F20736973616F276C207361702075742D7365274E`

ce qui correspond au code ASCII (ISO-8859-1) de la citation de Charles Baudelaire suivante :

N'es-tu pas l'oasis où je rêve ?

Les résultats que nous obtenons sont 2^d+1-t où :

d	t
2003	-54257716382449163322217965867619130414983986889031393504950 950274023567567915950050300483897958084268902717170259601749 275132829687119464101385043333372481793555545941317422170070 614774973636138071957047824575347543986113095686653298805813 2481864878669071309069011445043928366775143309774491815342764 15
2503	

(see correction below)

4001	80177251919375213193261956033994736597103479987285879213126779229998124645635997350713443221801494124679597962879601353149563605304969090722905778013218380455159252815609394183430501884092343715854897653812065968378998167795818332669775025471242918588076461110217915069806929966345724756739313913921549649218304511939473892507130103952955319780186267488478958909916316399436612052615768025750804995437396584580573502734408159103335730844509915511939253762122166415911083574594917926591069681653833543528814185123685606253156006996197604330750280736244961629710454938470970967466942969118418184438560705

Pour les corps de 5003 bits et 6007 bits, soit E la courbe $y^2 + xy = x^3 + a$ où le coefficient a est :

```
0x3F2065737365727669276C20746961206E6F27757120757672756F7020
2C6E6F63616C6620656C206574726F706D69277551203F20657373657274
EE616D20616C206574726F706D69277571202C746E696F7020646E617267
20656C207473652072656D6941202E6C69656C6F73207561206569762061
6C2074652072756F6D61276C202C74756F74207473652072756F6D61274C
```

ce qui correspond au code ASCII (ISO-8859-1) de la citation d'Alfred de Musset suivante :

L'amour est tout, l'amour et la vie au soleil.
Aimer est le grand point, qu'importe la maîtresse ?
Qu'importe le flacon, pourvu qu'on ait l'ivresse ?

Les résultats que nous obtenons sont $2^d + 1 - t$ où :

d	t
5003	-12734182923064800252301894383222693725210369465207679940892247761285528937720333277968830668283149327326976405477042429700613603598100188153437091590880037867183132923999681149769714896848348254458886092165205989332390122060361912880701782013926762209692683901776507703127960985164598128483220663153413380728800152684789019921321662881737609247282590283186866287033818802513632314727767766402202241891845855093283429411199385888870628208020779314136040773944417418869557393066077152081341137062591780876309752131614979471114816746937325909135993261402080320480272666653510918300147073590648602609106294024047130090799867896632902387389110488285751485154406317058265333490827141686023373558562360736861740574550504515673617506127095554076137907320675101 75

6007	3442061241831053996615832184729488073173960929415596873391624 0735074054386750995324726283712152853544174238412851376047070 8833119398328600011413068657966809197790402083599786447073895 7670892097869488100734744373625776913457011893379913446989775 9948146328306300644690018473496352595361381815087410129216348 6800454753434344865483117887437584475911403340275618360633469 6231378804501610228673410052580840098862304791612864276178562 3465183932446927985141947695864308965365832079922890622252441 3938585461377617126175689088978662090720513871209911870612646 2898948834053845355104577980983069522949252022515872310857412 6245720627861504154908945603509369314367877612679565045855007 9217430955154845364558025542982307460071763907044624173653064 9068697258585375195516895157040281805394439187185481758711498 9420593138961727685731114071309572168891196530781166053344563 9938870064211270693767042897900149946085199206561

Pour les corps de 7001 bits et 8009 bits, soit E la courbe $y^2 + xy = x^3 + a$ où le coefficient a est :

`0x3F636F64207075207327746168570`

ce qui correspond au code ASCII (ISO-8859-1) de la phrase de Bugs Bunny :

What's up doc ?

Les résultats que nous obtenons sont $2^d + 1 - t$ où :

d	t
7001	-581371373310534460112778003571913522920537044570507812766071 8250662124738792094539243327405833856928654524991608119042426 9820587241418605772914727331920107475316537894755087148567373 0967996250474412965784188133088012505743059546142132542704250 1629932666263555167348022048047267294187847087635155496091634 2015114299540309423356127723115310725723137130225445387222903 9207995763431245365186806999267459314058281699973113019652643 2687087941185720215715326693245353899060799921151318904540447 3504844815199599391092050732199028357086785246423505074138190 4965739448692663452746610614491278508031681354575958619186277 5226740342286968191763685776614604511244364034049534685257924 8707939797816040594991356325574740197885649990846063299054445 5441529706877442091824052857209486661754851767965943320080307 7079671022571234565541431726822737595043903717297883748966360 1823090240417077521645356540222923669323219342525668930924057 4509695883291712065992422967344009813656715459973153166333791 1112385166123289723881516583823493965719492507357848397233571 808377373646960699

8009	-17378149685594750502663500286963595380822933538157005646462 19394089505686350478329402199506511963606403774445812182470 56101375092227785899279859382375508813512228452707543448804 78303504536303182899934299550485448582714312355549259252180 02146297652260480619999262960763361539904566574812040349729 24818612705811737001932873239713976031333307121192031140124 67161102613442999923434626180947078833812395756923540626751 74312808492870478992705390275752742617858435029461809834041 92085330411964582201095084463986891949680756772569455776175 80984196275806202308814056970168378439117324900342195927360 38212331467792983817285353774705442794273977446148471220998 99476777494287080574838937079674483708654377667748782232512 90718854374337184606260246195457302298573358594529615914998 79473118032339677677469399798074962839080605378520850947719 67399825222359144733258976844620499589156331646085956322156 14932793087347196111480133304842922422068525558945631504290 33035718583585795982719859853933656740181710300520394197995 70708629753376721197597388299770441615351946293827847496574 97226247758645688520092102709152363954330048199824614925435 766219587259634877029770317456234950616362600955

Nous avons vérifié que ces résultats sont bien des multiples des ordres de nombreux points aléatoires de chaque courbe. Une vérification rigoureuse du nombre de points nécessiterait de factoriser complètement $q + 1 \pm t$ ce qui ne semble pas réalisable.

L'ensemble des temps de calculs est donné dans le tableau suivant.

Taille du corps	CPU	Temps de calcul	Mémoire utilisée	CPU fourni par
503	500 MHz Alpha EV6	6 mn		
1009	500 MHz Alpha EV6	1h		
1511	500 MHz Alpha EV6	5h		
2003	500 MHz Alpha EV6	14h		
2503	500 MHz Alpha EV6	40h	531 MB	
3001	667 MHz Alpha EV6	54h	932 MB	Paul Bourke (Swinburne University Astrophysics and Supercomputing)
3511	667 MHz Alpha EV6	97h	1.3 GB	Paul Bourke (Swinburne University Astrophysics and Supercomputing)
4001	750 MHz Alpha UP2000	132h	1.9 GB	Tom Morris (Alpha Processor Inc)
5003	750 MHz Alpha EV6	143h	4GB	Rajit Manohar (Cornell Computer Systems Lab.)
6007	750 MHz Alpha EV6	9 jours	7.1GB	Rajit Manohar (Cornell Computer Systems Lab.)
7001	667 MHz Alpha EV6	11 jours	11.3 GB	Pierrick Gaudry (LIX)
8009	750 MHz Alpha EV6	13 jours	16.9 GB	Rajit Manohar (Cornell Computer Systems Lab.)

Nous remercions particulièrement toutes les personnes qui nous ont procuré du temps CPU.

Chapitre 10

Améliorations de l'algorithme Satoh-FGH

Depuis la première implantation de l'algorithme Satoh-FGH en octobre 2000, de nombreuses améliorations ont été apportées à l'algorithme. Les améliorations ont porté sur le gain d'espace mémoire par Vercauteren, une nouvelle méthode de relèvement des courbes avec la moyenne arithmético-géométrique dont le principe est dû à Mestre et qui est développé par Harley et Gaudry, une nouvelle méthode pour calculer la norme d'un élément de $\mathbb{Z}_q$.

L'ensemble de ces algorithmes étant tous inspirés par l'algorithme de Satoh et son extension à la caractéristique 2 et 3 nous réutilisons les notations du chapitre précédent.

10.1 Première amélioration : Algorithme de Vercauteren

L'algorithme de Vercauteren a pour vocation de réduire la complexité en mémoire de l'algorithme de Satoh. En effet, l'un des freins à l'amélioration des records de calcul de cardinalité d'une courbe effectués avec l'algorithme de Satoh est l'espace mémoire nécessaire pour faire tourner l'algorithme. Vercauteren, Preneel et Vandewalle [VPV01] proposent une nouvelle version de l'algorithme de Satoh qui réduit la complexité en mémoire à $O(n^2)$ où n est tel que $q = p^n$ au lieu de $O(n^3)$.

La complexité en mémoire de l'algorithme original est dû au fait que l'on relève tout le cycle de j-invariants simultanément. Mais ce relèvement simultané est aussi la clé de l'efficacité de l'algorithme puisque cela nous permet de ne pas avoir à évaluer le petit Frobenius dans $\mathbb{Z}_q$. Vercauteren, Preneel et Vandewalle proposent de calculer le relèvement d'un unique j-invariant à la bonne précision sans n'avoir jamais à évaluer le petit Frobenius dans $\mathbb{Z}_q$ et ensuite d'obtenir le reste du cycle à partir d'itérations de Newton.

10.1.1 Relèvement d'un unique j-invariant à la précision n recherchée

Les j-invariants J_i et J_{i+1} satisfont les relations suivantes :

$$\Phi_p(J_i, J_{i+1}) = 0,\ J_i \equiv j_i \bmod p \text{ et } J_{i+1} \equiv j_{i+1} \bmod p.$$

Supposons que nous ayons réussi à relever le j-invariant J_{i+1} d'une courbe $\mathcal{E}_{i+1}$ à la précision n demandée i.e. $J_{i+1} \equiv j(\mathcal{E}_{i+1}) \bmod p^n$, alors il nous est possible de calculer J_i à la précision n en faisant une itération de Newton sur $\Phi_p(X, J_{i+1})$. Cette itération est donnée par :

$$J_i \leftarrow J_i - \frac{\Phi_p(J_i, J_{i+1})}{\Phi'_p(J_i, J_{i+1})} \tag{10.1}$$

où Φ'_p est encore la dérivée de Φ_p par rapport à X. L'approximation initiale de l'itération est $j_i \equiv j(\mathcal{E}_i) \bmod p$. Étant donné que l'équation modulaire satisfait la relation de Kronecker, $\Phi'_p(J_i, J_{i+1})$ est inversible dans $\mathbb{Z}_q$. On remarque que nous allons ainsi reconstruire le cycle mais "à l'envers" puisque $\frac{\partial \Phi_p}{\partial Y}(J_i, J_{i+1}) \equiv 0 \bmod p$. Il ne reste plus qu'à relever une courbe à la bonne précision. La proposition suivante nous donne la solution à ce problème.

Proposition 10.1.1 *Soit $\mathcal{K}$ une extension non-ramifiée de $\mathbb{Q}_p$ et soit $\mathbb{Z}_q$ son anneau de valuation. Soit $g \in \mathbb{Z}_q[X, Y]$ et supposons que x_0, $y_0 \in \mathbb{Z}_q$ tels que*

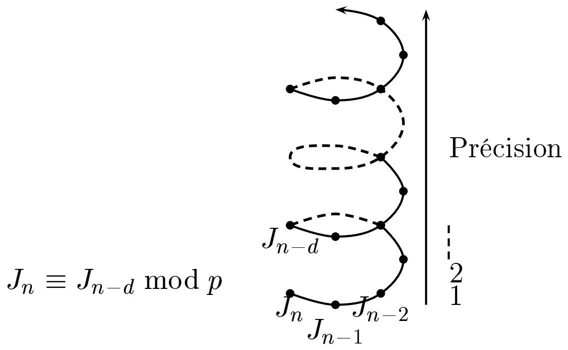
$$g(x_0, y_0) \equiv 0 \bmod p,\ \frac{\partial g}{\partial X}(x_0, y_0) \not\equiv 0 \bmod p \text{ et } \frac{\partial g}{\partial Y}(x_0, y_0) \equiv 0 \bmod p.$$

Alors les propriétés suivantes sont satisfaites :

1. *Pour tout $y \in \mathbb{Z}_q$ tel que $y \equiv y_0 \bmod p$ il existe un unique $x \in \mathbb{Z}_q$ tel que $x \equiv x_0 \bmod p$ et $g(x, y) = 0$.*
2. *Soit $y' \in \mathbb{Z}_q$ tel que $y \equiv y' \bmod p^m$, où $m \geqslant 1$ et soit $x' \in \mathbb{Z}_q$ l'unique élément tel que $x' \equiv x_0 \bmod p$ et $g(x', y') = 0$. Alors $x' \equiv x \bmod p^{m+1}$.*

Démonstration: Vercauteren et al. [VPV01] □

Cette proposition va nous permettre de relever un j-invariant à la précision n. En effet, si l'on applique cette proposition n fois, à chaque étape on va relever le j-invariant précédent dans le cycle au double de la précision. On va construire ainsi une helice de j-invariants.



10.1.2 Nouvel algorithme de relèvement des j-invariants

Comme on l'a vu dans la section précédente, l'algorithme de calcul de cardinalité d'une courbe de Vercauteren se décompose en deux parties : tout d'abord on relève un j-invariant à la précision n désirée et ensuite on relève étape après étape le j-invariant suivant ainsi que les coefficients de la courbe et le noyau du Frobenius afin d'en déduire la trace du Frobénius. Pour ces deux parties il est nécessaire d'avoir un algorithme qui calcule le relèvement du j-invariant précédent dans le cycle à partir du j-invariant que l'on est en train de traiter.

Procédure LiftJPrécédent
Entrées : Un j-invariant J_{i+1} relevé à une précision n et une précision désirée n'.
Sortie : Le j-invariant J_i relevé à une précision n'.

1. SI $n' = 2$ ALORS $J_i \leftarrow J_{i+1}^2 \bmod p$; GOTO 3 ;
2. SINON
   – $n' \leftarrow \lceil \frac{n}{2} \rceil$;
   – $J_i \leftarrow$ LiftJPrécédent(J_{i+1}, n') ;
   – $J_i \leftarrow J_i - \frac{\Phi_p(J_i,J_{i+1})}{\Phi'_p(J_i,J_{i+1})} \bmod p^{n'}$;
3. RETURN J_i.

À partir de cet algorithme on peut directement en déduire un algorithme qui relève le premier j-invariant à la précision voulue.

Procédure LiftPremierJ
Entrées : Un j-invariant j_0 dans $\mathbb{F}_q$ et une précision désirée n.
Sortie : J_0 tel que $J_0 \equiv j(\mathcal{E}_0) \bmod p^n$.

1. $J_0 \leftarrow j_0^{2^{d-(n+1)}} \bmod p$;
2. Pour $i := 2$ À n FAIRE $J_0 \leftarrow$ LiftJPrécédent(J_0, i) ;
3. RETURN J_0.

Pour calculer les coefficients c_i i.e. la trace du Frobenius, Vercauteren et al. se servent des mêmes algorithmes que nous avons proposés dans le chapitre précédent.

10.1.3 Complexité

Pour p fixé, le stockage en mémoire d'un élément dans $\mathbb{Z}_q$ nécessite $O(d^2)$ espace mémoire. À chaque pas on ne stocke en mémoire que $O(1)$ tels éléments. Par conséquent l'espace mémoire nécessaire est $O(d^2)$. La complexité en temps est la même que pour l'algorithme initial.

10.2 La moyenne Arithmético-Géométrique

L'idée de cet algorithme est aussi de construire une tour de j-invariants pour lesquels à chaque étape on double la précision. Cependant cette méthode ne va plus reposer sur un calcul à partir de l'équation modulaire, mais sur un calcul de termes de la moyenne arithmético-géométrique. On la définit très brièvement dans cette section, le lecteur intéressé par de plus amples informations consultera [BM88].

La moyenne arithmético-géométrique a été découverte par Legendre et Gauss indépendamment. Elle est définie comme suit :

Soient $a, b \in \mathbb{R}^+$. On pose $a_0 = a$ et $b_0 = b$. Alors on définit :

$$\begin{cases} a_{i+1} = \frac{a_i+b_i}{2} \\ b_{i+1} = \sqrt{a_i b_i} \end{cases} \tag{10.2}$$

Les suites (a_i) et (b_i) convergent vers un même élément $M(a,b)$. Cette convergence est quadratique, on a :

$$|a_{i+1} - b_{i+1}| \leqslant k|a_i - b_i|^2.$$

Gauss cherchait à calculer $\int_0^{\pi/2} \frac{dt}{\sqrt{\cos^2 t + 2\sin^2 t}}$ qui est égal à $\frac{\pi}{2M(1,\sqrt{2})}$. Il a prouvé par la suite que :

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2M(a,b)}. \tag{10.3}$$

10.2.1 Lien avec les courbes elliptiques

On peut interpréter cette moyenne par des 2-isogénies de courbes elliptiques. On a en effet la proposition suivante :

Proposition 10.2.1 *Soit E une courbe définie sur un corps de caractéristique zéro par l'équation suivante :*

$$E \ : \ y^2 = x(x - a^2)(x - b^2)$$

et soit E' la courbe d'équation :

$$E' \ : \ Y^2 = X(X - ab)(X - \frac{(a+b)^2}{4})$$

Alors ces deux courbes sont 2-isogènes. L'isogénie est définie par :

$$\begin{array}{lll} \varphi : E & & \to E' \\ (x,y) & \mapsto & \left(\frac{(x+ab)^2}{4x}, y\frac{(x-ab)(x+ab)}{8x^2}\right) \end{array}$$

et sa duale est donnée par :

$$\begin{array}{lll} \hat{\varphi} : E' & & \to E \\ (x,y) & \mapsto & \left(\frac{x(x-ab)}{x-\left(\frac{a+b}{2}\right)^2}, y\frac{\left(x-a\left(\frac{a+b}{2}\right)\right)\left(x-b\left(\frac{a+b}{2}\right)\right)}{\left(x-\left(\frac{a+b}{2}\right)^2\right)^2}\right) \end{array}$$

De plus, le noyau de cette isogénie est réduit à $\{(0,0), O_E\}$ et $\hat{\varphi}$ agit trivialement sur les formes différentielles :

$$\hat{\varphi}^*(\frac{\mathrm{d}X}{Y}) = \frac{\mathrm{d}x}{y}$$

On voit apparaître le premier lien avec l'algorithme de Satoh. Nous allons nous servir de cette isogénie qui est simple à calculer pour créer notre tour de j-invariant. Il faut donc considérer ces courbes dans des corps locaux. Nous allons particulièrement nous intéresser au corps 2-adique. Pour tous les détails pour les corps locaux quelconque, voir [HM89].

Par la suite, on note $p = 2$ et $q = 2^d$.

Soient a et $b \in \mathbb{Z}_q$ tels que :

$$a \equiv b \equiv 1 \bmod 4 \text{ et } \frac{b}{a} \equiv 1 \bmod 8. \tag{10.4}$$

Alors la racine carrée de ab existe dans $\mathbb{Z}_q$ et si on la prend telle qu'elle soit congrue à 1 mod 4 alors $a_1 = \frac{a+b}{2}$ et $b_1 = a\sqrt{\frac{b}{a}}$ satisfont les mêmes conditions que a et b. On peut ainsi construire les suites (a_i) et (b_i) et chaque terme des suites satisfait les conditions 10.4.

Soit $j_{a_i,b_i} = (256b^12/a^4 - 768b^10/a^2 + 1536b^8 - 1792a^2b^6 + 1536a^4b^4 - 768a^6b^2 + 256a^8)/(b^8 - 2a^2b^6 + a^4b^4)$ et soit E_{a_i,b_i} la courbe définie sur $\mathbb{F}_q$ par l'équation $y^2 + xy = x^3 + \frac{1}{j_{a_i,b_i} \bmod 2}$. On note $\mathcal{E}_{a_i,b_i}$ le relèvement canonique de E_{a_i,b_i} sur $\mathbb{Z}_q$ et $j(\mathcal{E}_{a_i,b_i})$ son j-invariant. Enfin, soit J_{a_i,b_i} le j-invariant de la courbe définie par : $y^2 = x(x - (a_i)^2)(x - (b_i)^2)$.

Le théorème suivant nous prouve que la suite des courbes d'équation : $y^2 = x(x - (a_i)^2)(x - (b_i)^2)$ converge vers le relèvement canonique.

Théorème 10.2.1 *Soient a_i et $b_i \in \mathbb{Z}_q$ satisfaisant les conditions 10.4. Supposons que pour $k \geqslant 2$,*

$$J_{a_i,b_i} \equiv j(\mathcal{E}_{a_i,b_i}) \bmod 2^k$$

alors

$$J_{a_{i+1},b_{i+1}} \equiv j(\mathcal{E}_{a_{i+1},b_{i+1}}) \bmod 2^{k+1}$$

Démonstration: Les j-invariants satisfont les conditions nécessaires à la proposition 10.1.1. □

10.2.2 Calcul de la trace du Frobenius

Théorème 10.2.2 *Soient a et $b \in \mathbb{Z}_q$ satisfaisant les conditions 10.4. Soit $\mathcal{E}$ la courbe d'équation $y^2 = x(x-a^2)(x-b^2)$ et supposons que cette courbe soit égale à son relèvement canonique. On définit une suite de courbes $\mathcal{E}_i$ telle que $\mathcal{E}_0 = \mathcal{E}$ et $\mathcal{E}_i$ a pour équation $y^2 = x(x-a_i^2)(x-b_i^2)$ où les coefficients a_i et b_i sont des éléments de la suite de la moyenne arithmético-géométrique initialisée avec a et b. Alors la trace de l'endomorphisme de Frobenius $\mathcal{F}$ est égale à :*

$$\mathrm{Tr}(\mathcal{F}) = \frac{a_0}{a_d} + 2^d \frac{a_d}{a_0}.$$

Démonstration: On a construit le cycle suivant :

$$\mathcal{E}_0 \xleftarrow{\hat{\varphi_0}} \mathcal{E}_1 \xleftarrow{\hat{\varphi_1}} \mathcal{E}_2 \xleftarrow{\hat{\varphi_2}} \cdots \xleftarrow{\hat{\varphi_{d-1}}} \mathcal{E}_d \simeq \mathcal{E}_0 \ .$$

On note λ l'isomorphisme $\mathcal{E}_0 \xrightarrow{\simeq} \mathcal{E}_d$. Cet isomorphisme est donné explicitement par

$$\lambda(x,y) = \left(\left(\frac{a_d}{a_0}\right)^2 x, \left(\frac{a_d}{a_0}\right)^3 y \right).$$

On considère maintenant l'endomorphisme $\hat{\mathcal{F}}$ de $\mathcal{E}$ défini par :

$$\hat{\mathcal{F}} = \hat{\varphi}_0 \circ \hat{\varphi}_1 \circ \cdots \circ \hat{\varphi}_{d-1} \circ \lambda.$$

Alors $\hat{\mathcal{F}}$ est le dual de l'endomorphisme de Frobenius de $\mathcal{E}$. En effet pour tout i, le morphisme φ_i est une isogénie de degré 2 dont le noyau est le point $(0,0)$ sur la courbe $\mathcal{E}_i$. Si l'on prend un modèle de $\mathcal{E}_i$ qui a bonne réduction modulo 2, on voit alors que ce point de 2-torsion est celui qui se réduit modulo 2 au point à l'infini. Donc φ_i se réduit au petit Frobenius σ_i. Par conséquent $\hat{\mathcal{F}}_i$ est le dual du Frobenius $\mathcal{F}$, l'isomorphisme λ nous assure que l'on revienne au même modèle de courbe.

Si on regarde maintenant l'action de $\hat{\mathcal{F}}$ sur les différentielles, on obtient :

$$\begin{aligned} \hat{\mathcal{F}}^* \left(\frac{\mathrm{d}x}{y}\right) &= \hat{\varphi}_0^* \circ \hat{\varphi}_1^* \circ \cdots \circ \hat{\varphi}_{d-1}^* \circ \lambda^* \left(\tfrac{\mathrm{d}x}{y}\right) \\ &= \lambda^* \left(\tfrac{\mathrm{d}x}{y}\right) \\ &= \tfrac{a_0}{a_d} \left(\tfrac{\mathrm{d}x}{y}\right) \end{aligned}$$

puisque les morphismes $\hat{\varphi}$ agissent trivialement sur les différentielles.

Par conséquent, $\frac{a_0}{a_d}$ est une racine du polynôme caractéristique de $\hat{\mathcal{F}}$ et donc

$$\mathrm{Tr}(\mathcal{F}) = \mathrm{Tr}(\hat{\mathcal{F}}) = \frac{a_0}{a_d} + 2^d \frac{a_d}{a_0}.$$

□

Dans ce cas à nouveau il nous suffit de connaitre le relèvement canonique de la courbe à une certaine précision n. D'après la borne de Hasse, la trace est dans l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$, donc calculer la trace modulo $2^{\lceil \frac{d}{2}+2 \rceil}$ est suffisant pour conclure.

10.2.3 Algorithme

Avant de donner l'algorithme, il nous faut trouver les valeurs qui vont l'initialiser. En effet, l'algorithme prend en entrée une courbe dans $\mathbb{F}_{2^d}$ d'équation $y^2 + xy = x^3 + a_6$ et on veut la transformer en une courbe dans $\mathbb{Z}_q$ ayant une équation de la forme $y^2 = x(x - a^2)(x - b^2)$ où $a \equiv b \equiv 1 \bmod 4$ et $\frac{a}{b} \equiv 1 \bmod 8$.

Lemme 10.2.1 *Soit E une courbe définie sur $\mathbb{F}_{2^d}$ d'équation $y^2 + xy = x^3 + a_6$. Soit E' l'image de E par le petit Frobenius σ. Alors E' est isomorphe dans $\mathbb{Z}_q$ a une courbe d'équation $y^2 = x(x - a^2)(x - b^2)$ où $a \equiv 1 + 8a_6 \bmod 16$ et $b \equiv 1 \bmod 16$.*

On va se servir de cette courbe comme initialisation de l'algorithme.

Procédure CALCULTRACEAGM
Entrées : Une courbe E définie sur $\mathbb{F}_{2^d}$ par l'équation $y^2 + xy = x^3 + a_6$, telle que $a_6 \in \mathbb{F}_{2^d}/\mathbb{F}_4$.
Sortie : La trace de la courbe E.

1. $a \leftarrow 1 + 8a_6 \bmod 16$; $b \leftarrow 1 \bmod 16$; $k \leftarrow 4$;
2. TANT QUE $k \leqslant \lceil \frac{d}{2} \rceil + 3$ FAIRE
   - $(a,\ b) \leftarrow \left(\frac{a+b}{2} \bmod 2^{k+1},\ \sqrt{ab} \bmod 2^{k+1} \right)$;
   - $k \leftarrow k + 1$;
3. $a_0,\ b_0 \leftarrow a,\ b$;
4. POUR $i := 1$ À d FAIRE $(a,\ b) \leftarrow \left(\frac{a+b}{2} \bmod 2^k,\ \sqrt{ab} \bmod 2^k \right)$;
5. RETURN $\frac{a_0}{a} \bmod 2^{\lceil \frac{d}{2} \rceil + 2}$ comme un entier dans l'intervalle $[-2\sqrt{2^d}, 2\sqrt{2^d}]$.

10.2.4 Complexité

Le coût de cet algorithme est le coût de $O(d)$ multiplications dans $\mathbb{Z}_q$. La précision maximale nécessaire est $\lceil \frac{d}{2} \rceil + 4$, donc la taille des éléments est en $O(d^2)$ bits. Par conséquent, la complexité en temps de l'algorithme est en $O(d^5)$ si on se sert d'une arithmétique naïve et en $O(d^{3+\epsilon})$ avec des algorithmes de multiplications rapides.

On stocke en mémoire un nombre constant d'éléments de $\mathbb{Z}_q$. L'espace mémoire nécessaire est donc $O(d^2)$.

10.3 Améliorations dans le calcul de la norme d'un élément de $\mathbb{Z}_q$

Dans cette section, on donne l'idée principale du nouvel algorithme de Satoh. Pour avoir de plus amples détails, voir l'article original [Sat01]. L'intérêt d'un tel algorithme est de pouvoir apporter directement des améliorations aux algorithmes de comptage des points d'une courbe que nous avons présentés dans cette partie.

10.3.1 Calcul de la norme d'un élément de $\mathbb{Z}_q$

Soient p un petit nombre premier fixé et $\mathbb{Q}_p$ un corps de nombres p-adiques. On note K une extension non-ramifiée de $\mathbb{Q}_p$ telle que $[K : \mathbb{Q}_p] = d$. L'anneau des entiers de K est alors $\mathbb{Z}_q$ où $q = p^d$.

Problème : Pour un $x \in \mathbb{Z}_q^*$ connu à une précision M donné, calculer la norme $N_{K/\mathbb{Q}_p}(x) \bmod p^M \in \mathbb{Z}/p^M\mathbb{Z}$ avec une complexité minimum en temps et en espace.

La norme de l'élément x est définie comme le produit $\prod_{i=0}^{d-1} \Sigma^i(x)$ où Σ est le petit Frobenius dans $\mathbb{Z}_q$.

Méthode naïve : On pose $K = \mathbb{Q}_p(\theta)$ où $\theta \in \mathbb{Z}_q$. Alors on peut exprimer x comme :

$$x \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{d-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{d-1} \end{pmatrix} \text{ où } A \in \mathrm{Mat}(d, \mathbb{Z}_p)$$

et

$$N_{K/\mathbb{Q}_p}(x) = \det\, A.$$

La complexité d'une telle méthode est de $O(Md^2)$ en espace mémoire et en temps en $O(d^3 T_M)$ en utilisant une élimination gaussienne ou en $O(d^{2.376} T_M)$ en se servant de l'algorithme de Coppersmith et Winograd [CW90] où T_M est la complexité en temps d'une multiplication dans $\mathbb{Z}/p^M\mathbb{Z}$.

Soit $x \in \mathbb{Z}_q^*$ connu à une précision M et soit $n \geqslant 1$. On pose $y_n = \Sigma^{-n+1}(x) \dots \Sigma^{-1}(x)x$. Alors

$$\begin{aligned} y_1 &= x \\ y_{2n} &= \Sigma^{-n}(y_n)y_n \\ y_{2n+1} &= \Sigma^{-1}(y_{2n})x \end{aligned}$$

et donc

$$y_d = N_{K/\mathbb{Q}_p}(x).$$

En considérant le développement binaire de d, on peut calculer y_d avec $O(\log\, d)$ appels à Σ^{-r} avec différentes valeurs de r et où la somme des entiers r est d. On a $\mathbb{Z}_q = \mathbb{Z}_p[\theta]$ et le polynôme minimal de θ est séparable. Alors en précalculant les $\Sigma^{-r}(\theta)$ qui apparaissent dans le précédent procédé, on obtient $\Sigma^{-r}(\sum_{i=0}^{d-1} a_i\theta^i) = \sum_{i=0}^{d-1} a_i(\Sigma^{-r}(\theta))^i$ en $d-2$ multiplications sur $\mathbb{Z}_q$. La complexité en général de cette méthode est en $O(d\log\, d)$.

Le but de l'algorithme de Satoh est de se débarasser du facteur $\log\, d$ dans la complexité précédente. L'amélioration de ce calcul est fondée sur les racines (p^d-1)-ème de l'unité dans $\mathbb{Z}_q$. Soit Ψ une racine (p^d-1)-ème de l'unité dans $\mathbb{Z}_q$ telle que $\Psi \equiv \theta \bmod p$. Comme $X^{p^d-1} - 1 \in \mathbb{F}_p[X]$ est un polynôme séparable, alors $\Sigma(\Psi)$ est tout simplement Ψ^p. Donc pour $x = \sum_{i=0}^{d-1} b_i\Psi^i$ et en réorganisant les termes, on a

$$\Sigma^{-1}(x) = \Sigma^{-1}(\sum_{i=0}^{\ell} b_i\Psi^i) = \sum_{i=0}^{p-1} \left(\sum_{0 \leqslant i+pj \leqslant \ell} b_{i+pj}\Psi^j \right) \Sigma^{-1}(\Psi^i).$$

L'intérêt d'utiliser Σ^{-1} est de diviser le degré du polynôme par p. Le polynôme $\Sigma^{-1}(\Psi^i)$ en Ψ est de degré inférieur ou égal à $d-1$. Ainsi si $\ell < 2d$, le degré en Ψ du membre de droite est inférieur à $2d$. Ainsi $\Sigma^{-n}(x)$ peut être calculé en $n(p-1)$ multiplications sur $\mathcal{P} = \{f \in \mathbb{Z}_p[X] | \deg f < d\}$ et une réduction modulo le polynôme minimal de Ψ.

D'autre part, le polynôme minimal de Ψ est dense donc multiplier deux éléments dans $\mathbb{Z}_q$ par rapport à Ψ consiste en trois multiplications sur $\mathcal{P}$. Ainsi exprimer $\sum a_i\theta_i$ en $\sum b_i\Psi^i$ nécessite $3(d-1)$ multiplications sur $\mathcal{P}$. En définitive calculer la norme avec cette méthode se fait en $(p+2)(d-1)+O(n)$ multiplications sur $\mathcal{P}$ et nécessite un stockage de $O(1)$ éléments de $\mathbb{Z}_q$.

10.3.2 Application aux algorithmes de calcul de cardinalité

Comme on peut le remarquer après l'étude des algorithmes de Vercauteren et al. et de l'AGM, toutes les améliorations portent sur le relèvement du cycle de courbes. En effet, Vercauteren ne relève plus simultanément l'ensemble du cycle de courbe et l'AGM passe par les coefficients de la courbe. Ce qui reste inchangé dans ces méthodes est le calcul final de la trace qui correspond au calcul de la norme de g_0 (comme indiqué en 9.1) dans le cas de Satoh-FGH et de Vercauteren et al. et à celui de $\frac{a_0}{a_1}$. On peut donc modifier ces trois algorithmes en utilisant ces nouveaux calculs de norme. Par exemple, dans le cas de l'AGM, dans la procédure CalculTraceAGM, on remplace les étapes 4 et 5 par les suivantes :

4. $(a_1,\ b_1) \leftarrow \left(\frac{a_0+b_0}{2} \bmod 2^k,\ \sqrt{a_0b_0} \bmod 2^k\right)$;
5. RETURN la norme de $\frac{a_0}{a_1}$ modulo $2^{\lceil \frac{d}{2} \rceil + 2}$ comme un entier dans l'intervalle $[-2\sqrt{2^d}, 2\sqrt{2^d}]$.

Chapitre 11

Application à la cryptographie

La naissance de nouveaux algorithmes de calcul de cardinalité d'une courbe elliptique présentés dans les chapites précédents nécessite aussi leur adaptation à la construction de courbes sûres cryptographiquement parlant. Ainsi similairement à Lercier [Ler97a], nous joignons à l'algorithme Satoh-FGH une stratégie de early-abort. Ce chapitre retranscrit les travaux réalisés en collaboration avec Pierrick Gaudry et Robert Harley [FGH01].

11.1 Bonnes courbes elliptiques en cryptographie

La sécurité des cryptosystèmes utilisant les courbes elliptiques dépend de la difficulté à résoudre le problème du logarithme discret sur une courbe elliptique (ECDL). Il existe de nombreuses attaques contre des courbes ayant des propriétés particulières comme celle contre les courbes de trace 1, la réduction MOV pour les courbes supersingulières, etc...

Pour des courbes aléatoires, la chance que l'une de ces méthodes puisse être appliquée est relativement petite. Cependant il existe d'autres attaques qui fonctionnent pour les groupes finis abéliens génériques.

La première méthode est la réduction de Pohlig-Hellman [PH78]. Quand l'ordre du groupe N a tous ses facteurs premiers petits, les logarithmes discrets peuvent être calculés rapidement en travaillant dans des petits sous-groupes. Donc pour une bonne sécurité il est essentiel de choisir un groupe dont l'ordre est divisible par un grand nombre premier.

Les autres attaques sont des algorithmes qui marche en temps $O(\sqrt{N})$. Ils incluent l'algorithme de Shanks : pas de bébé, pas de géant (voir [Coh96a]) et la méthode ρ Pollard [Pol78]. En pratique le logarithme discret sur une courbe elliptique le plus difficile calculé est sur une courbe de Koblitz sur $\mathbb{F}_{2^{109}}$ qui se sert d'une version distribuée de la méthode ρ-Pollard [Har].

En extrapolant le travail requis pour des tailles plus grandes et en se permettant des marges de sécurité pour les futures améliorations dans la puissance de calcul, il est généralement cru (voir [FIPS186], [LV00], [P1363], [Sil00]) qu'une courbe aléatoire dont l'ordre est divisible par un nombre premier d'au moins 160 bits offre une sécurité raisonnable, comparable aux systèmes symétriques de 80 bits ou à un RSA de 1024 bits. Pour des applications nécessitant de plus grandes mesures de sécurité, on peut prendre de plus grandes marges de sécurité.

Pour trouver une courbe sûre, Lercier [Ler97a] propose une stratégie de early-abort à utiliser lors du calcul de la cardinalité de la courbe en se servant de l'algorithme SEA. L'idée est de tester au vol si $q + 1 - t \equiv 0 \bmod \ell$. Si le test est bon, alors on rejette la courbe et on essaie à nouveau avec une nouvelle courbe. Comme SEA calcule $t \bmod \ell$, ce test est simple à implémenter et ne coute aucun temps de calcul. En caractéristique grande où l'algorithme Satoh-FGH ne s'applique

Taille du corps	163 bits	193 bits	239 bits	409 bits	571 bits
Coût d'une multiplication dans $\mathbb{F}_q$	0.488 μs	0.639 μs	0.917 μs	2.632 μs	4.685 μs

TAB. 11.1 – Coût d'une multiplication dans $\mathbb{F}_q$ sur une Alpha EV6 750 MHz.

Taille du corps de base	163 bits	193 bits	239 bits	409 bits	571 bits
Précision maximale	85	100	123	208	289
Coût d'une multiplication dans $\mathbb{Z}_q$	0.19 ms	0.24 ms	0.36 ms	4.6 ms	8.0 ms

TAB. 11.2 – Coût d'une multiplication dans $\mathbb{Z}_q$ sur une Alpha EV6 750 MHz.

pas c'est encore la meilleure méthode connue et nous nous referons à la littérature existante sur le sujet [LM95], [IKNY98], [MP98].

L'une des difficultés qui surgit lorsque l'on adapte une stratégie de early-abort à l'algorithme de Satoh-FGH est que $t \bmod \ell$ n'est pas obtenu au cours de l'algorithme (sauf lorsque ℓ est une puissance de p). Notre solution est d'implanter une version simplifiée de l'algorithm SEA pour déterminer si la courbe a un point de ℓ-torsion rationnel ou non pour les premiers nombres premiers ℓ dans une étape préliminaire avant de se servir de l'algorithme Satoh-FGH. Nous devons faire un trade-off entre le coût supplémentaire de ces calculs et le bénéfice de ne pas avoir àfaire un calcul intégral de cardinalité. En pratique nous avons trouvé que cette méthode vaut la peine et n ous avons obtenu des temps de calcul inférieurs à ceux précédemment connu.

11.2 Implantation et résultats

11.2.1 Détails d'implantation

Nous avons écrit des implantations optimisées de la stratégie du early-abort et de l'algorithme de Satoh-FGH pour la caractéristique deux en langage C. Cette implantaion de la stratégie du early-abort est indépendante de celle de Lercier. Pour la multiplication dans $\mathbb{F}_q$ nous nous sommes servis de l'algorithme de Karatsuba ; dans $\mathbb{Z}_q$ nous avons utilisé l'algorithme de Toom. Pour nous assurer que la réduction modulaire prenne peu de temps, nous avons choisi le polynôme irréductible comme étant un trinôme ou un pentanôme. Pour la division on a utilisé l'algorithme d'Euclide binaire dans $\mathbb{F}_q$ et l'inversion par des itérations de Newton dans $\mathbb{Z}_q$.

La plupart de nos tests de timing ont été effectué sur une Alpha EV6 750 MHz. Afin de pouvoir comparer certains de nos résultats avec ceux de [Ler97a], nous avons aussi réalisé des tests sur une Alpha EV4 266 MHz identique à celle dont Lercier s'est servi. Enfin on a mesuré le temps nécessaire à la génération d'une courbe sur un petit corps sur une puce StrongARM 275 MHz.

Dans la partie du early-abort, comme expliqué par la suite, ce qui demande le plus de temps de calcul sont des factorisations paresseuses de polynômes de petit degré sur $\mathbb{F}_q$. L'opération la plus fréquente est la multiplication dans $\mathbb{F}_q$. Nous donnons les timings correspondants sur l'Alpha 750 MHz dans le tableau 11.1.

L'opération la plus fréquente dans le calcul de la cardinalité est la multiplication dans $\mathbb{Z}_q$. Dans le tableau 11.2, nous donnons le temps pour une telle opération à la précision 2-adique maximale requise i.e., $\lceil d/2 \rceil + 3$ bits, pour différentes tailles de corps d. Ces mesures ont aussi été réalisées sur l'Alpha 750 MHz.

Taille du corps	SEA (temps de [Ler97b])			Satoh-FGH	Ratio
	Min	Max	Moy		
155 bits	58.8 s	132 s	86.5 s	36.3 s	2.4
196 bits	212 s	1029 s	308 s	68.8 s	4.5
300 bits	1519 s	3686 s	2434 s	408.4 s	6

TAB. 11.3 – Temps de calcul pour le calcul de la cardinalité sur une Alpha EV4 266 MHz.

Taille du corps	Satoh-FGH	Taille du corps	Satoh-FGH	Taille du corps	Satoh-FGH
157 bits	2.39 s	197 bits	4.45 s	283 bits	26.5 s
163 bits	2.76 s	233 bits	6.57 s	409 bits	76.3 s
193 bits	4.10 s	239 bits	6.94 s	571 bits	257 s

TAB. 11.4 – Timings pour le calcul de la cardinalité sur une Alpha EV6 750 MHz

11.2.2 Calcul du nombre de points d'une courbe

Quand on calcule la cardinalité d'une courbe, il faut décider s'il on utilise SEA ou Satoh. Deux cas doivent être traités séparément : le cas de grande caractéristique et celui de la petite caractéristique.

La complexité de l'algorithme de Satoh a une mauvaise dépendance en la caractéristique p du corps de base et quand p est grand, il n'est pas du tout efficace. Ceci est dù à l'utilisation de l'équation modulaire Φ_p pour relever les courbes. Cette équation a $O(p^2)$ coefficients qu'il est nécessaire de connaître au moins modulo $p^{(d/2)+O(1)}$. Par conséquent une complexité exponentielle en p semble être inévitable. D'un autre coté, l'algorithme SEA est en temps polynomial indépendamment de p. Par exemple, Morain a calculé le nombre de points d'une courbe sur un corps de taille $10^{499} + 153$ [Mor95].

Cependant en petite caractéristique l'algorithme dde Satoh est efficace. En particulier dans le cas de la caractéristique deux, Satoh-FGH est clairement plus rapide que SEA en pratique. Pour illustrer la différence de rapidité entre les deux algorithmes, nous comparons les résultats de Lercier [Ler97b] avec les timings que nous obtenons sur les mêmes corps, en se servant une Alpha 266 MHz identique. Les résultats sont donnés dans le tableau 11.3. Nous ne donnons pas de temps minimal ou maximal pour Satoh-FGH puisque les temps de calcul sont à peu près constant quand on traite des courbes différentes sur le même corps. Ces résultats montre que plus le corps est grand, plus l'avantage de Sath-FGH augmente.

Nous donnons les timings pour le calcul de la cardinalité sur une Alpha 750 MHz dans le tableau 11.4. La plupart des tailles de corps que nous avons choisi sont recommandées dans les standards de cryptographie (ANSI X9.63, IEEE P1363, IPSec, NIST, WAP).

Remarque : Dans certains cas, les algorithmes SEA et Satoh-FGH peuvent être combinés pour accélérer le calcul du nombre de points. Ceci fonctionne particulièrement bien quand la taille du corps est telle que la précision maximum requise dans Satoh-FGH est un peu plus qu'un multiple de la taille d'un mot de la machine. Un bon exemple est $q = 2^{251}$: la précision maximale dans le calcul des relèvements est $\lceil \frac{251}{2} \rceil + 3 = 129$ bits. Dans ce cas, calculer la trace modulo 3 à l'aide de l'algorithme SEA permet de réduire la précision à 128 bits ce qui correspond à un nombre entier de mots. Cette approche pourrait certainement être poussée plus loin, mais la complexité d'implantation semble dépasser le gain modéré en vitesse.

11.2.3 Calcul d'une bonne courbe

La stratégie naïve pour calculer une courbe pour des usages cryptographiques est de calculer le nombre de points de nombreuses courbes, jusqu'à en trouver une d'ordre quasi-premier. Comme mentionné precédemment, si l'algorithme SEA est utilisé alors de nombreuses mauvaises courbes peuvent être détectées rapidement ; cette agréable propriété ne tient pas dans le cas d l'algorithme de Satoh-FGH.

Par conséquent, pour de petites à moyennes tailles, la stratégie naïve en utilisant Satoh-FGH n'est pas meilleure que la stratégie de early-abort avec SEA. Par exemple sur $\mathbb{F}_{2^{155}}$, Lercier [Ler97b] a pu selectionner les bonnes courbes dans un ensemble de 1000 courbes aléatoires en 14112 secondes. Sur un ordinateur identique, la méthode de Satoh-FGH prend 36.5 secondes par courbe, donc sélectionner les bonnes courbes prendrait 36500 secondes avec la stratégie naïve et serait pire que la méthode SEA d'un facteur 2.5. (pour des tailles de corps plus grandes, ce phénomène disparait et Satoh-FGH est toujours meilleur.)

Pour contrer cela, nous tirons parti des deux méthodes : nous éliminons tout d'abord bon nombre de courbes par une stratégie de early-abort fondé sur les techniques de l'algorithme SEA, et ensuite d'utiliser Satoh-FGH sur celles qui restent.

Soit E une courbe définie sur $\mathbb{F}_q$. Pour un petit nombre premier ℓ, E est dite ℓ-bonne si son ordre est premier à ℓ, et ℓ-mauvaise sinon. Le early-abort fonctionne comme suit pour chaque ℓ :

1. Calculer le nombre de racines de $\Phi_\ell(X, j(E))$. Il peut y en avoir 0, 1, 2 ou $\ell+1$. (Les cas 1 ou $\ell+1$ ne peuvent arriver que quand q est un carré modulo ℓ.)
2. S'il n'y a pas de racines, E est ℓ-bonne.
3. Sinon, pour chaque racine de Φ_ℓ, construire le facteur correspondant du polynôme de ℓ-division et chercher une racine x du facteur. Si un tel x existe dans $\mathbb{F}_q$ et un y correspondant aussi, alors (x, y) est un point de ℓ-torsion sur $\mathbb{F}_q$ et E est ℓ-mauvaise.
4. Sinon E est ℓ-bonne.

Calculer X^q modulo $\Phi_\ell(X, j(E))$, qui a degré $\ell+1$ est ce qui consomme le plus de temps à l'étape 1. Pour accélerer les calculs, on remplace Φ_ℓ par un polynôme modulaire *canonique* Φ_ℓ^c, qui a le même degré mais qui est plus creux et implique de plus petites puissances de j. On se rapporte à [Mor95] pour la construction et les propriétés de ces équations.

Heuristiquement, dans la moitié des cas il n'y aura pas de racines (ce sont les nombres premiers d'Atkin) et nous aurons fini. Sinon, il faut continuer jusqu'à l'étape 3. Le facteur du polynôme de division correspondant à une racine du polynôme modulaire est calculé en se servant d'un système de formules dues à Lercier [Ler97a]. Pour un petit ℓ la solution à ce système peut être écrit explicitement, et obtenir le facteur ne coûte pratiquement rien en temps. (Pour un ℓ plus grand le système pourrait être résolu efficacement par un algorithme dù aussi à Lercier.) Le coût de la recherche d'une racine du facteur est dominé par le calcul de X^q modulo le facteur qui est de degré $(\ell-1)/2$.

Dans le tableau 11.5 on donne les temps de calcul pour cette procédure, mesuré sur une Alpha 750 MHz.

Il est nécessaire de borner la valeur maximum de ℓ pour équilibrer le coût du early-abort et le gain obtenu en évitant de calculer la cardinalité. En théorie, il serait bénéfique d'augmenter ℓ jusqu'à ce que la procédure de early-abort prenne un ℓ-ième du temps nécessaire pour calculer le nombre de points. Par conséquent la taille maximum de ℓ devrait augmenter avec la taille du corps.

Cependant presque tous les avantages à gagner viennent avec l'utilisation des nombres premiers et en pratique on a trouvé que $\ell \leqslant 19$ était un bon équilibre. Pour ces premiers il n'est pas

	$q = 2^{163}$		$q = 2^{239}$	
ℓ	Calcul des racines de $\Phi_\ell^c(X, j)$	Moyenne du temps total	Calcul des racines de $\Phi_\ell^c(X, j)$	Moyenne du temps total
3	0.17 ms	0.17 ms	0.28 ms	0.28 ms
5	0.34 ms	0.38 ms	0.61 ms	0.68 ms
7	0.34 ms	1.18 ms	0.56 ms	2.18 ms
11	4.42 ms	6.93 ms	9.14 ms	14.1 ms
13	1.07 ms	4.19 ms	1.94 ms	8.36 ms
17	3.71 ms	8.63 ms	7.34 ms	17.9 ms
19	4.97 ms	11.6 ms	10.1 ms	23.7 ms

TAB. 11.5 – Temps moyen de calcul pour vérifier si E est ℓ-bonne (EV6 – 750 MHz)

Taille de corps	SEA (de [Ler97b])	Satoh-FGH + early-abort
155 bits	14112 s	4490 s
196 bits	30254 s	7850 s

TAB. 11.6 – Temps de calcul pour sélectionner une bonne courbe sur 1000 (EV4 – 266 MHz)

difficil de déterminer si les courbes sont ℓ-bonnes : la construction de Lercier est relativement aisée, comme dans la recherche des points de ℓ-torsion, ce qui permet de conserver un programme simple.

Pour permettre la comparaison avec les résultats de Lercier qui se trouve dans [Ler97b], nous avons effectué d'autres calculs sur Alpha 266 MHz. Nous avons choisi une stratégie de early-abort similaire, en recherchant de bonnes courbes d'ordre $4p$ sans jamais considérer les tordues des courbes (mais voir ci-dessous). Les résultats sont dans le tableau 11.6. En premier lieu dans le early-abort, on détermine si l'ordre est divisible par 8. On peut le décider très rapidement en calculant $\operatorname{Tr} a_6$. Remarquez que l'on a fait des mesures de timings pour des corps de taille de 157 et de 197 bits au lieu de 155 et de 196 bits parce que des corps d'extension composée peuvent être faibles dans certains cas [GS99, GHS01b, HSS00, JMS01, Sma00, MQ01].

Ensuite, dans le but de maximiser les performances de la génération de courbes nous avons décidé de rechercher simultanément pour les tordues des courbes d'ordre $2p$ et ceci nous a permis de doubler à peu près la vitesse de calcul. Comme la trace de la tordue est l'opposé de celle de la courbe, il est clair que la cardinalité de la tordue peut être déduite immédiatement de la cardinalité de la courbe elle-même. De plus, la stratégie de early-abort peut être adaptée facilement pour prendre en compte la tordue de la courbe puisqu'elle a le même j-invariant et les mêmes polynômes de division (en effet la courbe et sa tordue sont isomorphe sur une clotûre algébrique et l'isomorphisme préserve les abscisses).

Une possibilité serait de rejeter une paire consistant en une courbe et sa tordue seulement si les deux courbes ne conviennent pas cryptographiquement. Alternativement on peut aussi adopter une stratégie plus agressive qui consiste à rejeter les deux courbes dès que l'une des deux ne convient pas et à passer de suite à une nouvelle paire de courbes. En utilisant cette dernière méthode pour 10000 paires de courbes aléatoires sur une Alpha 750 MHz, on a mesuré les temps de calcul donnés dans le tableau 11.7.

Bien que la complexité en espace en $O(d^3)$ grossisse rapidement, les astuces décrites en 9.2.1 permettent de garder le facteur constant petit. Avec ces astuces, la plus grande taille de clé (571 bits) que nous gérons demande moins de 10 mégabytes et pour des tailles de clés modérées

Taille du corps (en bits)	Temps pour le e.-a. sur 10000 courbes	Courbes restantes	Temps de calcul de la cardinalité des cbes restantes	Bonnes courbes	Temps moyen pour trouver une bonne cbe
157	21.1 s	435	17.3 min	45	23.6 s
163	23.1 s	473	21.7 min	55	24.1 s
193	25.1 s	402	27.5 min	33	50.7 s
197	30.8 s	415	30.8 min	43	43.6 s
233	40.3 s	402	44 min	29	92,4 s
239	43.5 s	435	50.3 min	29	105.6 s
283	122 s	418	3h 4 min	20	9.2 min
409	245 s	467	9h 54 min	22	27 min
571	524 s	375	26h 40 min	11	146 min

Tab. 11.7 – Temps de calcul moyen pour trouver une bonne courbe (EV6 – 750 MHz)

Taille du corps	Fréquence	Temps pour le calcul du nbre de points d'une cbe	Temps moyen pour trouver une bonne cbe	RAM + ROM utilisés
113 bits	275 MHz	5.9 s	38 s	240 KB + 136 KB

Tab. 11.8 – Temps nécessaire pour trouver une bonne courbe WAP sur une puce ARM

l'espace mémoire nécessaire est seulement de quelques centaines de kilobytes. Nous avons choisi d'utiliser un peu plus d'espace mémoire en échange d'une vitesse de calcul un peu plus rapide.

Pour rechercher la possibilité de générer des courbes sur des environnements contraints, on a fait des tests de courbes sur des corps de 113 bits sur une puce ARM. Cette petite taille de clé est recommandée pour les échanges de clés sur le WAP et peut être utilisé pour une sécurité à court terme à un niveau comparable que celui du DES. Ces résultats se trouve dans le tableau 11.8.

11.3 Conclusion

L'algorithme de Satoh-FGH a prouvé être la méthode à choisir quand l'on recherche à calculer la cardinalité d'une courbe aléatoire définie sur un corps fini de caractéristique deux. Mais malgré les excellents résultats de Satoh-FGH (voir tableau 11.4), l'algorithme SEA ne doit pas être abandonné trop rapidement. Dans le cas de la grande caractéristique c'est la seule méthode pratique à disposition. De plus la stratégie de early-abort, fortement liée à SEA, est nécessaire pour calculer une courbe à usage cryptographique , même en petite caractéristique. En combinant cette technique avec l'algorithme Satoh-FGH, nous obtenons une methode efficace pour calculer des courbes sûres (voir tableau 11.7). En conclusion, il n'est plus nécessaire d'utiliser des courbes précalculées en cryptographie puisque l'on peut calculer de nouvelles courbes sans difficultés.

Bibliographie

[P1363] IEEE P1363. Standard specifications for public key cryptography. Available at `http://www.manta.ieee.org/groups/1363/`.

[FIPS186] FIPS 186-2. Digital Signature Standard. Federal Information Processing Standards publication, Jan. 2000. U.S. Departement of Commerce/National Institute of Standards and Technology. Available at `http://csrc.nist.gov/cryptval/dss.htm`.

[ADH94] L. M. Adleman, J. DeMarrais, et M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroups of the jacobians of large genus hyperelliptic curves over finite fields. In L. M. Adleman et M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 28–40. Springer-Verlag, 1994.

[AHU74] A. V. Aho, J. E. Hopcroft, et J. D. Ullman. *The design and analysis of computer algorithms*. Addison–Wesley, 1974.

[Ami75] Y. Amice. *Les nombres p-adiques*. Presses universitaires de France, 1975.

[Apo76] T. M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, 1976.

[ARS78] L. M. Adleman, R. L. Rivest, et A. Shamir. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[Atk92] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Series of e-mails to the `NMBRTHRY` mailing list, 1992.

[BB87] J. M. Borwein et P. B. Borwein. *Pi and the AGM*. Wiley-Interscience, 1987.

[BC67] Z. I. Borevitch et I. R. Chafarevitch. *Théorie des nombres*. Gauthiers-Villars, Paris, 1967.

[BCH+66] A. Borel, S. Chowla, C.S. Herz, K. Iwasawa, et J.P. Serre. Seminar on complex multiplication. In *Lecture Notes in Mathematics*, 1966.

[BM88] J.-B. Bost et J.-F. Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.*, (38):36–64, 1988.

[BSS99] I. Blake, G. Seroussi, et N. Smart. *Elliptic curves in cryptography*, volume 265 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1999.

[Cas91] J.W.S. Cassels. *Lectures on elliptic curves*, volume 24. London Math. Soc. Stud. Texts, 1991.

[CCR91] L. S. Charlap, R. Coley, et D. P. Robbins. Enumeration of rational points on elliptic curves over finite fields. Draft, 1991.

[CDL+00] S. Cavallar, B. Dodson, A. K. Lenstra, W. Lioen, P. L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain,

A. Muffett, C. Putnam, C. Putnam, et P. Zimmermann. Factorization of a 512-bit RSA modulus. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 1–18. Springer-Verlag, 2000. Proc. International Conference on the Theory and Application of Cryptographic Techniques, Brugge, Belgium, May 2000.

[CDM96] J.-M. Couveignes, L. Dewaghe, et F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03, LIX, Avr. 1996. Available at `http://www.lix.polytechnique.fr/Labo/Francois.Morain/`.

[CM94] J.-M. Couveignes et F. Morain. Schoof's algorithm and isogeny cycles. In L. Adleman et M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 43–58. Springer-Verlag, 1994.

[CNST98] J. Chao, O. Nakamura, K. Sobataka, et S. Tsujii. Construction of secure elliptic cryptosystems using CM tests and liftings. In K. Ohta et D. Pei, editors, *Advances in Cryptology - Asiacrypt'98*, volume 1514 of *Lecture Notes in Comput. Sci.*, pages 95–109. Springer, Oct. 1998.

[Coh84] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95:389–402, 1984.

[Coh96a] H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1996. Third printing.

[Coh96b] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer–Verlag, 1996.

[Cou94] J.-M. Couveignes. *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, Juil. 1994.

[Cou96] J.-M. Couveignes. Computing l-isogenies using the p-torsion. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.

[Cox89] D. H. Cox. *Primes of the Form $x^2 + ny^2$.* Wiley-Interscience, 1989.

[CW90] D. Coppersmith et S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Comput.*, pages 251–280, 1990.

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.

[Dew95] L. Dewaghe. Un corollaire aux formules de Vélu. Preprint, Dec. 1995.

[Dew96] L. Dewaghe. *Calcul du nombre de points sur une courbe elliptique dans un corps fini.* Thèse, Université des sciences et technologies de Lille, Dec. 1996.

[Dew98] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.*, 67(223):1247–1252, Juil. 1998.

[DH76] W. Diffie et M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22-6:644–654, Nov. 1976.

[EG00] A. Enge et P. Gaudry. A general framework for subexponential discrete logarithm algorithms. Research Report LIX/RR/00/04, LIX, 2000.

[Elk91] N. D. Elkies. Explicit isogenies. Draft, 1991.

[Elk98] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell et J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[Eng99a] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. Combinatorics and Optimization Research Report CORR 99-04, University of Waterloo, Fev. 1999. To appear in *Math. Comp.*; available at http://cacr.math.uwaterloo.ca/techreports/1999/corr99-04.ps.

[Eng99b] A. Enge. *Elliptic curves and their applications to cryptography.* Kluwer academic publishers, 1999.

[Eng00] A. Enge. *Hyperelliptic cryptosystems: Efficiency and subexponential attacks.* PhD thesis, Universität Augsburg, Dec. 2000.

[FGH00] M. Fouquet, P. Gaudry, et R. Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, Dec. 2000.

[FGH01] M. Fouquet, P. Gaudry, et R. Harley. Finding secure curves with the Satoh-FGH algorithm and an early-abort strategy. In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 14–29. Springer-Verlag, 2001.

[FM00] M. Fouquet et F. Morain. Isogeny volcanoes and the SEA algorithm. Technical Report LIX/RR/00/05, École polytechnique, Juin 2000.

[FR94] G. Frey et H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[Gal99] S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *J. Comput. Math*, 2:118–138, 1999.

[Gau00a] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer-Verlag, 2000.

[Gau00b] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École polytechnique, Dec. 2000.

[GHS01a] S.D. Galbraith, F. Hess, et N.P. Smart. Extending the ghs weil descent attack. `http://eprint.iacr.org/`, 2001.

[GHS01b] P. Gaudry, F. Hess, et N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. To appear in J. Crypt., 2001.

[GS99] S. Galbraith et N. Smart. A cryptographic application of Weil descent. In *Cryptography and Coding, 7th IMA Conference*, volume 1746 of *Lecture Notes in Comput. Sci.*, pages 191–200. springer–Verlag, 1999. Full paper is HP-LABS Technical Report (Number HPL-1999-70).

[Har] R. Harley. `http://cristal.inria.fr/~harley/ecdl/`.

[HM89] G. Henniart et J.-F. Mestre. Moyenne arithmético-géométrique p-adique. *C. R. Acad. Sci. Paris Sér. I Math.*, pages 391–195, 1989.

[HSS00] F. Hess, G. Seroussi, et N. P. Smart. Two topics in hyperelliptic cryptography. Technical Report CSTR-00-008, Department of Computer Science, University of Bristol, Juin 2000.

[IKNY98] T. Izu, J. Kogure, M. Noro, et K. Yokoyama. Efficient implementation of Schoof's algorithm. In K. Ohta et D. Pei, editors, *Advances in Cryptology – ASIACRYPT '98*, volume 1514 of *Lecture Notes in Comput. Sci.*, pages 66–79. Springer-Verlag, 1998. International Conference on the theory and application of cryptology and information security, Beijing, China, October 1998.

[Jac99] M. J. Jacobson, Jr. Applying sieving to the computation of quadratic class groups. *Math. Comp.*, 68(226):859–867, 1999.

[JL98] A. Joux et R. Lercier. Counting points of elliptic curves defined over $\mathrm{GF}(2^n)$. E-mail to the NMBRTHRY mailing list, Juin 1998.

[JMS01] Michael Jacobson, Alfred Menezes, et Andreas Stein. Solving elliptic curve discrete logarithm problems using weil descent. Cryptology ePrint Archive, Report 2001/041, 2001. http://eprint.iacr.org/.

[Kat85] S. A. Katre. Jacobsthal sums in terms of quadratic partitions of a prime. In K. Alladi, editor, *Number Theory*, volume 1122 of *Lecture Notes in Math.*, pages 153–162. Springer-Verlag, 1985. Proceedings of the 4th Matscience Conference held at Ootacamund, India, January 5-10, 1984.

[Kna92] A. W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *J. Crypto.*, 1:139–150, 1989.

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Phd thesis, University of California, Berkeley, 1996.

[Lan87] S. Lang. *Elliptic functions*. Springer-Verlag, 2nd edition, 1987.

[Len96] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56:227–241, 1996.

[Ler96] R. Lercier. Computing isogenies in F_{2^n}. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 197–212. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.

[Ler97a] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, École polytechnique, Juin 1997.

[Ler97b] R. Lercier. Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 379–392. Springer-Verlag, 1997. International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997, Proceedings.

[LM95] R. Lercier et F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In L. C. Guillou et J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Comput. Sci.*, pages 79–94, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[LM98] R. Lercier et F. Morain. Algorithms for computing isogenies between elliptic curves. In D. A. Buell et J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 77–96. American Mathematical Society, International Press, 1998.

[LM00] R. Lercier et F. Morain. Computing isogenies between elliptic curves over F_{p^n} using Couveignes's algorithm. *Math. Comp.*, 69(229):351–370, Jan. 2000.

[LN83] R. Lidl et H. Niederreiter. *Finite fields*. Number 20 in Encyclopedia of mathematics and its applications. Addison-Wesley, 1983.

[LST64] J. Lubin, J. P. Serre, et J. Tate. Elliptic curves and formal groups. In *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964*, 1964. Scanned copies available at `http://www.ma.utexas.edu/users/voloch/lst.html`.

[LV00] A. Lenstra et E. Verheul. Selecting cryptographic key size. In *Public Key Cryptography*, pages 446–465, 2000.

[McC89] K. McCurley. Cryptographic key distribution and computation in class groups,. In Kluwer Academic Publishers, editor, *NATO ASI Number Theory and applications*, pages 459–479, 1989.

[Men93] A. J. Menezes. *Elliptic curve public key cryptosystems*. Kluwer academic publishers, 1993.

[Mil87] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1987.

[Mor95] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *Journal de Théorie des Nombres de Bordeaux*, 7:255–282, 1995.

[Mor97] F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique $\geqslant 3$. *Utilitas Math.*, 52:241–253, Dec. 1997.

[MOV91] A. Menezes, T. Okamoto, et S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. In *Proceedings 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 80–89. ACM Press, 1991. May 6–8, New Orleans, Louisiana.

[MP98] V. Müller et S. Paulus. On the generation of cryptographically strong elliptic curves. Preprint, 1998.

[MQ01] A. Menezes et M. Qu. Analysis of the Weil descent attack of gaudry, hess and smart. In D. Naccache, editor, *Topics in cryptology – CT-RSA 2001*, volume 2020 of *LNCS*, pages 308–318, 2001.

[MST99] V. Müller, A. Stein, et C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.*, 68(226):807–822, 1999.

[Mül95] V. Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Technischen Fakultät der Universität des Saarlandes, 1995.

[MV90] A. Menezes et S. Vanstone. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math.*, 38:135–153, 1990.

[PH78] S. Pohlig et M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Inform. Theory*, IT–24:106–110, 1978.

[Pol78] J. M. Pollard. Monte Carlo methods for index computation $\pmod p$. *Math. Comp.*, 32(143):918–924, Juil. 1978.

[Rib72] P. Ribenboim. *L'arithmétique des corps.* Hermann, 1972.

[SA98] T. Satoh et K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comm. Math. Univ. Sancti Pauli*, 47:81–92, 1998.

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, Dec. 2000.

[Sat01] T. Satoh. Asymptotically fast algorithm for computing the Frobenius substitution and norms overunramified extension of p-adic number fields. Preprint, 2001.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[Sch87] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46:183–211, 1987.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[Ser68] J. P. Serre. *Corps locaux.* Hermann, 1968.

[Ser70] J. P. Serre. *Cours d'arithmétique.* Presses universitaires de France, 1970.

[Sha71] D. Shanks. Class number, a theory of factorization, and genera. In *Proc. Symp. Pure Math. vol. 20*, pages 415–440. AMS, 1971.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer–Verlag, 1986.

[Sil87] R. D. Silverman. The multiple polynomial quadratic sieve. *Math. Comp.*, 48(177):329–339, 1987.

[Sil99] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer–Verlag, 1999. Second printing.

[Sil00] R. Silverman. A cost-based security analysis of symmetric and assymetric key lengths. Bulletin Number 13 of RSA Security, Avr. 2000.

[Sma99] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Crypto.*, 12:193–196, 1999.

[Sma00] N. P. Smart. How secure are elliptic curves over composite extension fields? Technical Report CSTR-00-017, Department of Computer Science, University of Bristol, Nov. 2000.

[SS71] A. Schönhage et V. Strassen. Schnelle multiplikation grosser Zahlen. *Computing*, 7:281–292, 1971.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 273:238–241, Juil. 1971. Série A.

[Ver99] F. Vercauteren. $\#\mathrm{EC}(\mathrm{GF}(2^{1999}))$. E-mail to the `NMBRTHRY` mailing list, Oct. 1999.

[Vol97] J. F. Voloch. The discrete logarithm problem on elliptic curves and descents. Preprint, 1997.

[VPV01] F. Vercauteren, B. Preneel, et J. Vandewalle. A memory efficient version of Satoh's algorithm. In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 1–13, 2001.

[vzGG99] J. von zur Gathen et J. Gerhard. *Modern computer algebra.* Cambridge university press, 1999.

[Wat69] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.

[Web02] H. Weber. *Lehrbuch der Algebra*, volume III. Chelsea Publishing Company, New York, 1902.