Courbes Elliptiques

Samuel Gallay

27 août 2022

Table des matières

1 Introduction **2**

2 Qu'est-ce qu'une courbe elliptique ? **2**

2.1 Définitions 2

2.2 Loi de groupe 5

2.3 Le protocole Diffie-Hellman 7

3 Premières propriétés **8**

3.1 Morphismes et isogénies 8

3.2 j-invariant 10

3.3 Degré 10

3.4 Séparabilité 11

3.5 Morphisme de Frobenius 12

3.6 Isogénie duale 13

3.7 Torsion 14

3.8 Pairing de Weil, trace d'une isogénie 14

3.9 Trace du morphisme de Frobenius 16

3.10 Borne de Hasse 17

4 Cryptographie par isogénies entre courbes supersingulières **18**

4.1 Courbes supersingulières 18

4.2 Graphe des isogénies 18

4.3 Construction d'une courbe initiale 20

4.4 Torsions de la courbe initiale 21

4.5 Formules de Vélu 23

4.6 Le protocole cryptographique 23

A Code **25**

1 Introduction

L'objectif de ce mémoire est de donner une présentation en français de l'article De Feo *et al.* (2014) "*Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*" accessible à des lecteurs n'étant pas des experts des courbes elliptiques. Cet article présente un nouveau protocole cryptographique d'échange de clefs, nommé SIDH pour *Supersingular Isogenies Diffie-Hellman*, basé sur des isogénies entre courbes elliptiques supersingulières. L'intérêt de ce protocole est sa supposée sécurité face à un attaquant disposant d'un ordinateur quantique. En effet, la sécurité de la plupart des systèmes cryptographiques utilisés actuellement reposent soit sur le problème de la factorisation d'entiers, comme le protocole RSA, soit sur le problème du logarithme discret. L'inconvénient de ces deux problèmes est qu'un attaquant disposant d'un ordinateur quantique suffisamment puissant serait capable de les résoudre facilement, et donc de lire toutes les communications chiffrées.

La majeure partie de ce rapport sera consacrée à la présentation des outils mathématiques utilisés par SIDH en s'appuyant principalement sur le livre *The Arithmetic of Elliptic Curves* de Silverman (1992). Ce livre a l'avantage d'être utilisé comme une oeuvre de référence par la communauté mathématique de la cryptographie des courbes elliptiques, dans le sens où plusieurs articles que j'ai pu rencontrer renvoient le lecteur souhaitant une preuve des résultats énoncés directement au texte de Silverman. Ce texte possède l'inconvénient d'utiliser régulièrement des outils de géométrie algébrique ou de la théorie de Galois, ce qui le rend difficilement accessible à un étudiant de Licence. J'ai aussi consulté le livre de Washington (2008) sur les courbes elliptiques qui présente souvent avec des outils plus simples (et des méthodes parfois calculatoires !) les résultats nécessaires à l'étude des courbes elliptiques.

2 Qu'est-ce qu'une courbe elliptique ?

Cette première partie cherche à donner une définition de ce qu'est une courbe elliptique, puis présente la loi de groupe que possède une courbe elliptique, et enfin présente un premier protocole d'échange de clefs très régulièrement utilisé de nos jours.

2.1 Définitions

La tâche consistant à donner la définition de ce qu'est une courbe elliptique s'avère bien plus délicate que ce que j'imaginais dans un premier temps. En effet, il est possible de donner plusieurs définitions équivalentes d'une courbe elliptique présentant chacune leur intérêt mais dont la preuve de ladite équivalence requiert des outils avancés. Je vais donc présenter en dessous deux définitions de ce qu'est une courbe elliptique, et sans démontrer l'équivalence je vais essayer de donner l'intuition de la raison pour laquelle elles représentent le même objet. La première définition utilise de nombreux concepts venant de la géométrie algébrique et la seconde en revanche est beaucoup plus élémentaire, et à l'avantage de pouvoir être manipulée directement par un ordinateur.

Définition 2.1 (Géométrie algébrique)**.** *Une courbe elliptique est une courbe projective lisse de genre* 1 *dont a spécifié un point.*

Définition 2.2 (Pratique)**.** *Soit K un corps de caractéristique différente de* 2 *et de* 3*. Une courbe elliptique définie sur K est un ensemble de la forme $\{(x, y) \in \overline{K} \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$ ou a et b sont des éléments de K tels que la quantité $\Delta = -16(4a^3 + 27b^2)$ soit non nulle.*

Dans toute la suite, je suppose que les corps utilisés ne sont ni de caractéristique 2, ni de caractéristique 3.

Fixons pour cette partie un corps K (de caractéristique différente de 2 et de 3) et notons $\overline{K}$ sa clôture algébriques. Nous allons maintenant essayer de comprendre la première définition, et d'expliquer pourquoi une courbe elliptique au sens de la définition pratique est bien une courbe elliptique au sens de la première. Le premier terme à comprendre est le mot *projectif*.

Définition 2.3. *Posons $\mathcal{A} = \overline{K}^3 \setminus (0,0,0)$. On définit une relation d'équivalence sur $\mathcal{A}$ de la sorte : étant donné (x,y,z) et (x',y',z') deux éléments de A, ces derniers sont équivalents s'il existe une constante $\lambda \in \overline{K}^\times$ telle que $(x,y,z) = (\lambda x', \lambda y', \lambda z')$.*

L'espace projectif $\mathbb{P}^2$ sur K est définit comme le quotient de $\mathcal{A}$ par cette relation d'équivalence.

De façon moins formelle, l'espace $\mathbb{P}^2$ est l'ensemble des droites vectorielles de $\overline{K}^3$. Dans notre cadre, l'espace projectif sert principalement à donner un cadre rigoureux à l'ajout de points à l'infini dans l'espace. Pour maintenant donner un sens à la notion de *courbe*, il faut définir ce qu'est un ensemble algébrique, puis ce qu'est une variété.

Définition 2.4. *Soit I un idéal de $\overline{K}[X,Y,Z]$ engendré par des polynômes homogènes. On définit l'ensemble $Z(I)$ par $Z(I) = \{P \in \mathbb{P}^2 : f(P) = 0$ pour tout f homogène de $I\}$.*

Un ensemble est dit algébrique s'il est de la forme $Z(I)$ pour un certain I.

La notation $Z(I)$ désigne ici l'ensemble des zéros communs à tous les polynômes homogènes de I. On ne considère que les polynômes homogènes de I puisque dans l'espace projectif la propriété $f(P) = 0$ n'est pas bien définie pour des polynômes qui ne seraient pas homogènes. En effet, l'espace projectif est définit par un quotient et cette propriété n'est pas indépendante du choix d'un représentant. En revanche, cette propriété l'est pour des polynômes homogènes.

Donnons dès à présent un exemple d'ensemble algébrique, qui permettra d'illustrer la définition et de faire un premier lien entre les deux définitions d'une courbe elliptique.

Soient a et b dans K, et considérons le polynôme de $f(x,y) = y^2 - x^3 - ax - b$ de $K[x,y]$. L'intérêt de tels polynômes est que l'ensemble leurs zéros dans $\overline{K}$ (que nous noterons aussi $Z(f)$ ou $Z(\langle f \rangle)$) définit une courbe elliptique au sens de la définition pratique. Un tel polynôme n'est pas homogène, mais un procédé simple permet de l'homogénéiser. Posons $F(X,Y,Z) = Z^3 f(\frac{X}{Z}, \frac{Y}{Z})$. Un tel F est un polynôme homogène de $K[X,Y,Z]$, puisque $F(X,Y,Z) = Z^3\big((\frac{Y}{Z})^2 - (\frac{X}{Z})^3 - a\frac{X}{Z} - b\big) = Y^2Z - X^3 - aXZ^2 - bZ^3$. En considérant $\langle F \rangle$ l'idéal de $\overline{K}[X,Y,Z]$ engendré par F, $Z(\langle F \rangle)$ définit bien un ensemble algébrique. Pour alléger les notations, on notera $Z(F)$ à la place de $Z(\langle F \rangle)$.

Continuons de faire le lien entre $\overline{K}^2$ et $\mathbb{P}^2$. Pour x, y et z des éléments de $\overline{K}$, la notation $[x,y,z]$ désigne la classe d'équivalence de (x,y,z) dans $\mathbb{P}^2$.

Proposition 2.5. *Notons $U = \{[x,y,z] \in \mathbb{P}^2 \mid z \neq 0\}$. L'application $\phi : \overline{K}^2 \to U$ définie par $\phi(x,y) = [x,y,1]$ est bijective.*

Démonstration. Soit $[x,y,z] \in U$. On vérifie facilement que le couple $(\frac{x}{z}, \frac{y}{z})$ est l'unique antécédent de $[x,y,z]$ par ϕ. □

La proposition précédente montre que $\mathbb{P}^2$ contient une copie de $\overline{K}^2$. Montrons que $Z(F)$ contient une copie de $Z(f)$ par le même isomorphisme.

Proposition 2.6. *Avec les mêmes notations que la question précédente, ϕ induit une bijection entre $Z(f)$ et $Z(F) \cap U$.*

Démonstration. Soit $(x, y) \in \overline{K}^2$ tel que $f(x, y) = 0$, alors $F([x, y, 1]) = 1^3 f(\frac{x}{1}, \frac{y}{1}) = f(x, y) = 0$. Réciproquement, soit $[x, y, z] \in U$. Si $F([x, y, z]) = 0$, alors $z^3 f(\frac{x}{z}, \frac{y}{z}) = 0$, donc $f(\frac{x}{z}, \frac{y}{z}) = 0$. □

On peut maintenant s'intéresser aux points de $Z(F) \setminus U$. Soit $[x, y, z] \in Z(F) \setminus U$. Alors $z = 0$ et $0 = F(x, y, z) = F(x, y, 0) = -x^3$, donc $x = 0$. Ainsi $[x, y, z] = [0, y, 0] = [0, 1, 0]$, car y ne peut pas être nul puisque $[0, 0, 0]$ n'appartient pas à $\mathbb{P}^2$. On vient de montrer que le seul point de $Z(F)$ qui n'appartient pas à U est $[0, 1, 0]$, et c'est ce point que l'on considérera comme "point à l'infini" dans $\overline{K}^2$. Ainsi on a une correspondance simple entre $Z(f) \cup \{\infty\}$ et $Z(F)$. L'espace projectif a un intérêt théorique puisque beaucoup de résultats s'y expriment de façon bien plus élégantes, mais l'espace K^2 est plus facile à se représenter mentalement.

Définition 2.7. *À un ensemble algébrique V, on associe un idéal :*

$$I(V) = \{f \in \overline{K}[X, Y, Z] : f \text{ est homogène et } f(P) = 0 \text{ pour tout } P \in V\}$$

Si $I(V)$ est premier dans $\overline{K}[X, Y, Z]$, on dit que V est une variété (projective). Si $I(V)$ est engendré par des polynômes homogènes de $K[X, Y, Z]$, on dit que V est définie sur K.

Continuons l'exemple précédent en montrant que $Z(f)$ est une variété. Le polynôme f défini précédemment est un polynôme de homogène irréductible de $K[X, Y, Z]$. Quel que soit l'idéal I de $K[X, Y, Z]$, il est toujours vrai que $I \subseteq I(Z(I))$, donc $\langle F \rangle \subseteq I(Z(F))$. Dans ce cas particulier, il se trouve que la réciproque est vraie. Soit $g \in I(Z(F))$: par la version forte du théorème des zéros de Hilbert (que nous ne démontrons pas ici), il existe $n \in \mathbb{N}^*$ tel que $g^n \in \langle F \rangle$. Puisque $\overline{K}[X, Y, Z]$ est factoriel et puisque F est irréductible, $\langle F \rangle$ est premier. Ainsi $g \in \langle F \rangle$ et donc $I(Z(F)) = \langle F \rangle$. On en déduit que V est une variété (projective) définie sur K.

Nous pouvons enfin donner la définition d'une courbe projective :

Définition 2.8. *Une courbe (projective) est une variété de dimension 1 de l'espace (projectif).*

Je n'ai pas envie de définir formellement (de manière purement algébrique) la dimension d'une variété, mais on peut se convaincre que $Z(f) = \{(x, y) \in \overline{K}^2 \mid y^2 = x^3 + ax + b\}$ est de dimension 1 par analogie avec le cas réel puisque étant donné une valeur de $x \in \overline{K}$, il existe au plus deux valeurs de $y \in \overline{K}$ telles que $(x, y) \in Z(f)$. La condition sur Δ implique que la variété $Z(F)$ est lisse, dans le sens où elle ne possède ni croisements ni rebroussements (il est important que l'on puisse définir une tangente en chaque point de la courbe). Le dernier concept qui est plus délicat est celui de genre d'une variété, qui intuitivement correspond au nombre de *trous* de la variété, l'outil clef pour le définir est le théorème de Riemann-Roch. Le point spécifié de la courbe projective dans la définition formelle est le point $[0, 1, 0]$, qui correspond au point à l'infini dans la définition pratique.

J'espère avoir pu vous convaincre qu'une courbe elliptique donnée par la deuxième définition constitue bien une courbe elliptique au sens de la première définition. Une preuve de l'équivalence peut être trouvée dans Silverman (1992), à la proposition III.3.1.

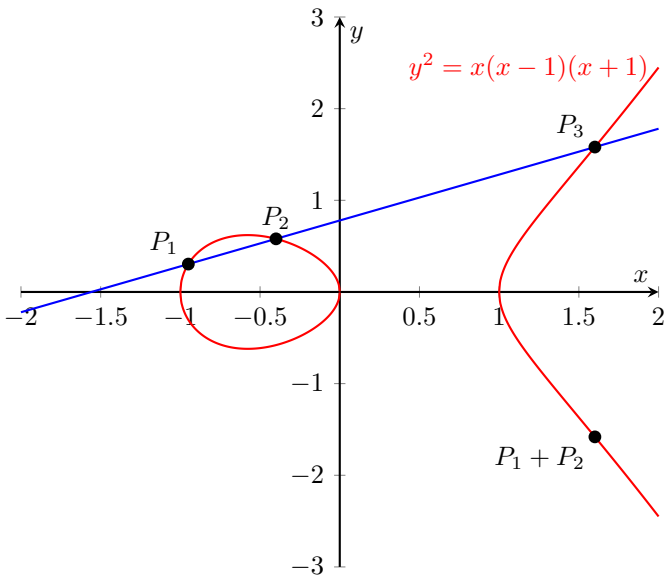
Je pense qu'il était important de mentionner le fait que les courbes elliptiques soient des objets d'étude important de la géométrie algébrique. Par exemple la preuve par Andrew Wiles la conjecture de Shimura-Taniyama-Weil concernant des courbes elliptiques a permis la démonstration du dernier théorème de Fermat. En revanche, l'étude de la cryptographie utilisant les courbes elliptiques peut se faire, quitte à admettre certains résultats, uniquement à partir de la seconde définition. Le lecteur peut maintenant oublier la partie précédente puisque que lorsque l'on considérera une courbe elliptique E définie sur K, ce que l'on notera E/K, cela signifiera que l'on s'est donné une équation $y^2 = x^3 + ax + b$, a et b étant des éléments de K tels que $\Delta = -16(4a^3 + 27b^2)$ soit non nul, et que l'on étudiera l'ensemble des solutions de cette équation dans $\overline{K}^2 \cup \{\infty\}$ avec la convention que ∞ est solution de l'équation.

2.2 Loi de groupe

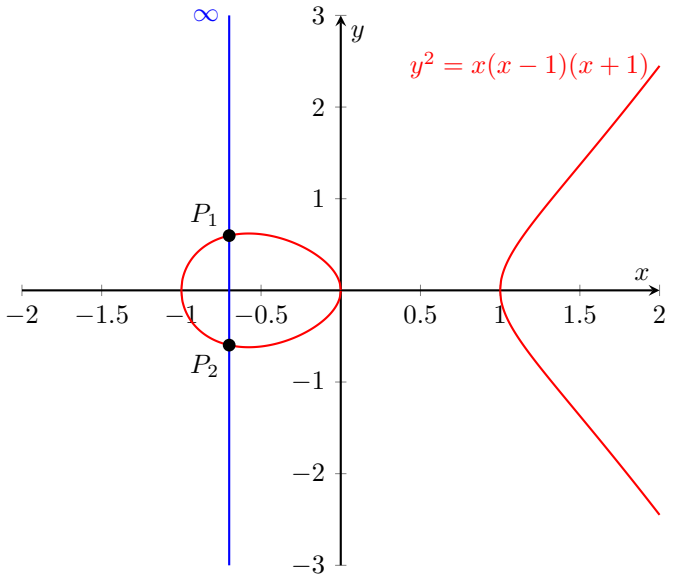
Ce qui rend les courbes elliptiques intéressantes, notamment en cryptographie, c'est que l'on peut les munir d'une loi de groupe. Soit E/K une courbe elliptique. Nous allons construire une loi sur E notée $+$ telle que $(E, +, \infty)$ formera un groupe abélien.

Définition 2.9. *Pour définir la somme de deux points P_1 et P_2, on commence par tracer la droite $\mathcal{D}$ entre P_1 et P_2. Cette droite possède une troisième intersection P_3 avec la courbe E. On note alors $P_1 + P_2$ la réflexion de P_3 par rapport à l'axe des abscisses.*

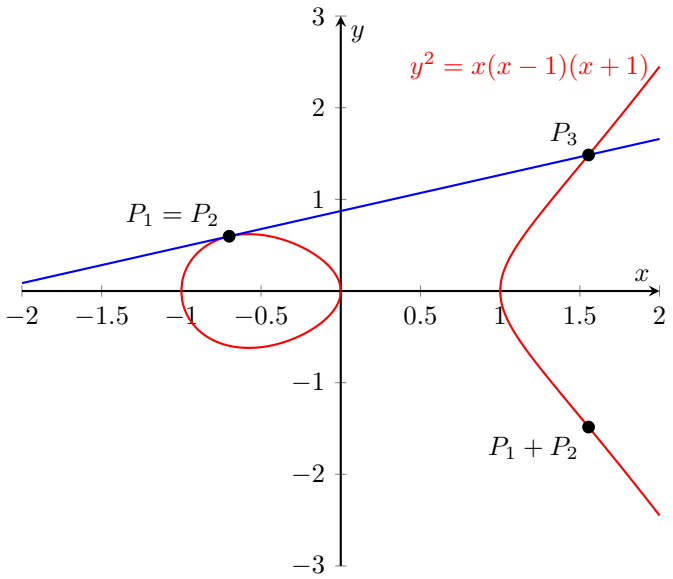
Cette définition d'est pas claire pour plusieurs raisons. Quelle sont les droites passant par ∞ par exemple ? On souhaite que ∞ soit l'élément neutre soit le neutre de cette loi, donc si par exemple $P_1 = \infty$, on définit : $P_1 + P_2 = \infty + P_2 = P_2$. Maintenant traitons le cas où les deux points sont différents de ∞. Notons ces deux points P_1 et P_2, et leurs coordonnées (x_1, y_1) et (x_2, y_2) :



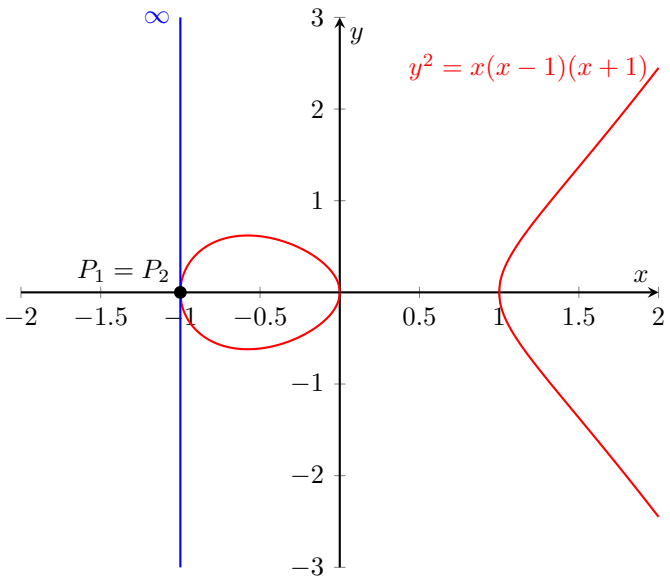
Cas $x_1 \neq x_2$. On considère la droite $\mathcal{D}$ passant par P_1 et P_2. La pente de cette droite est $m = \frac{y_2 - y_1}{x_2 - x_1}$ et son équation est $y = m(x - x_1) + y_1$. Les points d'intersection entre la droite $\mathcal{D}$ et E sont les points (x, y) vérifiant $y^2 = x^3 + ax + b$ et $y = m(x - x_1) + y_1$. En combinant les deux équations, on obtient $(m(x - x_1) + y_1)^2 = x^3 + ax + b$. En ne cherchant à expliciter que les termes de degré 2 et 3 en x, on obtient : $x^3 - m^2x^2 + \alpha x + \beta = 0$. Cette équation est de degré 3 en x, mais on en connait déjà deux solutions x_1 et x_2, donc en utilisant les relations racines coefficients, on obtient $x_1 + x_2 + x_3 = m^2$ soit $x_3 = m^2 - x_1 - x_2$ où x_3 est la troisième solution. La valeur de y_3 est $m(x_3 - x_1) + y_1$ en réutilisant l'équation de la droite. On définit le point $P_1 + P_2$ comme le point de coordonnées $(x_3, -y_3)$.



Cas $x_1 = x_2$ et $y_1 \neq y_2$. La droite $\mathcal{D}$ est verticale et on définit $P_1 + P_2$ comme valant ∞.



Cas $P_1 = P_2$ et $y_1 \neq 0$. On considère pour $\mathcal{D}$ dans ce cas là la tangente à E passant par P_1. Pour trouver la pente de la tangente, on dérive l'équation de la courbe par rapport à x : $2y\frac{dy}{dx} = 3x^2 + a$, donc $m = \frac{3x_1^2+a}{2y_1}$ puisque $y_1 \neq 0$. On construit $P_1 + P_1$ comme précédemment : la droite $\mathcal{D}$ possède une intersection de multiplicité double avec$E$ en P_1 puisqu'elle est tangente, et on obtient la troisième intersection en utilisant les relations racines-coefficients.



Cas $P_1 = P_2$ et $y_1 = 0$. Dans le cas précédent, on peut montrer que si $y_1 = 0$, alors $3x_1^2 + a \neq 0$. On montre plus précisément que $\Delta \neq 0$ si et seulement si $(x^3 + ax + b) \wedge (3x^2 + a) = 1$. Dans ce cas particulier $y_1 = 0$, on définit $P_1 + P_1$ comme valant ∞.

Remarque 2.10. Il est remarquable que la loi définie ci-dessus soit une loi de groupe. Le point ∞ est l'élément neutre par définition. Il est facile de voir que la loi est commutative. En effet, la droite passant par P_1 et P_2 est la même que la droite passant par P_2 et P_1. Il est facile de calculer l'opposé d'un point :

Proposition 2.11. *L'opposé de l'élément (x_1, y_1) est l'élément $(x_1, -y_1)$.*

Démonstration. Si $y_1 \neq 0$, $y_1 \neq -y_1$ donc $(x_1, y_1) + (x_1, -y_1) = \infty$ par définition, on est dans le cas 2. Si $y_1 = 0$, on est dans le cas 4 et donc il reste vrai que $(x_1, y_1) + (x_1, -y_1) = \infty$. □

Le plus dur est de montrer l'associativité de cette loi. Il est possible de tout écrire à la main, mais il est aussi possible d'utiliser le théorème de Riemann-Roch, comme le fait Silverman (1992) au théorème III.3.4e.

2.3 Le protocole Diffie-Hellman

Nous décrivons dans cette section le protocole d'échange de clefs de Diffie et Hellman. Soit $G = \langle g \rangle$ un groupe monogène supposé connu de tous. On suppose que le générateur g ainsi que l'ordre n du groupe sont publics.

Deux individus Alice et Bob cherchent à partager un élément du groupe G sans qu'un espion Eve capable d'écouter toutes leurs communications ne puisse l'identifier. Cet élément peut par exemple servir de clef secrète pour un chiffrement symétrique comme AES permettant de sécuriser la communication entre Alice et Bob. Voici les étapes suivies par Alice et Bob :

1. Alice et Bob choisissent chacun un entier compris entre 0 et $n-1$ qu'ils gardent secret. Notons a l'entier d'Alice et b celui de Bob.
2. Alice calcule g^a et l'envoie à Bob. Bob calcule g^b et l'envoie à Alice.
3. Alice calcule $(g^b)^a$ connaissant a et g^b. Bob calcule $(g^a)^b$ connaissant b et g^a.

Puisque $(g^b)^a = g^{ab} = (g^a)^b$, Alice et Bob partagent un secret commun. Ève ayant écouté toutes les communications connait g, g^a et g^b et cherche à retrouver g^{ab} : c'est le *Computational Diffie-Hellman problem* (CDH).

Un problème très proche de CDH est le *problème du logarithme discret* (DLP), qui consiste connaissant g et g^a à retrouver a. Évidemment, si Ève parvient à résoudre le DLP dans le groupe G, Ève peut résoudre le problème CDH et donc déchiffrer les communications entre Alice et Bob. Il se trouve que dans de nombreux groupes, on ne sait pas faire mieux que de résoudre le DLP pour résoudre le problème CDH.

L'opération consistant à calculer g^a en connaissant a (l'inverse du DLP) peut se faire en $O(\log a) = O(\log n)$ opérations dans le groupe par l'algorithme d'exponentiation rapide. Sur un groupe générique, c'est à dire sans information particulière sur le groupe, les meilleurs algorithmes pour résoudre le DLP sont de complexité $O(\sqrt{n})$: voir l'algorithme ρ de Pollard par exemple. Un tel groupe serait idéal pour Alice et Bob : l'échange de clef pour de larges valeurs de n est peu couteux et le problème du logarithme discret est très couteux.

Il faut ensuite se poser la question de quel groupe utiliser dans ce protocole cryptographique. En effet, dans certains groupe le logarithme discret est très facile à résoudre : Dans $(\mathbb{Z}/n\mathbb{Z}, +)$ il suffit de calculer une relation de Bézout par l'algorithme d'Euclide ce qui est très peu couteux. Dans le groupe multiplicatif de $\mathbb{F}_q$, les algorithmes de calcul d'indice peuvent résoudre le logarithme discret en temps sous-exponentiel (ce qui ne veut pas dire polynômial). Enfin, sur certaines courbes elliptiques les meilleurs algorithmes connus pour résoudre le problème du logarithme fonctionnent en temps exponentiel : c'est de cette façon que l'on utilise généralement les courbes elliptiques dans des protocoles d'échanges de clefs sur internet (par exemple le 's' dans 'https').

3 Premières propriétés

3.1 Morphismes et isogénies

Cette partie est consacrée à l'étude des morphismes entre courbes elliptiques. Les isogénies sont des morphismes particuliers qui seront utilisés dans la description du protocole SIDH.

Définition 3.1. *Soient E_1 et E_2 deux courbes elliptiques définies sur K. Un morphisme $\phi : E_1 \to E_2$ est une application de la forme $\phi(x, y) = (R_1(x, y), R_2(x, y))$ avec R_1 et R_2 des fractions rationnelles en x et y qui envoie ∞_{E_1} sur ∞_{E_2}.*

Remarque 3.2. A priori les fractions rationnelles peuvent être définies sur n'importe extension de L de K. On dit alors que le morphisme est défini sur L.

Théorème 3.3. *Soit E_1/K et E_2/K deux courbes elliptiques. Un morphisme $\phi : E_1 \to E_2$ défini sur L une extension de K (possiblement égale à K) induit un morphisme de groupe entre $E_1(L)$ et $E_2(L)$.*

Démonstration. Admise. □

Le théorème précédent permet de donner les définitions usuelles associées aux ensembles d'endomorphismes. Soit E/K, E_1/K et E_2/K trois courbes elliptiques définies sur K et soit L une extension de K.

Définition 3.4. *On note $\mathrm{Hom}_L(E_1, E_2)$ l'ensemble des morphismes de E_1 dans E_2 définis sur L. En définissant l'addition de morphismes comme l'addition point par point, $\mathrm{Hom}_L(E_1, E_2)$ devient un groupe abélien.*

Définition 3.5. *On note $\mathrm{End}_L(E)$ le groupe $\mathrm{Hom}_L(E, E)$. Muni de la loi de composition des morphismes, $\mathrm{End}_L(E)$ est un anneau. Les éléments de $\mathrm{End}_L(E)$ sont appelés endomorphismes de E.*

Nous donnons maintenant une forme plus simple aux isogénies :

Proposition 3.6. *Un morphisme ϕ peut toujours se mettre sous la forme $\phi(x,y) = (r_1(x), r_2(x)y)$ avec r_1 et r_2 des fonctions rationnelles (i.e. des quotients de polynômes en x).*

Démonstration. Soit $R(x,y)$ une fraction rationnelle. Puisque les points de E vérifient $y^2 = x^3 + ax + b$, on peut éliminer les puissances de y plus grande que 2 au numérateur et au dénominateur de R. On peut donc supposer R de la forme :

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} = \frac{(p_1(x) + p_2(x)y)(p_3(x) - p_4(x)y)}{p_3(x)^2 - p_4(x)^2y^2} = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

On a multiplié le dénominateur et le numérateur par la quantité conjuguée $(p_3 - p_4y)$ et réutilisé l'équation de la courbe pour éliminer y au dénominateur.

Le morphisme ϕ peut se mettre sous la forme $\phi(x,y) = (R_1(x,y), R_2(x,y))$ avec R_1 et R_2 de la forme donnée ci-dessus. Puisque ϕ est un morphisme de groupes, en utilisant trois fois la proposition 2.11, on obtient $(R_1(x,-y), R_2(x,-y)) = \phi(x,-y) = \phi(-(x,y)) = -\phi(x,y) = (R_1(x,y), -R_2(x,y))$. On peut donc réécrire $R_1(x,y) = p_1(x)/q_1(x)$ et $R_2(x,y) = p_2(x)y/q_2(x)$. On obtient bien la forme désirée. □

Remarque 3.7. Si deux fractions rationnelles en x prennent les mêmes valeurs sur une infinité de points alors elles sont égales. Les isogénies sont définies sur $E(\overline{K})$ (les points de la courbe elliptique sur la clôture algébrique de K) qui est infini, donc l'écriture précédente est unique.

On peut donner maintenant la définition très simple d'une isogénie :

Définition 3.8. *Une isogénie est un morphisme non constant.*

Notons dès à présent qu'étant donné deux courbes elliptiques définies sur un corps K, il est a priori difficile de trouver une isogénie entre elles.

Théorème 3.9. *Une isogénie est surjective.*

Démonstration. C'est magique ! □

Proposition 3.10. *Soit E/K et soit $m \in \mathbb{Z}$. L'application $[m] : E \to E, P \mapsto mP$ est un endomorphisme de E défini sur K.*

Proposition 3.11. *Le morphisme $[m]$ commute avec tous les morphismes.*

Démonstration. Soit $\phi : E_1 \to E_2$ un morphisme et $m \in \mathbb{Z}$. Soit $P \in E_1$. $(\phi \circ [m]_{E_1})(P) = \phi(P + \ldots + P) = \phi(P) + \ldots + \phi(P) = ([m]_{E_2} \circ \phi)(P)$. □

Théorème 3.12. *Soient E_1 et E_2 deux courbes elliptiques définies sur K. Un isomorphisme de courbes elliptiques entre E_1 et E_2 est toujours de la forme $(x,y) \mapsto (u^2x, u^3y)$ avec $u \in \overline{K}$.*

Démonstration. Voir la proposition III.3.1 (b) dans Silverman (1992). □

3.2 j-invariant

Dans cette partie noue introduisons la notion de j-invariant :

Définition 3.13. *Soit $E/K : y^2 = x^3 + ax + b$ une courbe elliptique définie sur K. Son discriminant Δ est non nul et défini par $\Delta = -16(4a^3 + 27b^2)$. Son j-invariant est défini par :*

$$j = -1728\frac{(4a)^3}{\Delta} = 1728\frac{4a^3}{4a^3 + 27b^2}$$

Cette quantité a la particularité de caractériser complètement les classes de $\overline{K}$-isomorphismes de courbes elliptiques définies sur K.

Théorème 3.14. *Soient deux courbes elliptiques E_1 et E_2 définies sur un corps K par $y^2 = x^3 + a_1x + b_1$ et $y^2 = x^3 + a_2x + b_2$ respectivement. Notons j_1 et j_2 leurs j-invariants respectifs. Les courbes E_1 et E_2 sont isomorphes sur $\overline{K}$ si et seulement si $j_1 = j_2$.*

Démonstration. Supposons d'abord que $j_1 = j_2$ et explicitons un isomorphisme entre E_1 et E_2. Dans le cas où a_1 est différent de 0, j_1 est différent de 0 et donc j_2 et a_2 le sont aussi. Il existe donc $\mu \in \overline{K}$ tel que $a_2 = \mu^4 a_1$. Ainsi,

$$\frac{4a_2^3}{4a_2^3 + 27b_2^2} = \frac{4a_1^3}{4a_1^3 + 27b_1^2} = \frac{4\mu^{-12}a_2^3}{4\mu^{-12}a_2^3 + 27b_1^2} = \frac{4a_2^3}{4a_2^3 + 27\mu^{12}b_1^2}$$

Finalement $b_2^2 = \mu^{12}b_1^2$, donc $b_2 = \pm\mu^6 b_1$. Quitte à remplacer μ par $i\mu$, où $i \in \overline{K}$ est tel que $i^2 = -1$, on peut supposer que $a_2 = \mu^4 a_1$ et $b_2 = \mu^6 b_1$. L'application $\psi : E_1 \to E_2$ définie par $\psi(x, y) = (\mu^2 x, \mu^3 y)$ est bien définie et est un morphisme. En effet, étant donné (x, y) dans E_1, $(\mu^3 y)^2 = \mu^6 y^2 = \mu^6 x^3 + \mu^6 a_1 x + \mu^6 b_1 = (\mu^2 x) + a_2(\mu^2 x) + b_2$ donc $\psi(x, y)$ appartient à E_2. Il est clair que ψ est bijective et que sa réciproque est aussi un morphisme : E_1 et E_2 sont donc isomorphes.

Dans le cas où $a_1 = 0$, $j_2 = j_1 = 0$, donc $a_2 = 0$. Puisque les discriminants de E_1 et E_2 sont tous deux non nuls, b_1 et b_2 sont différents de 0. Il existe donc $\mu \in \overline{K}$ tel que $b_2 = \mu^6 b_1$, on peut donc conclure comme précédemment.

Pour montrer la réciproque, nous utilisons le théorème 3.12 que nous n'avons pas démontré ici. Si E_1 et E_2 sont isomorphes, alors il existe $u \in \overline{K}$ tel que pour tout $(x, y) \in \overline{K}^2$ $(x, y) \in E_1$ si et seulement si $(u^2 x, u^3 y) \in E_2$. Ainsi pour tout $(x, y) \in \overline{K}^2$,

$$u^6(x^3 + a_1x + b_1) = u^6y^2 = (u^3y)^2 = (u^2x)^3 + a_2(u^2x) + b_2 = u^6(x^3 + a_2u^{-4}x + u^{-6}b_2)$$

Le corps $\overline{K}$ étant infini E_1 est infini et ceci montre que $a_1 = a_2u^{-4}$ et $b_1 = u^{-6}b_2$. Alors

$$j_1 = 1728\frac{4a_1^3}{4a_1^3 + 27b_1^2} = 1728\frac{4u^{-12}a_2^3}{4u^{-12}a_2^3 + 27u^{-12}b_2} = 1728\frac{4a_2^3}{4a_2^3 + 27b_2^2} = j_2$$

□

Remarque 3.15. Deux cas particuliers sont intéressants. Les courbes de la forme $E/K : y^2 = x^3 + b$ avec $b \neq 0$ sont de j-invariant 0. Les courbes de la forme $E/K : y^2 = x^3 + ax$ sont elles de j-invariant 1728.

3.3 Degré

Cette sous-partie introduit la notion de degré d'un morphisme.

Définition 3.16 (Degré d'un morphisme)**.** *. Soit $\phi : E_1 \to E_2$ une isogénie. La fonction $\phi^* : K(E_2) \to K(E_1)$ définie par $\phi^*(f) = f \circ \phi$ est une injection entre deux corps. On peut montrer que l'extension $K(E_1)/\phi^*(K(E_2))$ est finie (voir R. Hartstone, Algebraic Geometry). On définit le degré de ϕ comme le degré de cette extension.*

Par convention, on décrète que le degré du morphisme $[0]$ vaut 0.

Le degré d'une extension finie L/K est la dimension de L en temps que K-espace vectoriel et est noté $[L : K]$.

Proposition 3.17. *Le degré est multiplicatif. Soient $\phi : E_1 \to E_2$ et $\psi : E_2 \to E_3$ deux morphisme. Alors* $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$

Démonstration. Le cas où ϕ ou ψ est nul est trivial. Dans le cas ou ϕ et ψ sont des isogénies, cela vient directement de la multiplicativité du degré d'une extension de corps : $\deg(\psi \circ \phi) = [K(E_3) : K(E_1)] = [K(E_3) : K(E_2)][K(E_2) : K(E_1)] = \deg(\psi)\deg(\phi)$. La preuve de la multiplicativité du degré d'extensions finies peut se faire de façon élémentaire en considérant des bases $(e_i)_i$ du $K(E_1)$-espace vectoriel $K(E_2)$ et $(f_j)_j$ du $K(E_2)$-espace vectoriel $K(E_3)$ et en montrant que la famille $(e_i f_j)_{ij}$ forme une base du $K(E_1)$-espace vectoriel $K(E_3)$. □

Proposition 3.18. *Soit E une courbe elliptique. L'anneau* $\mathrm{End}(E)$ *est intègre.*

Démonstration. Soit ϕ et ψ deux morphismes de E tels que $\phi \circ \psi = 0$. Par la proposition 3.17, $(\deg \phi)(\deg \psi) = \deg(\phi \circ \psi) = \deg[0] = 0$. Ainsi $\deg \phi = \deg \psi = 0$ donc $\phi = \psi = 0$. □

On cherche maintenant à avoir une forme canonique pour effectuer des calculs sur les isogénies, et pour pouvoir calculer plus facilement leur degré. La proposition suivante va nous permettre de lire le degré d'une isogénie sur son expression canonique définie précédemment.

Proposition 3.19. *Soit $\phi = (r_1(x), r_2(x)y)$ une isogénie. La fonction rationnelle r_1 peut se mettre sous la forme $r_1(x) = p(x)/q(x)$ avec p et q des polynômes premiers entre eux. Le degré de ϕ est alors égal au maximum des degrés de p et de q.*

Démonstration. Admise. □

3.4 Séparabilité

Avec le degré, une autre propriété importante des isogénies est leur caractère séparable ou non.

Définition 3.20. *Une isogénie ϕ est dite séparable si c'est le cas de l'extension $K(E_1)/\phi^*(K(E_2))$. Une isogénie qui n'est pas séparable est dite inséparable.*

On rappelle brièvement la notion de séparabilité pour une extension de corps. Une extension algébrique L/K est dite séparable si pour tout $a \in L$, le polynôme minimal de a à coefficients dans K ne contient que des racines simples (dans $\overline{K}$). On dit qu'une extension est inséparable quand elle n'est pas séparable, c'est à dire quand il existe un élément dont le polynôme minimal sur K n'est pas à racines simples dans $\overline{K}$. Les extensions purement inséparables sont un cas particulier d'extensions séparables où tous les éléments $a \in L \setminus K$ ont un polynôme qui n'est pas à racines simples.

Un outil pour étudier la séparabilité d'une extension de corps est la notion de degré de séparabilité (ou degré séparable). Soit L/K une extension algébrique. Le degré de séparabilité de L/K noté $[L : K]_s$ est défini formellement comme le nombre de prolongements à L du morphisme d'inclusion de K dans K.

Proposition 3.21. *Les seules propriétés que nous allons utiliser sont les suivantes :*

1. *Le degré de séparabilité est multiplicatif :* $[M : K]_s = [M : L]_s[L : K]_s$.
2. *Pour une extension algébrique* L/K, $[L : K]_s$ *divise* $[L : K]$. *On note* $[L : K]_i$ *l'unique entier tel que* $[L : K]_s[L : K]_i = [L : K]$. *C'est le degré d'inséparabilité de l'extension.*
3. *Le degré d'inséparabilité est multiplicatif et est égal à une puissance de la caractéristique.*
4. *L'extension* L/K *est séparable si et seulement si* $[L : K]_s = [L : K]$ *si et seulement si* $[L : K]_i = 1$.
5. *On dit que l'extension* L/K *est purement inséparable si* $[L : K]_s = 1$.
6. *Une extension purement inséparable non triviale est inséparable.*

Définition 3.22. *On définit alors le degré de séparabilité et d'inséparabilité* $\deg_s(\phi)$ *et* $\deg_i(\phi)$ *d'une isogénie* $\phi : E_1 \to E_2$ *comme les degré de séparabilité et d'inséparabilité de l'extension* $K(E_1)/\phi^*(K(E_2))$.

Ici encore, la forme canonique donnée aux isogénies précédemment permet de donner caractérisation plus simple de la séparabilité.

Proposition 3.23. *Une isogénie* $\phi(x, y) = (r_1(x), r_2(x)y)$ *est séparable si et seulement si* $r_1'(x) \neq 0$.

Démonstration. Admise. □

3.5 Morphisme de Frobenius

Nous introduisons maintenant le morphisme de Frobenius, qui est l'exemple le plus important d'isogénie inséparable.

Définition 3.24. *Soit* $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ *une courbe elliptique avec* $q = p^n$. *Pour tout* r *puissance de* p *on définit la courbe* $E^{(r)}$ *par l'équation* $y^2 = x^3 + a^r x + b^r$. *On appelle morphisme de Frobenius l'application* $\pi_r : E \to E^{(r)}$ *qui à* (x, y) *associe* (x^r, y^r). *On remarque que si* r *est une puissance de* q, π_r *est un endomorphisme.*

Remarque 3.25. Par les propositions 3.19 et 3.23, on déduit immédiatement que π_r est une isogénie inséparable de degré r. Les propositions et corollaire suivants vont montrer que toute isogénie de $E/\mathbb{F}_q$ peut s'écrire comme la composition d'une isogénie séparable

Proposition 3.26. *Soit* k *un corps de caractéristique* p. *Soit* $\phi(x, y) = (r_1(x), r_2(x)y)$ *une isogénie avec* $r_1(x) = u(x)/v(x)$, u *et* v *étant des polynômes de* $\overline{K}[x]$ *premiers entre eux. Alors* ϕ *est inséparable si et seulement si il existe deux polynômes* f *et* g *tels que* $u(x) = f(x^p)$ *et* $v(x) = g(x^p)$.

Démonstration. Supposons ϕ inséparable, soit $r_1' = 0$ par 3.23. Puisque $0 = r_1' = \frac{u'v - uv'}{v^2}$ on obtient que $u'v = uv'$, et puisque u et v sont premiers entre eux, u divise u', ce qui implique que $u' = 0$ pour des raisons de degré. En notant $u(x) = \sum_{k=0}^{+\infty} a_k x^k$, on obtient $0 = u'(x) = \sum_{k=0}^{+\infty} k a_k x^{k-1}$ et donc $\forall k \in \mathbb{N}, ka_k = 0$. Puisque $\overline{K}$ est de caractéristique p, cela implique que $a_k = 0$ si $p \not\equiv 0\ [p]$. Ainsi il existe bien f tel que $u(x) = f(x^p)$. De même, $v(x) = g(x^p)$.

Réciproquement, si $u(x) = f(x^p)$ et $v(x) = f(x^p)$, $u'(x) = f'(x^p) \cdot px^{p-1} = 0$ et de même pour v, donc $u' = v' = 0$. Alors $r_1' = (\frac{u}{v})' = \frac{u'v - uv'}{v^2} = 0$, et donc ϕ est inséparable par 3.23. □

Corollaire 3.27. *Soit* $E_1/\mathbb{F}_q$ *une courbe elliptique. Toute isogénie* $\phi : E_1 \to E_2$ *peut s'écrire* $\phi = \psi \circ \pi_p^n$ *avec* $n \in \mathbb{N}$ *et* ψ *une isogénie séparable.*

Démonstration. Si ϕ est séparable, il n'y a rien à démontrer. Supposons ϕ inséparable : par la proposition précédente il existe ψ_1 tel que $\phi = \psi_1 \circ \pi_p$. Tant que ψ_k est inséparable, on réapplique la proposition ψ_k et on a donc $\phi = \psi_k \circ \pi_p^k$. Par multiplicativité du degré $\deg(\phi) = \deg(\psi_k)\deg(\pi_p^k) = \deg(\psi_k) \cdot p^k$. Ainsi le processus termine, et donc il existe ψ séparable et $n \in \mathbb{N}$ tels que $\phi = \psi \circ \pi_p^n$. □

Remarque 3.28. Cette expression est unique. Supposons que $\phi = \psi_a \circ \pi_p^{n_a} = \psi_b \circ \pi_p^{n_b}$ comme dans le corollaire précédent. Sans perte de généralité on peut supposer que $n_a \leq n_b$. Alors $(\psi_a - \psi_b \circ \pi_p^{n_b - n_a}) \circ \pi_p^{n_a} = 0$, donc en utilisant la multiplicativité du degré et la convention $\deg(0) = 0$, on obtient $\psi_a = \psi_b \circ \pi_p^{n_b - n_a}$. Puisque ψ_a est séparable, en utilisant la proposition 3.23 on en déduit que $n_a = n_b$, et donc $\psi_a = \psi_b$.

3.6 Isogénie duale

Dans cette sous-partie, on introduit l'isogénie duale d'une isogénie (ou d'un morphisme).

Théorème 3.29. *Soit $\phi : E_1 \to E_2$ une isogénie (non constante). Il existe une unique isogénie $\widehat{\phi} : E_2 \to E_1$ telle que $\widehat{\phi} \circ \phi = [\deg \phi]$. Elle est appelée l'isogénie duale de ϕ.*

Démonstration. Admise. □

Remarque 3.30. Dans le cas où $\phi = [0]$, on définit $\widehat{\phi} = [0]$ et on étend ainsi le concept d'isogénie duale à tous les morphismes.

Proposition 3.31. *Soit $\phi : E_1 \to E_2$ un morphisme.*

1. *$\widehat{\phi} \circ \phi = [\deg \phi]$ sur E_1 et $\phi \circ \widehat{\phi} = [\deg \phi]$ sur E_2.*
2. *Soit $\lambda : E_2 \to E_3$ un autre morphisme. Alors $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$.*
3. *Soit $\psi : E_1 \to E_2$ un autre morphisme. Alors $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.*
4. *Pour tout $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ et $\deg([m]) = m^2$.*
5. *$\deg \widehat{\phi} = \deg \phi$ et $\widehat{\widehat{\phi}} = \phi$.*

Démonstration. Toutes ces propriétés sont triviales dans le cas ou les morphismes sont nuls. On ne considère dans cette démonstration que des isogénies.

1. Par le théorème 3.29 la propriété $\widehat{\phi} \circ \phi = [\deg \phi]_{E_1}$ est la définition de l'isogénie duale. Pour la deuxième partie, on observe que $(\phi \circ \widehat{\phi}) \circ \phi = \phi \circ (\widehat{\phi} \circ \phi) = \phi \circ [\deg \phi]_{E_1} = [\deg \phi]_{E_2} \circ \phi$ et donc ϕ étant surjective, on obtient bien $\phi \circ \widehat{\phi} = [\deg \phi]_{E_2}$.
2. En remarquant que $(\widehat{\phi} \circ \widehat{\lambda}) \circ (\lambda \circ \phi) = \widehat{\phi} \circ [\deg \lambda]_{E_2} \circ \phi = [\deg \lambda]_{E_1} \circ \widehat{\phi} \circ \phi = [\deg \lambda]_{E_1} \circ [\deg \phi]_{E_1} = [\deg(\lambda)\deg(\phi)] = [\deg(\lambda \circ \phi)]$ et en utilisant le théorème 3.29, on montre que $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$.
3. La démonstration que je vais donner ne sera pas très satisfaisante puisqu'elle utilise l'existence du pairing de Weil qui sera admise en 3.36. Soit $T_1 \in E_1[m]$ et $T_2 \in E_2[m]$. $e_m(T_1, (\widehat{\phi + \psi})(T_2)) = e_m((\phi + \psi)(T_1), T_2) = e_m(\phi(T_1), T_2) e_m(\psi(T_1), T_2) = e_m(T_1, \widehat{\phi}(T_2)) e_m(T_1, \widehat{\psi}(T_2)) = e_m(T_1, (\widehat{\phi} + \widehat{\psi})(T_2))$. Ainsi $e_m(T_1, (\widehat{\phi + \psi} - \widehat{\phi} - \widehat{\psi})(T_2)) = 1$ pour tout T_1, ce qui montre que $(\widehat{\phi + \psi} - \widehat{\phi} - \widehat{\psi})(T_2) = 0$. Ceci étant vrai pour tout $T_2 \in E_2[m]$ pour tout $m \in \mathbb{Z}$, cela montre que $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$ (en tout cas dans le cas des courbes définies sur $\overline{\mathbb{F}_p}$ où il est évident que chaque élément est d'ordre fini).
4. Montrons d'abord par récurrence pour $m \in \mathbb{N}$ que $\widehat{[m]} = [m]$. Le cas $m = 0$ est vrai par définition (voir la remarque précédente). Les cas $m = \pm 1$ se montrent par le théorème 3.29 en sachant que puisque $[1](x, y) = (x, y)$ et $[-1](x, y) = (x, -y)$, on montre par la proposition 3.19 que $\deg[-1] = \deg[1] = 1$. La

propriété étant vraie à un certain rang m, le point 2 montre l'hérédité : $\widehat{[m+1]} = \widehat{[m]+[1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1]$ et $\widehat{[m-1]} = \widehat{[m]+[-1]} = \widehat{[m]} + \widehat{[-1]} = [m] + [-1] = [m-1]$. Enfin $[\deg[m]] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]$ montre la deuxième partie de l'assertion, le morphisme $[] : \mathbb{Z} \to \mathrm{End}_{E_1}$ étant injectif.

5. Par le point précédent, $(\deg \phi)^2 = \deg([\deg \phi]) = \deg(\widehat{\phi} \circ \phi) = (\deg \widehat{\phi})(\deg \phi)$, donc $\deg \widehat{\phi} = \deg \phi$. Avec le point 1, $\phi \circ \widehat{\phi} = [\deg \phi] = [\deg \widehat{\phi}]$, donc en réutilisant le théorème 3.29 on obtient bien $\widehat{\widehat{\phi}} = \phi$.

□

3.7 Torsion

On définit ici la m-torsion d'une isogénie pour $m \in \mathbb{Z}$.

Définition 3.32. *Soit E/K une courbe elliptique. Pour $m \in \mathbb{Z}$, on définit la m-torsion de E par* $E[m] = \mathrm{Ker}([m]) = \{P \in E(\overline{K}) \mid mP = O\}$.

Théorème 3.33. *Soit $E/\mathbb{F}_q$ une courbe elliptique. Soit $m \in \mathbb{Z}$ tel que p ne divise pas m. Alors $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*

Démonstration. Soit d un diviseur de m. Par la proposition 3.31, $\deg([d]) = d^2$. Puisque p ne divise pas d^2 , et puisque le degré d'inséparabilité de $[d]$ doit être une puissance de p divisant d^2 , le degré d'inséparabilité de $[d]$ vaut 1. Ainsi $[d]$ est séparable. Donc par le théorème 3.40, $d^2 = \deg([d]) = \deg_s([d]) = \#\,\mathrm{Ker}([d]) = \#E[d]$. Avec cette condition sur les cardinaux des $E[d]$ et sachant $E[m]$ est abélien, on peut conclure par le lemme 3.34 que $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

Lemme 3.34. *Soit m premier avec p. Sachant que $\#E[d] = d^2$ pour tout d diviseur de m, $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Démonstration. Pour tout m premier avec p, notons $\mathcal{P}(m)$ la propriété à démontrer.

Supposons dans un premier temps que $m = l^n$, avec l un nombre premier. La propriété $\mathcal{P}(l^0)$ est trivialement vérifiée. Supposons que $\mathcal{P}(l^n)$ soit vraie pour un certain entier n : $E[l^n] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$. Puisque $E[l^n] \subseteq E[l^{n+1}]$, par le théorème de structure des groupes abéliens finis il n'y a que trois cas possibles *a priori* pour la structure de $E[l^{n+1}]$. Soit (1) $E[l^{n+1}] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z} \times G$ avec $\#G = l^2$, soit (2) $E[l^{n+1}] \simeq \mathbb{Z}/l^{n+1}\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, soit (3) $E[l^{n+1}] \simeq \mathbb{Z}/l^{n+1}\mathbb{Z} \times \mathbb{Z}/l^{n+1}\mathbb{Z}$. Montrons que les cas (1) et (2) sont impossibles. Par hypothèse, le nombre d'éléments d'ordre l^{n+1} dans $E[l^{n+1}]$ est $l^{2n+2} - l^{2n} = l^{2n}(p^2 - 1)$. Dans le cas (1) il n'y a pas d'éléments d'ordre l^{n+1}, et dans le cas (2) il y en a $(l^{n+1} - l^n)l^n l = l^{2n}(l^2 - l)$: puisque $p > 1$, ces deux cas sont impossibles. Ainsi $E[l^{n+1}] \simeq \mathbb{Z}/l^{n+1}\mathbb{Z} \times \mathbb{Z}/l^{n+1}\mathbb{Z}$.

Supposons maintenant la propriété $\mathcal{P}$ vraie pour l et m deux entiers premiers entre eux (et non divisible par p). Alors $E[lm] \simeq G_l \times G_m$ avec $\#G_l = l^2$ et $\#G_m = m^2$ par le théorème de structure. De plus, puisque $E[l] \subseteq E[lm]$ et $E[m] \subseteq E[lm]$, on obtient $E[l] \simeq G_l$ et $E[m] \simeq G_m$, ce qui montre que $\mathcal{P}(lm)$ est vraie.

Ainsi, par induction, $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ pour tout m non divisible par p. □

Le but de cette partie est de compter le nombre de points dans $\mathbb{F}_{q^n}$ d'une courbe elliptique E définie sur $\mathbb{F}_q$.

3.8 Pairing de Weil, trace d'une isogénie

Le pairing de Weil est un outil dont on va admettre l'existence et qui va nous permettre de prouver la proposition 3.39.

Définition 3.35. *Soit $\phi \in \mathrm{End}(E)$, et soit l un nombre premier. ϕ induit un endomorphisme $\phi_l : E[l] \to E[l]$. Si $l \neq p$, ϕ_l est un endomorphisme du $\mathbb{Z}/l\mathbb{Z}$-espace vectoriel de dimension 2 $E[l]$.*

Ici l est un nombre premier différent de p.

Proposition 3.36. *Il existe une forme bilinéaire alternée non dégénérée $e_l : E[l] \times E[l] \to \mathbb{U}_l$ telle que pour toute isogénie ϕ, ϕ et $\widehat{\phi}$ soient adjoints pour e_l. Ici, $\mathbb{U}_l \subset \mathbb{C}$ désigne l'ensemble des racines l-èmes de l'unité.*

Démonstration. Admise. □

Lemme 3.37. *Soit $S \in E[l]$ non nul. L'application $e_l(S, \cdot) : E[l] \to \mathbb{U}_l$ est surjective.*

Démonstration. L'image de $e_l(S, \cdot)$ est un sous groupe de $\mathbb{U}_l$: cela ne peut être que $\{1\}$ ou $\mathbb{U}_l$. Mais puisque S est non nul, le caractère non dégénéré du pairing de Weil e_l implique que l'image ne peut pas être réduite à $\{1\}$. L'application est donc surjective. □

Lemme 3.38. *Soient $v_1, v_2 \in E[l]$ tels que $e(v_1, v_2)$ soit une racine l-ème primitive de l'unité. Alors (v_1, v_2) est une base de $E[l]$.*

Démonstration. Puisque $E[l]$ est de dimension 2 par le théorème 3.33, il suffit de montrer que (v_1, v_2) est libre. Par bilinéarité de e_l, v_1 et v_2 sont non nuls. Soient $a, b \in \mathbb{Z}$ tels que $av_1 + bv_2 = 0$. Alors $av_1 = -bv_2$, donc $1 = e_l(av_1, -bv_2) = e_l(v_1, v_2)^{-ab} = e_l(v_1, v_2)^{ab}$. Puisque par hypothèse $e_l(v_1, v_2)$ est une racine l-ème primitive de l'unité, cela implique que l divise ab. Puisque l est premier, on peut supposer sans perte de généralité que l divise a. Ainsi $av_1 = 0$ (dans $E[l]$), et donc $bv_2 = -av_1 = 0$. Puisque $E[l]$ est un $\mathbb{Z}/l\mathbb{Z}$ espace vectoriel et puisque v_1 et v_2 sont non nuls, cela signifie que $a = b = 0$ dans $\mathbb{Z}/l\mathbb{Z}$. □

Proposition 3.39. *Soit ϕ un endomorphisme de E, l un nombre premier différent de p, et ϕ_l l'endomorphisme induit par ϕ sur $E[l]$. Alors $\det(\phi_l) = [\deg(\phi)]_l$, et $\mathrm{tr}(\phi_l) = [1 + \deg(\phi) - \deg(1 - \phi)]_l$, où pour tout $m \in \mathbb{Z}$, $[m]_l$ désigne la classe de m modulo l.*

La proposition précédente montre qu'il fait sens de définir la trace de ϕ par $\mathrm{tr}(\phi) = 1 + \deg(\phi) - \deg(1 - \phi)$.

Démonstration. Par le lemme 3.37, il est possible de choisir v_1 et v_2 dans $E[l]$ tels que $e_l(v_1, v_2)$ soit une racine l-ème primitive de l'unité. Par le lemme 3.38, cela montre que (v_2, v_2) est une $\mathbb{Z}/l\mathbb{Z}$-base de la l-torsion $E[l] \simeq \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice de ϕ_l dans la base (v_1, v_2).

$$
\begin{aligned}
e_l(v_1, v_2)^{\deg \phi} &= e_l([\deg \phi] v_1, v_2) && \text{Linéarité à gauche} \\
&= e_l(\widehat{\phi_l}(\phi_l(v_1)), v_2) && \text{Définition de } \widehat{\phi} \\
&= e_l(\phi_l(v_1), \phi_l(v_2)) && \text{Caractère adjoint de } \widehat{\phi} \\
&= e_l(av_1 + cv_2, bv_1 + dv_2) && \text{Écriture dans la base } (v_1, v_2) \\
&= e_l(v_1, v_1)^{ab} e_l(v_1, v_2)^{ad} e_l(v_2, v_1)^{bc} e_l(v_2, v_2)^{cd} && \text{Bilinéarité} \\
&= e_l(v_1, v_2)^{ad} e_l(v_2, v_1)^{bc} = e_l(v_1, v_2)^{ad - bc} && \text{Caractère alterné de } e_l \\
&= e_l(v_1, v_2)^{\det \phi_l} && \text{Définition de } \det(\phi_l)
\end{aligned}
$$

Puisque $e_l(v_1, v_2)$ est une racine l-ème primitive de l'unité, on peut conclure que $\det \phi_l$ est égal à la classe de $\deg \phi$ modulo l.

L'égalité suivante est vraie pour toute matrices 2×2 : $\det(1-A) = (1-a)(1-d) - bc = 1-a-d+ad-bc = 1-\mathrm{tr}(A)+\det(A)$. Ainsi, en utilisant cette égalité et le lien entre le degré et le déterminant d'un endomorphisme on obtient bien $tr(\phi_l) = 1 + deg(\phi) - deg(1-\phi)$. □

3.9 Trace du morphisme de Frobenius

La trace du morphisme de Frobenius π_q d'une courbe elliptique définie sur $\mathbb{F}_q$ est complètement relié au cardinal de la courbe sur $\mathbb{F}_q$.

Théorème 3.40. *Soit $\phi : E_1 \to E_2$ une isogénie séparable. Alors $\#\operatorname{Ker}(\phi) = \deg(\phi)$.*

Démonstration. Voir le théorème III.4.10 (c) dans Silverman (1992). □

Lemme 3.41. *Soit $E/\mathbb{F}_q$ une courbe elliptique. Le morphisme $1-\pi_q$ est séparable, et $\#E(\mathbb{F}_q) = deg(1-\pi_q)$.*

Démonstration. On calcul explicitement l'expression du morphisme $(1-\pi_q)(x,y) = (x,y) - (x^q, y^q)$ et on utilise la propriété 3.23 pour montrer que $1-\pi_q$ est séparable.

Puisque $1-\pi_q$ est séparable, par le théorème 3.40 $\deg(1-\pi_q) = \#\operatorname{Ker}(1-\pi_q)$. Or $\operatorname{Ker}(1-\pi_q) = \{(x,y) \in E(\overline{\mathbb{F}_p}) : (x,y) = (x^q, y^q)\} = E(\mathbb{F}_q)$. Ainsi $\#E(\mathbb{F}_q) = \deg(1-\pi_q)$. □

Proposition 3.42. *Soit $E/\mathbb{F}_q$ une courbe elliptique. Alors $\#E(\mathbb{F}_q) = q + 1 - \mathrm{tr}(\pi_q)$.*

Démonstration. Par la proposition 3.39, $\mathrm{tr}(\pi_q) = \deg(\pi_q) + 1 - \deg(1-\pi_q)$. Par les propositions 3.25 et 3.41, on sait que $\deg(\pi_q) = q$ et $\#E(\mathbb{F}_q) = deg(1-\pi_q)$. Ainsi $\mathrm{tr}(\pi_q) = q + 1 - \#E(\mathbb{F}_q)$, ce qui démontre l'égalité annoncée. □

Théorème 3.43. *Soit $E/\mathbb{F}_q$ une courbe elliptique et π_q l'endomorphisme de Frobenius. Alors $\pi_q^2 - \mathrm{tr}(\pi_q)\pi_q + [q] = 0$.*

Démonstration. Soit $\pi_{q,l}$ l'endomorphisme induit par π_q sur $E[l]$. Le polynôme caractéristique de ϕ_l est $X^2 - \mathrm{tr}(\pi_{q,l})X + \det(\pi_{q,l})$. Par le théorème de Cayley-Hamilton, et en appliquant deux fois la proposition 3.39 on obtient que $\pi_{q,l}^2 - t\pi_{q,l} + q = 0$. En appliquant une dernière fois 3.39, on obtient $\deg(\pi_q^2 - \mathrm{tr}(\pi_q)\pi_q + q) = \det(\pi_{q,l}^2 - \mathrm{tr}(\pi_q)\pi_{q,l} + q) = \det(0) = 0$, et donc par définition du degré on obtient l'égalité souhaitée. □

Lemme 3.44. *Soit A une matrice 2×2 à coefficients dans un corps K. Pour tout $n \in \mathbb{N}$, $\mathrm{tr}(A^{n+2}) = \mathrm{tr}(A)\,\mathrm{tr}(A^{n+1}) - \det(A)\,\mathrm{tr}(A^n)$.*

Démonstration. La trace et le déterminant restent inchangés si l'on considère la matrice A comme étant à coefficients dans une extension de K. En prenant la clôture algébrique de K on peut donc se ramener au cas où K est algébriquement clos. De plus, la trace et le déterminant sont invariants par changement de base, donc on peut supposer la matrice A triangulaire supérieure (A est trigonalisable si et seulement si son polynôme caractéristique est scindé, ce qui est le cas en supposant K algébriquement clos.) En posant $A = \begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix}$, on vérifie immédiatement que $\mathrm{tr}(A^{n+2}) = \alpha^{n+2} + \beta^{n+2} = (\alpha+\beta)(\alpha^{n+1} + \beta^{n+1}) - \alpha\beta(\alpha^n + \beta^n) = \mathrm{tr}(A)\,\mathrm{tr}(A^{n+1}) - \det(A)\,\mathrm{tr}(A^n)$. □

Théorème 3.45. *Soit ϕ un endomorphisme de $E/\mathbb{F}_q$ une courbe elliptique et π_q le morphisme de Frobenius. Pour $n \in \mathbb{N}$ notons $t_n = \mathrm{tr}(\pi_{q^n}) = \mathrm{tr}(\pi_q^n)$. Alors $t_0 = 1$ et pour tout $n \in \mathbb{N}$, $t_{n+2} = t_1 t_{n+1} - q t_n$.*

Démonstration. Soit $n \in \mathbb{N}$. Soit ϕ un endomorphisme. Pour tout entier l premier différent de p,

$$\begin{aligned}[\operatorname{tr}\phi^{n+2}]_l &= \operatorname{tr}(\phi_l^{n+2}) = \operatorname{tr}(\phi_l)\operatorname{tr}(\phi_l^{n+1}) - \det(\phi_l)\operatorname{tr}(\phi_l^n) \\ &= [\operatorname{tr}(\phi)]_l[\operatorname{tr}(\phi^{n+1})]_l - [\deg(\phi)]_l[\operatorname{tr}(\phi_l)]_l \\ &= [\operatorname{tr}(\phi)\operatorname{tr}(\phi^{n+1}) - \deg(\phi)\operatorname{tr}(\phi^n)]_l\end{aligned}$$

Cette égalité étant vraie pour une infinité d'entiers l, on obtient $\operatorname{tr}\phi^{n+2} = \operatorname{tr}(\phi)\operatorname{tr}(\phi^{n+1}) - \deg(\phi)\operatorname{tr}(\phi^n)$. En appliquant cette égalité à $\phi = \pi_q$ et sachant que $\deg(\pi_q) = q$, on obtient bien $t_{n+2} = t_1 t_{n+1} - q t_n$.

□

3.10 Borne de Hasse

Le théorème 3.50 donne une borne sur le nombre de points dans $\mathbb{F}_q$ d'une courbe elliptique définie sur $\mathbb{F}_q$.

Définition 3.46 (Forme quadratique)**.** *Soit G un groupe abélien et $d : G \to \mathbb{Z}$. On dit que d est une forme quadratique si pour tout $g \in G$, $d(g) = d(-g)$ et si l'application $G \times G \to \mathbb{Z}$, définie par $\langle g, h\rangle_d = d(g+h) - d(g) - d(h)$ est bilinéaire.*

Si de plus $d(g) = 0$ si et seulement si $g = 0$, on dit que d est définie. Si $d(g) \geq 0$ pour tout $g \in G$, on dit que d est positive.

Remarque 3.47. Soit $g, h \in G$ et $n \in \mathbb{Z}$. On remarque que $\langle g, -g\rangle_d = d(g + (-g)) - d(g) - d(-g) = d(0) - d(g) - d(g) = -2d(g)$, donc $2d(g) = -\langle g, -g\rangle_d = \langle g, g\rangle_d$. On remarque aussi que par définition $\langle \cdot, \cdot\rangle_d$ est symétrique. Ainsi on peut développer les formes quadratiques de façon usuelle : $d(g+h) = d(g) + \langle g, h\rangle_d + d(h)$ et $d(ng) = n^2 d(g)$.

Lemme 3.48 (Inégalité de Cauchy-Schwarz)**.** *Soit G un groupe abélien. Et $d : G \to \mathbb{Z}$ une forme quadratique définie positive. Alors $|\langle g, h\rangle_d| \leq 2\sqrt{d(g)d(h)}$ pour tout $g, h \in G$.*

Démonstration. Soit $g, h \in G$. On peut supposer $g \neq 0$, l'inégalité dans le cas $g = 0$ étant triviale. Puisque d est positive, pour tout $m, n \in \mathbb{Z}$ on a $0 \leq d(mg + nh) = m^2 d(g) + mn\langle g, h\rangle_d + n^2 d(h)$. En particulier choisissons $m = -\langle g, h\rangle_d$ et $n = 2d(g)$. On obtient $0 \leq \langle g, h\rangle_d^2 d(g) - 2d(g)\langle g, h\rangle_d^2 + 4d(g)^2 d(h) = d(g)(-\langle g, h\rangle_d^2 + 4d(g)d(h))$. Ainsi, puisque $g \neq 0$, $d(g) \neq 0$ et donc $\langle g, h\rangle_d^2 \leq 4d(g)d(h)$. On en déduit directement le résultat énoncé. □

Proposition 3.49. *Soit E une courbe elliptique. L'application* $\deg : \operatorname{End}(E) \to \mathbb{N}$ *est une forme quadratique.*

Démonstration. On remarque premièrement que par définition, le degré est défini positif. Soit ϕ un endomorphisme de E non constant. On remarque que $(-\phi)^* K(E) = \phi^* K(E)$, (on utilise le fait que $K(E)$ est un corps, et que $[-1]$ est un endomorphisme) donc $\deg(-\phi) = \deg(\phi)$. Il ne reste plus qu'à montrer la bilinéarité de $\langle \phi, \psi\rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$. On utilise pour cela le morphisme d'anneaux injectif $[\cdot] : \mathbb{Z} \to \operatorname{End} E$. En remarquant que $[\langle \phi, \psi\rangle] = \widehat{(\phi + \psi)}(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = (\widehat{\phi} + \widehat{\psi})(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = \widehat{\phi}\psi + \widehat{\psi}\phi$, on voit clairement que $\langle \cdot, \cdot\rangle$ est bilinéaire. □

Théorème 3.50 (Borne de Hasse)**.** *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Alors $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.*

Démonstration. Appliquons l'inégalité de Cauchy-Schwarz (lemme 3.48) la forme quadratique définie positive $\deg : \operatorname{End} E \to \mathbb{Z}$ (proposition 3.49). Pour $\phi, \psi \in \operatorname{End} E$, $|\deg(\phi + \psi) - \deg\phi - \deg\psi| \leq 2\sqrt{(\deg\phi)(\deg\psi)}$. Utilisons cette inégalité avec $\phi = [1]$ et $\psi = -\pi_q$. On sait déjà que $\deg[1] = 1$ (remarque 3.25) et $\deg(-\pi_q) = q$ (propriété 3.31). Par le lemme 3.41, on sait que $\#E(\mathbb{F}_q) = \deg([1] - \pi_q)$, donc finalement $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$. □

4 Cryptographie par isogénies entre courbes supersingulières

4.1 Courbes supersingulières

On s'intéresse maintenant particulièrement aux courbes elliptiques supersingulières que nous allons définir et qui seront utilisées dans le protocole SIDH.

Définition 4.1. *Une courbe elliptique $E/\mathbb{F}_q$ (q étant une puissance de p) est dite supersingulière si $E[p]$ est réduit à ∞.*

Proposition 4.2. *Soit $E/\mathbb{F}_q$ une courbe elliptique. La courbe E est supersingulière si et seulement si $\widehat{\pi_q}$ est (purement) inséparable.*

Démonstration. Notons $q = p^r$.

Supposons que $E/\mathbb{F}_q$ soit supersingulière, c'est à dire que $E[p] = \{0\}$. Alors $1 = \#E[p] = \deg_s[p] = \deg_s(\widehat{\pi_p} \circ \pi_p) = \deg_s(\widehat{\pi_p})$. Ainsi $\deg_s(\widehat{\pi_q}) = \deg_s(\widehat{\pi_p})^r = 1$, donc $\widehat{\pi_{p^r}}$ est purement inséparable.

Supposons que E ne soit pas supersingulière et montrons que $\widehat{\pi_q}$ est séparable. Puisque $E[p] \neq \{0\}$, p divise $\#E[p] = \deg_s(\widehat{\pi_p})$. Or $\deg_s(\widehat{\pi_p})$ divise $\deg(\widehat{\pi_p}) = \deg(\pi_p) = p$. Donc $\deg_s(\widehat{\pi_p}) = \deg(\widehat{\pi_p}) = p$, ce qui montre que $\widehat{\pi_p}$ est séparable, et donc que $\widehat{\pi_q}$ est séparable. □

Proposition 4.3. *$E/\mathbb{F}_q$ est supersingulière si et seulement si $\mathrm{tr}(\pi_q) \equiv 0\ [p]$.*

Démonstration. Appliquons le théorème 3.45 : notons $t_n = \mathrm{tr}(\pi_{q^n})$ et alors pour tout $n \in \mathbb{N}$, $t_{n+2} = t_1 t_{n+1} - q t_n$. En raisonnant modulo p, on obtient $t_{n+2} \equiv t_1 t_{n+1}\ [p]$, donc $t_n \equiv t_1^n\ [p]$. De plus, $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \mathrm{tr}(\pi_{q^n}) \equiv 1 - t_n\ [p]$.

Supposons $t_1 = \mathrm{tr}(\pi_q) \equiv 0\ [p]$. Alors $\#E(\mathbb{F}_{q^n}) = 1 - t_1^n \equiv 1\ [p]$ pour tout $n \geq 1$, donc par le théorème de Lagrange, $E(\mathbb{F}_{q^n})$ ne contient pas d'éléments d'ordre p, et donc $E[p] = \{0\}$.

Supposons $t_1 = \mathrm{tr}(\pi_q) \not\equiv 0\ [p]$. Alors $t_{p-1} = t_1^{p-1} \equiv 1\ [p]$, donc $\#E(\mathbb{F}_{q^{p-1}}) \equiv 0\ [p]$. Par le théorème de Cauchy, $E(\mathbb{F}_{q^{p-1}})$ contient un élément d'ordre p, et donc $E[p] \neq \{0\}$. □

Proposition 4.4. *Toute courbe elliptique $E/\overline{\mathbb{F}_p}$ a son j-invariant dans $\mathbb{F}_{p^2}$, donc une telle courbe est $\overline{\mathbb{F}_p}$-isomorphe à une courbe définie sur $\mathbb{F}_{p^2}$.*

Démonstration. Puisque E est supersingulière, $\widehat{\pi_p} : E^{(p)} \to E$ est purement inséparable, donc $\widehat{\pi_p} = \psi \circ \pi_p$ avec $\psi : E^{(p^2)} \to E$ une isogénie de degré 1. Une telle isogénie est un isomorphisme, donc $E^{(p^2)}$ est $\overline{\mathbb{F}_p}$-isomorphe à E. Ainsi $j(E) = j(E^{(p^2)}) = j(E)^{p^2}$ donc $X^{p^2} - X$ annule $j(E)$, ce qui revient à dire que $j(E)$ appartient à $\mathbb{F}_{p^2}$. Deux courbes sont isomorphes si et seulement si elles possèdent le même j-invariant, ce qui démontre la fin de la proposition. □

4.2 Graphe des isogénies

Le but de cette partie est de montrer que le graphes des isogénies entre $\overline{\mathbb{F}_p}$-isomorphismes de courbes elliptiques supersingulières définies sur $\mathbb{F}_{p^2}$ est connexe. Puisque chaque courbes elliptique supersingulière est $\overline{\mathbb{F}_p}$-isomorphe à une courbe définie sur $\mathbb{F}_{p^2}$, on restreindra notre étude aux courbes elliptiques définies sur F_{p^2}.

Définition 4.5 (Graphe des isogénies)**.** *Les sommets du graphe (non-orienté) des isogénies est l'ensemble des courbes elliptiques définies sur $\mathbb{F}_{p^2}$ quotienté par la relation "être $\overline{\mathbb{F}_p}$-isomorphe". Deux sommets sont reliés par une arête si il existe une $\mathbb{F}_{p^2}$-isogénie d'un représentant d'un des sommets vers un représentant de l'autre sommet.*

Remarque 4.6. Le théorème d'existence de l'isogénie duale assure que s'il existe une isogénie dans un sens, il existe une isogénie dans l'autre. En revanche, étant donné deux représentant particuliers de deux sommets du graphe reliés par une arête, il n'existe pas forcément une isogénie entre ces deux représentants.

Proposition 4.7. *Soit $E/\mathbb{F}_p$ une courbe elliptique supersingulière définie sur $\mathbb{F}_p$. Alors $\#E(\mathbb{F}_p) = p+1$ et $\#E(\mathbb{F}_{p^2}) = (p+1)^2$.*

Démonstration. Comme dans le théorème 3.45, notons t_1 et t_2 les traces des morphismes π_p et π_{p^2}. Utilisons d'abord la borne de Hasse (théorème 3.50), qui affirme que $-2\sqrt{p} \leq t_1 \leq 2\sqrt{p}$. Ensuite, en utilisant la proposition 4.3, le fait que E soit supersingulière indique que $t_1 \equiv 0\ [p]$. Puisque de plus $p \geq 5$, $p > 2\sqrt{p}$. Ainsi la seule possibilité est $t_1 = 0$.

En appliquant le théorème récurrence on obtient $t_2 = t_1 t_0 - p t_0 = 0 - 2p = -2p$. Enfin en appliquant la proposition 3.42 on obtient $\#E(\mathbb{F}_p) = p + 1 - t_1 = p+1$ et $\#E(\mathbb{F}_{p^2}) = p + 1 - t_1 = p + 1 + 2p = (p+1)^2$. □

Proposition 4.8. *Soit $E/\mathbb{F}_{p^2}$ une courbe supersingulière définie sur $\mathbb{F}_{p^2}$. La courbe E est $\mathbb{F}_{p^2}$-isomorphe à une courbe définie sur $\mathbb{F}_{p^2}$ de cardinal $E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p = (p+1)^2$.*

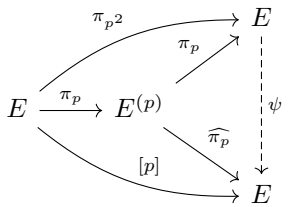
Démonstration. Soit π_{p^2} le Frobenius de la courbe E. En combinant la borne de Hasse $-2p \leq \mathrm{tr}(\pi_{p^2}) \leq 2p$ (théorème 3.50) et la proposition 4.3 $\mathrm{tr}(\pi_{p^2}) \equiv 0\ [p]$, on obtient $\mathrm{tr}(\pi_{p^2}) \in \{-2p, -p, 0, p, 2p\}$. Nous allons distinguer les cas selon la valeur de $\mathrm{tr}(\pi_{p^2})$.

Si $\mathrm{tr}(\pi_{p^2}) = -2p$, il n'y a rien à faire. On rappelle juste que $E(\mathbb{F}_{p^2}) = p^2 + 1 - \mathrm{tr}(\pi_{p^2})$

Supposons que $\mathrm{tr}(\pi_{p^2}) = 2p$. Tous les $\overline{\mathbb{F}_p}$-isomorphismes entre courbes elliptiques préservant la forme de Weierstrass réduite sont de la forme $\varphi : E \to E', (x,y) \mapsto (u^2 x, u^3 y)$ avec $u \in \overline{\mathbb{F}_p}$. Notons $E : y^2 = x^3 + ax + b$. L'équation E' s'écrit donc $E' : u^6 y^2 = u^6 x^3 + u^2 a x + b$, (soit $E' : y^2 = x^3 + u^{-4} a x + u^{-6} b$ si l'on souhaite une forme réduite). On peut choisir $u^2 \in \mathbb{F}_{p^2}$ avec $u \notin \mathbb{F}_{p^2}$, et alors E' est définie sur $\mathbb{F}_{p^2}$, mais ne possède pas le même nombre de points dans $\mathbb{F}_{p^2}$ que E.

Comptons le nombre de points de $\#E(\mathbb{F}_{p^2}) + \#E'(\mathbb{F}_{p^2})$. E' se réécrit encore $E' : u^2 (u^2 y)^2 = (u^2 x)^3 + a(u^2 x) + b$. Puisque $u^2 \in \mathbb{F}_{p^2}^\times$, $\#E'(\mathbb{F}_{p^2}) = \#E''(\mathbb{F}_{p^2})$ avec $E'' : u^2 y^2 = x^3 + ax + b$, soit encore $E'' : y^2 = u^{-2}(x^3 + ax + b)$. La multiplication par u^2 est une bijection entre les carrés de $\mathbb{F}_{p^2}^\times$ et les éléments qui ne sont pas des carrés de $\mathbb{F}_{p^2}^\times$. Ainsi, si $x^3 + ax + b$ est un carré non nul de $\mathbb{F}_{p^2}$, E possède deux solutions pour un tel x et E'' aucune. Si ce n'est pas un carré, E ne possède pas de solutions et E'' en possède deux. Enfin si cette quantité est nulle, E et E'' possèdent chacune une solution. Dans tous les cas, pour une abscisse x fixée, E et E'' possèdent au total 2 points possédant une telle abscisse. En n'oubliant que le point à l'infini appartient aussi aux deux courbes, on obtient : $\#E(\mathbb{F}_{p^2}) + \#E'(\mathbb{F}_{p^2}) = 2p^2 + 2 = 2(p^2+1)$. Ainsi $\#E'(\mathbb{F}_{p^2}) = p^2 + 1 + \mathrm{tr}(\pi_{p^2}) = p^2 + 1 + 2p$.

Pour traiter les derniers cas nous serons amenés à étudier les automorphismes de E (voir le théorème III.10.1 dans Silverman). Puisque E est supersingulière, $\widehat{\pi_p} : E^{(p)} \to E$ est purement inséparable donc se factorise en $\widehat{\pi_p} = \psi \circ \pi_p$. Sachant que $\deg(\widehat{\pi_p}) = \deg(\pi_p) = p^2$, ψ est de degré 1 et donc est un isomorphisme. De plus $\widehat{\pi_p}\pi_p = [p]$, et $E^{(p^2)} = E$, le diagramme suivant est commutatif :



Ainsi $\pi_{p^2} = \psi^{-1} \circ [p]$.

Dans le cas où $\mathrm{tr}(\pi_{p^2}) = 0$, $\pi_{p^2}^2 + [p^2] = 0$ donc $-[p^2] = \pi_{p^2}^2 = (\psi^{-1} \circ [p])^2 = \psi^{-2} \circ [p^2]$ puisque tout morphisme commute avec $[m]$. Alors $(\psi^{-2} + 1) \circ [p^2] = 0 \in \mathrm{End}(E)$ donc $[p^2]$ étant surjective, $\psi^2 = -\mathrm{Id}$. Ainsi ψ est d'ordre 4, donc par le théorème III.10.1 (Silverman) (caractéristique $\neq 2, 3$) $j(E) = 1728$. Ainsi E est $\overline{\mathbb{F}_p}$-isomorphe à une courbe $y^2 = x^3 + ax$ qui est de cardinal $(q+1)^2$. On a utilisé ici un des cas particuliers

Dans les dernier cas, où $\mathrm{tr}(\pi_{p^2}) = \pm p$, $X^2 \pm pX + p^2$ annule $\pi_{p^2}^2$ et puisque $X^6 - p^6 = p^6((\frac{X}{p})^6 - 1) = (X-1)(X+1)(X^2-pX+p^2)(X^2+pX+p^2)$, $\pi_{p^2}^6 = [p^6]$. Ainsi $[p^6] = \pi_{p^2}^6 = (\psi^{-1} \circ [p])^6 = \psi^{-6} \circ [p^6]$, donc $\psi^6 = \mathrm{Id}$. Le théorème III.10.1 permet de conclure si l'ordre de ψ est 3 ou 6, il suffit donc de montrer que l'ordre de ψ ne peut être ni 1, ni 2. Si ψ est d'ordre 1, $\pi_{p^2} = [p]$, donc $\mathrm{tr}(\pi_{p^2}) = \mathrm{tr}([p]) = 1 + \deg([p]) - \deg([1-p]) = 1 + p^2 - (p-1)^2 = 2p$, ce qui contredit l'hypothèse $\mathrm{tr}(\pi_{p^2}) = \pm p$. Si ψ est d'ordre 2, $\pi_{p^2}^2 = (\psi^{-1} \circ [p])^2 = \psi^{-2} \circ [p^2] = -[p^2]$, donc $\pi_{p^2}^6 = -[p^6]$ ce qui contredit $[p^6] = \pi_{p^2}^6$. □

Théorème 4.9 (Tate)**.** *Étant donné deux courbes elliptiques E_1 et E_2 définies sur $\mathbb{F}_q$, et soit $n \in \mathbb{N}^*$. Il existe une isogénie (non constante par définition) $\varphi : E_1 \to E_2$ définie sur $\mathbb{F}_{q^n}$ si et seulement si $\#E_1(\mathbb{F}_{q^n}) = \#E_2(\mathbb{F}_{q^n})$.*

Démonstration. Admise. □

Corollaire 4.10. *Le graphe des isogénies entre courbes supersingulières définies sur $\mathbb{F}_{p^2}$ est connexe.*

Démonstration. En combinant du théorème de Tate (4.9) et de la proposition 4.8, on obtient qu'entre deux classe de $\overline{\mathbb{F}_p}$-isomorphisme entre courbes elliptiques supersingulières définies sur $\mathbb{F}_{p^2}$ il existe toujours une isogénie. □

Remarque 4.11. On a même montré qu'en partant d'un courbe supersingulière définie sur $\mathbb{F}_{p^2}$ de cardinal $E(\mathbb{F}_{p^2}) = (p+1)^2$ et en se promenant sur le graphe des isogénies on atteint toutes les courbes supersingulières.

4.3 Construction d'une courbe initiale

Le protocole utilise une courbe elliptique supersingulière E_0 définie sur $\mathbb{F}_{p^2}$ de cardinal $E_0(\mathbb{F}_{p^2}) = (p+1)^2 = (2^a 3^b f)^2$ avec 2 et 3 ne divisant pas f. La sécurité du protocole repose sur la taille des entiers a et b, il est donc nécessaire de pouvoir construire de telles courbes avec de grands a et b. C'est ce que nous faisons dans cette partie. Plus précisément, nous allons étudier la courbe $E_0 : y^2 = x^3 + b$ avec $b \in \mathbb{F}_p^\times$ et montrer que sous certaines conditions sur p, cette courbe est supersingulière et de bonne cardinalité (en considérant le nombre de points dans $\mathbb{F}_{p^2}$).

Commençons par compter le nombre de points de E_0 sur $\mathbb{F}_p$. Pour cela nous montrons d'abord un résultat sur le nombre de carrés dans $\mathbb{F}_p$.

Proposition 4.12. *Soit p un nombre premier impair. $\mathbb{F}_p$ contient $\frac{p+1}{2}$ carrés.*

Démonstration. $\mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p-1$. Notons g un générateur de $\mathbb{F}_p^\times$.

L'application $\varphi\colon \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \to \mathbb{F}_p^\times$, $[k] \mapsto g^k$ est bien définie et est un isomorphisme de groupes. Soit $a \in \mathbb{F}_p^\times$, et soit $[k] = \psi^{-1}(a)$. Si k est pair, ce qui a un sens puisque $p-1$ est pair, $a = g^k = (g^{\frac{k}{2}})^2$, donc a est un carré. Réciproquement, si a est un carré, il existe $[l] \in \mathbb{Z}/(p-1)\mathbb{Z}$ tel que $a = (g^l)^2 = g^{2l}$. Alors $[k] = [2l]$ donc k est pair. Il y a donc autant de carrés dans $\mathbb{F}_p^\times$ que de nombres pairs dans $\mathbb{Z}/(p-1)\mathbb{Z}$, soit $\frac{p-1}{2}$. En comptant 0, il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$. □

Proposition 4.13. *Si p est impair et si $p \equiv 2$ [3], alors $\#E_0(\mathbb{F}_p) = p + 1$.*

Démonstration. Considérons le morphisme de groupes $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^3$. Soit $x \in \ker\varphi$, $x^3 = 1$, donc l'ordre de x noté $o(x)$ divise 3. Par le théorème de Lagrange, $o(x) \mid \#\mathbb{F}_p^\times$, donc $o(x) \mid p-1$. Or par hypothèse $p - 1 \equiv 1[3]$, donc $o(x) = 1$, donc $x = 1$. Ainsi $\ker\varphi = 1$, donc φ est injective, et donc bijective par égalité des cardinaux.

On en déduit immédiatement que l'application $x \mapsto x^3 + b$ de $\mathbb{F}_p$ dans $\mathbb{F}_p$ est bijective. Nous pouvons maintenant compter le nombre de points de E dans $\mathbb{F}_p$. Si $x^3 + b$ est un carré non nul de $\mathbb{F}_p$, deux valeurs différentes de y sont solutions de l'équation E. Si $x^3 + b = 0$, $y = 0$ est la seule valeur qui convient. Enfin si $x^3 + b$ n'est pas un carré de $\mathbb{F}_p$, E ne possède pas de solution. En n'oubliant pas que le point à l'infini O est aussi solution de E, et en utilisant le lemme, on obtient : $\#E(\mathbb{F}_p) = 2\frac{p-1}{2} + 1 + 1 = p + 1$. □

À partir de maintenant on suppose que p est un nombre premier impair congru à 2 modulo 3. Ainsi $\#E_0(\mathbb{F}_p) = p + 1$.

On cherche maintenant à calculer le nombre de points de la courbe E_0 sur $\mathbb{F}_{p^2}$ en connaissant le nombre de points de la courbe sur $\mathbb{F}_p$.

Corollaire 4.14. $\#E_0(\mathbb{F}_{p^2}) = (p+1)^2$.

Démonstration. En utilisant le théorème 3.45, avec $q = p$, on obtient $t_2 = t_1^2 - pt_0 = -2p$. Donc $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - t_2 = p^2 + 1 + 2p = (p+1)^2$. □

Montrons maintenant que la courbe E_0 est supersingulière. Puisque $t_2 = -2p$, $t_2 \equiv 0$ $[p]$, donc par la proposition 4.3, E_0 est supersingulière.

4.4 Torsions de la courbe initiale

Dans la partie 4.4 nous comptons le nombre de sous groupes cycliques de la 2^a ou 3^b-torsion de E_0. On souhaite que ce nombre soit important pour le protocole cryptographique.

On s'intéresse maintenant à la structure des groupes de torsion de E_0 sur $\mathbb{F}_{p^2}$. Pour cela nous avons d'abord besoin d'informations sur la structure de groupes des points $\mathbb{F}_{p^2}$ rationnels de la courbe E_0.

Proposition 4.15.

$$E_0(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$$

Démonstration. Utilisons à nouveau le théorème 3.43 en posant $q = p^2$. Posons π_{p^2} le morphisme de Frobenius. En constatant que $\mathrm{tr}(\pi_{p^2}) = -2p$, on obtient que $\pi_{p^2}^2 + 2p\pi_{p^2} + [p^2] = 0$, donc que $\left(\pi_{p^2} + [p]\right)^2 = 0$ dans $\mathrm{End}(E_0)$. Ainsi $\deg(\pi_{p^2} + [p])^2 = 0$, donc $\deg(\pi p^2 + [p]) = 0$, donc $\pi_{p^2} + [p] = 0$.

Soit $P \in E_0(\overline{\mathbb{F}_p})$. $P \in E_0(\mathbb{F}_{p^2})$ ssi $\pi_{p^2}(P) = P$, donc $E_0(\mathbb{F}_{p^2}) = \mathrm{Ker}(\mathrm{Id} - \pi_{p^2}) = \mathrm{Ker}([1] + [p]) = \mathrm{Ker}([p+1])$. En utilisant la proposition 3.33, puisque p ne divise pas $p + 1$, on obtient le résultat souhaité. □

Puisque l'on a déjà supposé $p \geq 3$ et $p \equiv 2$ [3], on a $a, b \geq 1$. Avec ces notations, on s'intéresse à la 2^a et à la 3^b-torsion de E_0. Pour éviter d'écrire deux fois la même chose, le couple (l, e) désigne soit le couple $(2, a)$ soit le couple $(3, b)$ dans les preuves suivantes.

Proposition 4.16.

$$E_0(\mathbb{F}_{p^2})[l^e] \simeq \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$$

Démonstration. D'abord, par la proposition précédente, $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ est isomorphe à un unique sous-groupe de $E_0(\mathbb{F}_{p^2})$. Il suffit donc de montrer une double inclusion entre deux sous-groupes de $E_0(\mathbb{F}_{p^2})$. L'inclusion

$E_0(\mathbb{F}_{p^2})[l^e] \supseteq \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ est évidente en remarquant que tout élément de $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ a un ordre qui divise l^e.

Pour l'inclusion réciproque on peut par exemple utiliser les théorèmes de Sylow. Par définition, $E_0(\mathbb{F}_{p^2})[l^e]$ est un l-sous-groupe de $E_0(\mathbb{F}_{p^2})$, il est donc contenu dans un l-Sylow. Puisque $E_0(\mathbb{F}_{p^2})$ est abélien, et puisque les l-Sylow sont conjugués, il existe un unique l-Sylow. En remarquant que $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ est un l-Sylow par la proposition précédente, on démontre l'inclusion manquante et donc l'isomorphisme annoncé. □

Ainsi, puisque $E_0(\mathbb{F}_{p^2})[l^e] \simeq \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ par la proposition 3.33, on en déduit que la l^e-torsion est $\mathbb{F}_{p^2}$-rationnelle. On s'intéresse maintenant au nombre de sous-groupes cycliques de la 2^a ou 3^b-torsion.

Proposition 4.17. *$E_0(\mathbb{F}_{p^2})[l^e]$ contient $l^{e-1}(l+1)$ sous-groupes cycliques d'ordre l^e.*

Démonstration. Comptons le nombre d'éléments d'ordre l^e dans $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$. Soit $(x, y) \in \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$, $o((x, y)) = \text{ppcm}(o(x), o(y)) = \max(o(x), o(y))$, donc un couple d'éléments de $\mathbb{Z}/l^e\mathbb{Z}$ est d'ordre l^e si et seulement si un des éléments est d'ordre l^e. Alors,

$$\#\{(x, y) \mid o((x, y)) = l^e\} = \#\{(x, y) \mid o(x) = l^e\} + \#\{(x, y) \mid o(y) = l^e\} - \#\{(x, y) \mid o(x) = o(y) = l^e\}$$

Notons $\alpha = l^e - l^{e-1}$ le nombre de générateurs de $\mathbb{Z}/l^e\mathbb{Z}$. Ainsi le nombre de sous sous-groupes cycliques d'ordre l^e de la l^e-torsion est $(2l^e\alpha - \alpha^2)/\alpha = 2l^e - \alpha = l^e + l^{e-1} = l^{e-1}(l+1)$. □

La proposition suivante permet d'écrire un algorithme pour calculer une base de $E_0[l^e] \simeq \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$.

Proposition 4.18. *Soient P et Q deux éléments de $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$. La famille (P, Q) est $\mathbb{Z}/l^e\mathbb{Z}$-libre ssi $(l^{e-1}P, l^{e-1}Q)$ est $\mathbb{Z}/l\mathbb{Z}$-libre.*

Démonstration. L'équivalence précédente se réécrit :

$$(\forall a, b \in \mathbb{Z},\ aP + bQ = 0 \Rightarrow a \equiv b \equiv 0\ [l^e]) \iff \left(\forall a, b \in \mathbb{Z},\ al^{e-1}P + bl^{e-1}Q = 0 \Rightarrow a \equiv b \equiv 0\ [l]\right)$$

Montrons l'implication directe. Soient $a, b \in \mathbb{Z}$ tels que $al^{e-1}P + bl^{e-1}Q = 0$. Par hypothèse, $l^{e-1}a \equiv l^{e-1}b \equiv 0\ [l^e]$, ce qui montre directement que $a \equiv b \equiv 0\ [l]$.

Montrons maintenant l'implication réciproque. Soient $a, b \in \mathbb{Z}$ tels que $aP + bQ = 0$. Dans le cas où a et b sont non nuls, on réécrit $a = a'l^{v_l(a)}$ et $b = b'l^{v_l(b)}$ avec $v_l(a)$ et $v_l(b)$ les valuations l-adiques de a et de b. Ainsi, $a'l^{v_l(a)}P + b'l^{v_l(b)}Q = 0$. Sans perte de généralité, on peut supposer que $v_l(a) \leq v_l(b)$. Si $v_l(a) \leq e-1$, en multipliant l'équation précédente par $l^{e-1-v_l(a)}$ on obtient $a'l^{e-1}P + b'l^{e-1+v_l(b)-v_l(a)}Q = 0$, et ainsi $a' \equiv 0\ [l]$, ce qui contredit la définition de $v_l(a)$. Ainsi $v_l(b) \geq v_l(a) \geq e$, donc $a \equiv b \equiv 0\ [l^e]$. Le cas $a = b = 0$ est trivial. Dans le cas où $a \neq 0$ et $b = 0$ par exemple, la preuve précédente reste correcte en écrivant $b = 0 \cdot l^{v_l(a)}$. □

Remarque 4.19. Soit $P, Q \in \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ une un couple d'éléments de la l^e-torsion choisis au hasard. Avec une importante probabilité la famille (P, Q) est libre, ce qui peut être vérifié avec la proposition précédente en un temps proportionnel à e. En effet le calcul de $l^{e-1}P$ peut se faire en temps $O(\log(l^{e-1}) = O(e)$ par l'algorithme d'exponentiation rapide. Ensuite le test de la $\mathbb{Z}/l\mathbb{Z}$ liberté de la famille $(l^{e-1}P, l^{e-1}Q)$ peut se faire en temps $O(l^2) = O(1)$ puisqu'il n'y a que l^2 combinaisons linéaires possibles et puisque l vaut 2 ou 3. Enfin si (P, Q) est $\mathbb{Z}/l^e\mathbb{Z}$-libre c'est aussi une base puisque le nombre de combinaisons linéaires possibles est égal à la cardinalité de $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$.

4.5 Formules de Vélu

Les formules de Vélu servent à construire des isogénies à partir de la connaissance de leur noyau.

Théorème 4.20. *Soit E/K une courbe elliptique et G un sous groupe fini de $E(K)$. Il existe à isomorphisme près une unique courbe elliptique E' et une unique isogénie séparable $\phi : E \to E'$ telle que* $\operatorname{Ker}\phi = G$. *La courbe E' est notée E/G.*

Démonstration. Voir Silverman (1992) III.4.12. □

Les formules de Vélu permettent de calculer explicitement une telle courbe E/G et une telle isogénie ϕ :

Proposition 4.21. *Soit $E/K : y^2 = x^3 + ax + b$ une courbe elliptique et G un sous groupe fini de $E(K)$. Notons G_2 l'ensemble des points d'ordre 2 de G. Soit R un sous ensemble de G tel que $G = \{\infty\} \sqcup G_2 \sqcup R \sqcup (-R)$. Notons $S = R \sqcup G_2$. Pour tout point $Q = (x_Q, y_Q) \in G \setminus \{\infty\}$, notons*

$$u_Q = 4y_Q^2 \quad et \quad v_Q = \begin{cases} (3x_Q^2 + a) \ si\ 2Q = \infty \\ 2(3x_Q^2 + a) \ sinon \end{cases}$$

Posons ensuite

$$v = \sum_{Q \in S} v_Q \quad et \quad w = \sum_{Q \in S} (u_Q + x_Q v_Q)$$

.

Alors E/G est donnée par $y^2 = x^3 + (a - 5v)x + (b - 7w)$, et $\phi(x, y) = (X, Y)$ est donné par les formules suivantes :

$$X = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right)$$

$$Y = y - \sum_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} + \frac{2y_Q(3x_Q^2 + a)}{(x - x_Q)^2} \right)$$

Démonstration. Voir la partie 12.3 dans Washington (2008). □

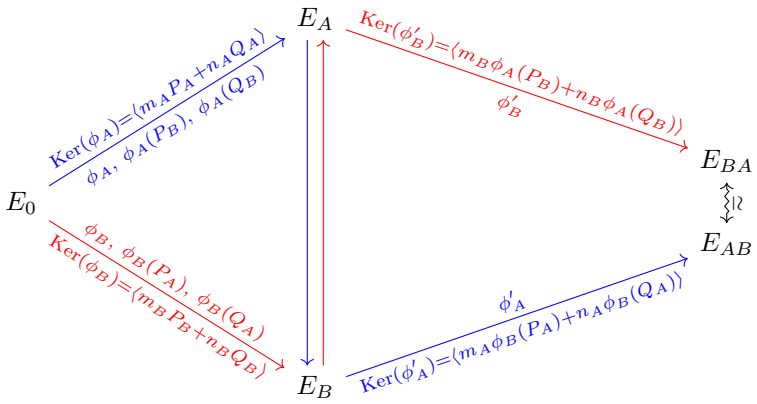
4.6 Le protocole cryptographique

Dans cette partie nous décrivons enfin le protocole SIDH de l'article De Feo *et al.* (2014). Deux correspondants Alice et Bob souhaitent s'échanger secrètement le j-invariant d'une courbe elliptique supersingulière définie sur $\mathbb{F}_{p^2}$.

1. Les paramètres publiques sont une courbe elliptique E_0 comme construite dans la partie 4.3, une base (P_A, Q_A) de la 2^a-torsion et une base (P_B, Q_B) de la 3^b-torsion de E_0.
2. Alice choisit deux entiers secrets m_A et n_A dans $\mathbb{Z}/2^a\mathbb{Z}$ et calcule $\phi_A : E_0 \to E_A$ l'unique isogénie partant de E_0 et de noyau $\langle m_A P_A + n_A Q_A \rangle$ par les formules de Vélu. Alice envoie $\phi_A(P_B)$, $\phi_A(Q_B)$ et E_A à Bob.
3. Bob choisit deux entiers secrets m_B et n_B dans $\mathbb{Z}/3^b\mathbb{Z}$ et calcule $\phi_B : E_0 \to E_B$ l'unique isogénie partant de E_0 et de noyau $\langle m_B P_B + n_B Q_B \rangle$ par les formules de Vélu. Bob envoie $\phi_B(P_A)$, $\phi_B(Q_A)$ et E_B à Alice.
4. Alice calcule $\phi'_A : E_B \to E_{AB}$ de noyau $\langle m_A \phi_B(P_A) + n_A \phi_B(Q_A) \rangle$.

5. Bob calcule $\phi'_B : E_A \to E_{BA}$ de noyau $\langle m_B\phi_A(P_B) + n_B\phi_A(Q_B)\rangle$.

Posons $\alpha = m_AP_A + n_AQ_A$ et $\beta = m_BP_B + n_BQ_B$ et calculons le noyau de $\phi'_B \circ \phi_A$. $P \in \mathrm{Ker}(\phi'_B \circ \phi_A)$ ssi $\phi_A(P) \in \langle \phi_A(\beta)\rangle$ ssi $\phi_A(P) = k\phi_A(\beta)$ ssi $P - k\beta \in \langle\alpha\rangle$ ssi $P \in \langle\alpha, \beta\rangle$. Ainsi, en procédant de même avec $\phi'_A \circ \phi_B$ on obtient que $\mathrm{Ker}(\phi'_A \circ \phi_B) = \mathrm{Ker}(\phi'_B \circ \phi_A) = \langle\alpha, \beta\rangle$. En utilisant le théorème 4.20, cela signifie que les courbes E_{BA} et E_{AB} sont isomorphes. Enfin puisque deux courbes isomorphes possèdent le même j-invariant, Alice et Bob peuvent utiliser ce j-invariant comme secret commun. Le diagramme suivant résume l'échange :



La différence principale avec le protocole Diffie-Hellman classique est la nécessité d'envoyer l'image de points de la base par les isogénies secrètes. La sécurité du protocole repose sur le fait qu'il est difficile de retrouver ϕ_A ou $\mathrm{Ker}\,\phi_A$ à partir de E_A, $\phi_A(P_B)$, et $\phi_A(Q_B)$.

La proposition 4.17 assure qu'il y a suffisamment de sous groupes cycliques dans les 2^a et 3^b-torsions de E_0 pour qu'il y ait suffisamment de courbes E_A et E_B différentes possibles. La proposition 4.18 permet en tirant des éléments au hasard de trouver rapidement une base des torsions.

Des technicités apparaissent dans le calcul de $\phi_A(P_B)$, $\phi_A(Q_B)$ et de E_A par Alice (et de leurs analogues pour Bob). Les formules de Vélu utilisant une somme sur tous les éléments du noyau, 2^a étant grand, il est impossibles de les utiliser directement pour calculer ϕ_A. La solution est de décomposer ϕ_A en a isogénies de degré au plus 2.

Conclusion

J'espère que ce rapport vous aura éclairé comme une sur les courbes elliptiques et sur la cryptographie utilisant les isogénies entre courbes supersingulière. Il se trouve que le protocole SIDH qui semblait être d'une sécurité suffisante a été montré inutilisable à cause d'une nouvelle attaque par Castryck et Decru (2022) publiée début août. Le protocole SIDH aura été un des quatre derniers protocoles retenus par le National Institute of Standards and Technology, l'organisme américain chargé de désigner les protocoles qui seront utilisés sur internet.

Références

Wouter Castryck et Thomas Decru : An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. URL https://eprint.iacr.org/2022/975. https://eprint.iacr.org/2022/975.

Luca De Feo, David Jao et Jérôme Plût : Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014. ISSN 1862-2976. URL https://doi.org/10.1515/jmc-2012-0015.

Joseph H. Silverman : *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. ISBN 0-387-96203-4. Corrected reprint of the 1986 original.

Lawrence C. Washington : *Elliptic curves*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, second édition, 2008. ISBN 978-1-4200-7146-7 ; 1-4200-7146-7. URL https://doi.org/10.1201/9781420071474. Number theory and cryptography.

A Code

Le code ci-dessous utilise le logiciel libre SageMath, et peut normalement être exécuté sans modifications. Avec une telle implémentation je peux calculer un échange avec un nombre p de 784 bits en quelques dizaines de secondes. L'endroit où l'algorithme passe le plus de temps est dans la recherche d'une base de la torsion.

Recherche d'un nombre premier p

```
lA = 2
eA = 300

lB = 3
eB = 300

f = 1
p = lA ^ eA * lB ^ eB * f - 1
while f % lA == 0 or f % lB == 0 or p not in Primes():
    f += 1
    p = lA ^ eA * lB ^ eB * f - 1

print("p : ", p)
print("Sécurité : log2(p)=", numerical_approx(log(p)/log(2)))
print("Debug : f =", f)

q = p^2
Fq = FiniteField((p, 2), 'a')
```

Recherche d'une courbe initiale

```
E = EllipticCurve([Fq(0), Fq(1)])
print(E)
print("Supersingulière :", E.is_supersingular())
desiredCardinality = (lA ^ eA * lB ^ eB * f) ^ 2
print("Bonne cardinalité :", E.cardinality() == desiredCardinality)
```

Base des torsions

```
is_a_base = False
while not is_a_base:
    PA = 0
    while PA.order() != lA^eA: PA = (lB^eB * f) ^2 * E.random_point()
    QA = 0
    while QA.order() != lA^eA: QA = (lB^eB * f) ^2 * E.random_point()
    is_a_base = PA.weil_pairing(QA, lA^eA) ^ (lA^(eA-1)) != 1

is_a_base = False
while not is_a_base:
    PB = 0
    while PB.order() != lB^eB: PB = (lA^eA * f) ^2 * E.random_point()
    QB = 0
    while QB.order() != lB^eB: QB = (lA^eA * f) ^2 * E.random_point()
    is_a_base = PB.weil_pairing(QB, lB^eB) ^ (lB^(eB-1)) != 1
```

Chaine d'isogénies

```
def chain_isogenies(E, R, l, e, points):
    phi = E.identity_morphism()
    Ei = E
    Ri = R
    for i in range(e):
        phi_i = Ei.isogeny(l^(e-i-1) * Ri)
        Ri = phi_i(Ri)
        Ei = phi_i.codomain()
        points = [phi_i(P) for P in points]
    return (Ei, points)
```

Création des secrets et calcul des isogénies

```
def random_secret(l, e):
    badCouple = True
    while badCouple:
        m, n = randrange(l^e), randrange(l^e)
        badCouple = m % l == 0 and n % l == 0
    return (m, n)

mA, nA = random_secret(lA, eA)

(EA, [phiA_PB, phiA_QB]) = chain_isogenies(E, mA * PA + nA * QA, lA, eA, [PB, QB])

print("Secret :", mA, nA)
```

```
print("Publique :", EA)
print("Publique :", phiA_PB, phiA_QB)

mB, nB = random_secret(lB, eB)

(EB, [phiB_PA, phiB_QA]) = chain_isogenies(E, mB * PB + nB * QB, lB, eB, [PA, QA])

print("Secret :", mB, nB)
print("Publique :", EB)
print("Publique :", phiB_PA, phiB_QA)
```

Détermination du secret commun

```
chain_isogenies(EB, mA * phiB_PA + nA * phiB_QA, lA, eA, [])[0].j_invariant()
chain_isogenies(EA, mB * phiA_PB + nB * phiA_QB, lB, eB, [])[0].j_invariant()
```