Courbes Elliptiques et Calcul d'Ordre

Dario Shariatian

TIPE ENS 2019

Table des matières

Introduction

Le but de cette étude est de présenter la théorie des courbes elliptiques, en particulier dans le cadre des corps finis. Il s'agira d'en donner les propriétés principales, ainsi que les outils nécessaires à l'utilisation pratique d'un tel objet. On pense notamment à la mise en place d'un cryptosystème, une des applications les plus populaires de la théorie, qui tire à son avantage le problème du logarithme discret sur le groupe que forment les points d'une courbe. On se concentrera donc sur des questions de structure, conjointement à la mise en place d'algorithmes efficaces. Ces derniers concerneront principalement des calculs de cardinalité, et le point culminant de ce travail sera l'algorithme de Schoof (1985), historiquement connu comme le premier algorithme déterministe comptant en temps polynomial les points sur une courbe.

Première partie
Construction et Définitions

Les courbes elliptiques furent d'abord introduites pour la résolution d'équations diophantiennes, formant une structure sous-jacente à l'ensemble de leurs solutions. Il s'agit des solutions à une *équation de Weierstrass* $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. En effet, il est possible de munir l'ensemble des points d'une courbe d'une loi de groupe, géométriquement interprétée comme loi de *sécante-tangente* ; depuis un ou plusieurs points de la courbe représentants des solutions particulières à une équation diophantienne, il est alors possible d'en trouver une multitude d'autre, et possiblement toutes.

Il s'avère en fait que l'on sait bien caractériser la structure de tels groupes.

1 Construction

Définition 1.1. *Espace Projectif* Soit E un $\mathbb{K}$-espace vectoriel non nul. On définit sur E la relation d'équivalence $\equiv$: $\forall x, y \in E, \quad x \equiv y \Leftrightarrow x \in y\mathbb{K}$. Alors on appelle espace projectif sur E l'ensemble $P(E) = E/_{\equiv}$. On appelle espace projectif de dimension 2 associé à un corps $\mathbb{K}$, noté $\mathbb{P}^2(\mathbb{K})$, l'espace projectif $P(\mathbb{K}^3)$. Les classes $(X, Y, Z) \in \mathbb{P}^2(\mathbb{K})$ sont appelées coordonnées homogènes.

Définition 1.2. *Courbe Elliptique*

Une courbe elliptique est une courbe lisse définie sur un corps commutatif $\mathbb{K}$. Notée $E(\mathbb{K})$, elle correspond à l'ensemble des racines dans $\mathbb{P}^2(\mathbb{K})$ d'un polynôme $F \in \mathbb{K}[X, Y, Z]$ homogène de degré 3 en 3 variables vérifiant *une équation de Weierstrass* : $E(\mathbb{K}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{K}) \quad / \quad F(X, Y, Z) = X^3 + a_1X^2Z + a_2XZ^2 + a_3Z^3 - Y^2Z - a_4XYZ - a_5YZ^2 = 0\}$

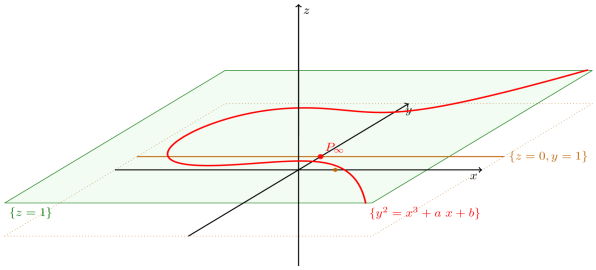
La dénomination *courbe lisse* signifie que l'on peut définir une tangente en tout point de la courbe : $\forall P \in E(\mathbb{K}), \quad (\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)) \neq (0, 0, 0)$.

Définition 1.3. *Coordonnées Non Homogènes et Point à l'Infini*

Pour toutes courbes, seule une classe vérifie $Z = 0$, c'est la classe $(0, 1, 0)$ nommée point à l'infini et notée $\mathcal{O}$. On remarquera de plus que $\mathcal{O}$ n'est jamais un point singulier.

Pour toutes les autres classes, comme $Z \neq 0$, il existe un unique représentant de la forme $(X, Y, 1)$. On peut donc réécrire l'équation de Weierstrass vérifiée par la courbe dans le plan $Z = 1$ à l'aide des coordonnées non homogènes $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$ et on peut tout simplement voir la courbe comme la solution d'une équation de Weierstrass dans le plan muni d'un point à l'infini :

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \quad / \quad y^2 + a_4xy + a_5y = x^3 + a_1x^2 + a_2x + a_3\} \cup \{\mathcal{O}\}$$



On pourra aussi définir une courbe E par l'équation qu'elle vérifie (par exemple $E : y^2 = x^3 + ax + b$).

1.1 Équation de Weierstrass Réduite

Si la caractéristique du corps $\mathbb{K}$ est différente de 2 et 3, alors en faisant les changements de variable successifs $y \to 1/2(y - a_1x - a_3)$ puis $(x, y) \to ((x - 3b_2)/36, y/216)$ dans E, où $b_2 = a_1^2 + 4a_2$, on obtient $E : y^2 = x^3 - 27c_4x - 54c_6$ avec $b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Dès lors on peut travailler avec une *équation de Weierstrass réduite* : $E : y^2 = x^3 + Ax + B$. Dorénavant on ne travaillera que sur des corps de caractéristique différente de $2, 3$.

2 Loi de Groupe

2.1 Aspect géométrique

Théorème 2.1. Admis *Troisième point*

Soient E une courbe elliptique et D une droite, toutes deux définies sur un corps $\mathbb{K}$. Si D coupe E en deux points, alors D coupe E en trois points.

Définition 2.1. Soit $E(\mathbb{K})$ une courbe elliptique définit sur un corps $\mathbb{K}$.
- Soient deux points distincts $P, Q \in E(\mathbb{K})$, Si $P \neq Q$ alors la droite (PQ) recoupe la courbe E en un troisième point $R = P * Q$.
- Soit un point $P \in E(\mathbb{K})$, on peut alors définir le point $P * P$ comme le point d'intersection de la courbe $E(\mathbb{K})$ avec sa tangente au point P (existence **admise**).

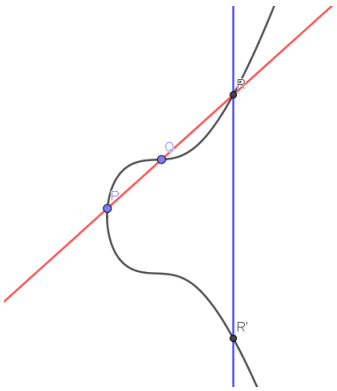


FIGURE 1 – Construction du troisième point

2.2 Structure de groupe

Théorème 2.2. *Structure de groupe*

Soit $\mathbb{K}$ un corps. Si E est une courbe elliptique définie sur $\mathbb{K}$, alors la loi : $+ : (P, Q) \longmapsto \mathcal{O} * (P * Q)$ confère à E une structure de groupe abélien d'élément neutre $\mathcal{O}$.

Proposition Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur un corps $\mathbb{K}$ et $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{K})$ avec $P_1, P_2 \neq \mathcal{O}$. On a alors $P_1 + P_2 = P_3 = (x_3, y_3)$ avec :

1. $x_1 \neq x_2$. Alors $x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y1,$ avec $m = \frac{y_2 - y_1}{x_2 - x_1}$.
2. $x_1 = x_2$ mais $y_1 \neq y_2$. Alors $P3 = \mathcal{O}$.
3. $P_1 = P_2$ et $y1 \neq 0$. Alors $x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1,$ avec $m = \frac{3x_1 + a}{2y_1}$
4. $P_1 = P_2$ et $y_1 = 0$. Alors $P_3 = 0$. De plus $\forall P \in E(\mathbb{K}),\ P + \mathcal{O} = P$.

3 Endomorphismes

On donne quelques propriétés sur les endomorphismes de courbes elliptiques, qui nous seront utiles dans la suite. En particulier cela va nous permettre d'obtenir des résultats relatifs à l'endomorphisme de Froebenius, essentiel aux questions de calculs d'ordre, ainsi que l'endomorphisme correspondant à la multiplication d'un point par un entier n.

3.1 Définitions et Propriétés

Définition 3.1. *Endomorphisme de courbe elliptique*

Un endomorphisme de courbe elliptique est un morphisme $\alpha : E(\overline{\mathbb{K}}) \longrightarrow E(\overline{\mathbb{K}})$ donné par des fonctions rationnelles $R_1, R_2 \in \overline{\mathbb{K}}(X, Y)$, donc tel que $\alpha(x, y) = (R_1(x, y), R_2(x, y))$. $\overline{\mathbb{K}}$ désigne la clôture algébrique de $\mathbb{K}$. L'espace des endomorphismes d'une courbe E, notée $\mathrm{End}(E)$, est stable par composition et multiplication par un entier.

Exemple Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur $\mathbb{K}$ de caractéristique différente de 2 ou 3. Le morphisme $\alpha : P \mapsto 2P$ est tel que $\alpha(x, y) = (m^2 - 2x, m(3x - m^2) - y)$ où $m = \dfrac{3x + a}{2y}$. Il est alors clair que α est un endomorphisme de courbe elliptique.

Théorème 3.1. Tout endomorphisme de courbe elliptique α peut s'exprimer par la donnée d'un couple $(r_1, r_2) \in (\overline{\mathbb{K}}(X))^2$ tel que $\alpha(x, y) = (r1(x), yr_2(x))$.

Démonstration. Soit α un endomorphisme de courbe elliptique $E : y^2 = x^3 + ax + b$. On se donne $R_1, R_2 \in \overline{\mathbb{K}}(X, Y)$ tel que $\alpha(x, y) = (R_1(x, y), R_2(x, y))$.

Pour $R = R_i$, on peut écrire $R(x, y) = \dfrac{p_1(x) + yp_2(x)}{p_3(x) + yp_4(x)}$ et en multipliant par $p_3(x) - yp_4(x)$, comme $y^2 = x^3 + ax + b$: $R(x, y) = \dfrac{s_1(x) + ys_2(x)}{s_3(x)} = q_1(x) + yq_2(x)$ où $p_i, s_i \in \overline{\mathbb{K}}[X]$ et $q_i \in \overline{\mathbb{K}}(X)$. Mais $\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y)$ donc $R_1(x, -y) = R_1(x, y)$ et $R_2(x, -y) = -R_2(x, y)$. Ainsi $R_1 \in \overline{\mathbb{K}}(X), R_2 \in y\overline{\mathbb{K}}(X)$ ce qui conclut. □

Théorème 3.2. Soit $\alpha \in \mathrm{End}(E)$, α étant décrit par $(r_1 = \dfrac{p}{q}, r_2)$. Alors pour $P = (x, y) \in E(\overline{\mathbb{K}}), P \neq \mathcal{O}$, $\alpha(P) = \mathcal{O} \Longleftrightarrow q(x) = 0$. Le sens indirect est admis par convention.

Démonstration. Supposons $q_1(x_0) \neq 0$ et montrons que $r_2(x_0)$ est bien définie. Dés lors on aura $\alpha(x_0, y_0) \neq \mathcal{O}$. On écrit $r_2 = \dfrac{s}{t}, s \wedge t = 1$. Comme pour $(x, y), \alpha(x, y) \in E(\overline{\mathbb{K}})$: $(yr_2)^2 = r_1^3 + ar_1 + b$ et donc $(x^3 + ax + b)\dfrac{s^2}{t^2} = \dfrac{p_1^3 + ap_1q_1^2 + bq_1^3}{q_1^3}$.
Ainsi $t^2 \mid (x^3 + ax + b)q_1^3$ car $s \wedge t = 1$. Or les racines de $x^3 + ax + b$ sont simples (la courbe est lisse) contrairement à celles de t^2 qui sont multiples. Comme x_0 n'est pas racine de q_1, il est alors clair qu'il n'est pas non plus racine de t, ce qui conclut. □

Définition 3.2. *Degré d'un endomorphisme de courbe elliptique*

Pour $\alpha \in \mathrm{End}(E)$ décrit par $(r_1 = \dfrac{p}{q}, r_2)$, on définit son degré par $\deg(\alpha) = \max(deg(p), deg(q))$ si $\alpha \neq 0$, $deg(\alpha) = 0$ sinon.

Définition 3.3. *Séparabilité*

$\alpha \in \mathrm{End}(E)$ est dit séparable si $r_1' \neq 0$. Cela est équivalent à $(p', q') \neq (0, 0)$ où $r_1 = \dfrac{p}{q}, p \wedge q = 1$.

Le théorème suivant est essentiel à la démonstration du theorème de Hasse qui sera présenté plus tard.

Théorème 3.3. Soit E une courbe elliptique, $\alpha \neq 0 \in \mathrm{End}(E)$. Alors :

1. Si α est séparable, alors $\deg(\alpha) = \#Ker(\alpha)$
2. Sinon $\deg(\alpha) > \#Ker(\alpha)$

Démonstration. On utilise les notations habituelles. Comme $r_1' \neq 0$, $p'q - pq' \neq 0$. Soit S l'ensemble des racines dans $\overline{\mathbb{K}}$ de $(p'q - pq')$. On se donne $(a, b) \in E(\overline{\mathbb{K}})$ tel que :

1. $a, b \neq 0, (a, b) \neq \mathcal{O}$
2. $\deg(p - aq) = \max(deg(p), deg(q)) = \deg(\alpha)$
3. $a \notin r_1(S)$
4. $(a, b) \in \alpha(E(\overline{\mathbb{K}}))$

Comme α est séparable, $p'q - pq' \neq 0$ donc S est fini. De plus $Im_{\overline{\mathbb{K}}} r_1$ est infini et comme $\forall x \in \overline{\mathbb{K}} \exists y \in \overline{\mathbb{K}}/(x,y) \in E(\overline{\mathbb{K}})$, $\alpha(E(\overline{\mathbb{K}}))$ est infini. Un tel point (a,b) existe. Pour l'un d'entre eux montrons que $\#\alpha^{-1}(a,b) = \deg(\alpha)$. Comptons les points $(x,y) \in E(\overline{\mathbb{K}})/\alpha(x,y) = (a,b)$. Si l'on s'en donne un on peut écrire :

$$\frac{p(x)}{q(x)} = a, \quad yr_2(x) = b$$

Mais $(a,b) \neq \mathcal{O}$ donc $q(x) \neq 0$. De plus $b \neq 0$ donc on a $y = \frac{b}{r_2(x)}$; les valeurs de x déterminent celle de y. Comptons donc les valeurs de x. On sait que $p - aq$ possède $\deg(\alpha)$ racine comptées avec multiplicité. Supposons par l'absurde que x_0 en soit une racine multiple. Dès lors $p(x_0) - aq(x_0) = p'(x_0) - aq'(x_0) = 0$ et $p(x_0)q'(x_0) = p'(x_0)q(x_0)(a \neq 0)$, et $x_0 \in S$ i.e $a = r_1(x_0) \in r_1(S)$ ce qui est impossible. On obtient donc l'égalité recherchée $\#\alpha^{-1}(a,b) = deg(p - aq) = \deg(\alpha)$. Enfin, cela met en évidence que le cardinal des classes de $E(\overline{\mathbb{K}})_{/ker(\alpha)}$ est égal à $\deg(\alpha)$ (α est un morphisme rappelons-le) et en particulier : $\deg(\alpha) = \#ker(\alpha)$.

Dans le cas où α est séparable, il suffit de mener le même raisonnement que précédemment avec comme seuls restrictions sur le couple $(a,b) \in \alpha(E(\overline{\mathbb{K}}))$ les points (1), (2), et (4) (plus besoin de l'ensemble S). Comme cette fois $p' - aq' = 0$, $p - aq$ a toujours des racines multiples et admet strictement moins de solutions que $\deg(\alpha)$ ce qui conclut. □

Théorème 3.4. *Surjectivité*

Soit $\mathbb{K}$ un corps algébriquement clôt. Un endomorphisme de courbe elliptique $E : y^2 = x^3 + ax + b$ est surjectif.

Démonstration. Soit $(e_x, e_y) \in E(\overline{\mathbb{K}})$. Puisque $\alpha(\mathcal{O}) = \mathcal{O}$, on peut supposer $(e_x, e_y) \neq \mathcal{O}$. On reprend les notations habituelles, avec α décrit par r_1, r_2 etc.

Comme $deg(\alpha) = \#ker(\alpha)$ est fini, les classes de $E(\mathbb{K})_{/ker(\alpha)}$ sont finies. De plus pour $x' \in \mathbb{K}$, il n'y a qu'un nombre fini de solutions y' à $y'^2 = x'^3 + a'x + b'$ (il y en a 2).

Ainsi $\{(x,y) \in E(\mathbb{K}) \ / \ \exists y' \in \overline{\mathbb{K}} \ / \ \alpha(x,y) = (r_1(x), yr_2(x)) = (\frac{p(x)}{q(x)}, yr_2(x)) = (x', y')\}$ est fini. Mais $E(\mathbb{K})$ est infini donc $\frac{p}{q}$ ne peut pas être constant. En fait p et q ne peuvent être toutes deux constantes.

Dès lors $p - e_x q$ n'est pas constant et on peut s'en donner x_0 une racine. Comme $p \wedge q = 1$ on ne peut avoir $q(x_0) = 0$. On se donne $y_0 \in \mathbb{K}$ racine de $x_0^3 + ax_0 + b$ ($\mathbb{K}$ algébriquement clôt). Comme $q(x_0) \neq 0$, par une propriété précédente on est assuré que $\alpha(x_0, y_0)$ est définie et de plus $\alpha(x_0, y_0) = (e_x, e'_y)$ où $e'^2_y = e_y^2 = e_x^3 + ae_x + b$. Ainsi quitte à remplacer y_0 par $-y_0$ on a trouvé un antécédent par α de (e_x, e_y). □

3.2 Endomorphismes de Froebenius et d'Exponentiation

Définition 3.4. *Endomorphisme de Froebenius*

Soit $E(\mathbb{F}_q), q = p^n$ une courbe elliptique définie sur $\mathbb{F}_q$. On définit l'endomorphisme de Froebenius par $\phi_q : (x,y) \in \overline{\mathbb{F}_q} \longmapsto (x^q, y^q)$. ϕ_q agit donc comme l'identité sur $\mathbb{F}_q$.

Théorème 3.5. $\phi_q \in \mathrm{End}(E), \deg(\phi_q) = q$ et ϕ_q n'est pas séparable.

Démonstration. Il est clair que ϕ_q est décrit par des fonctions rationnelles et qu'il est de degré q. Montrons qu'il s'agit d'un morphisme de $\overline{\mathbb{F}_q} \longmapsto \overline{\mathbb{F}_q}$. On a besoin de deux propriétés : comme la caractéristique de $\overline{\mathbb{F}_q}$ est p, $(x+y)^q = x^q + y^q$. De plus, toutes les racines de $X^q - X$ sont les éléments de $\mathbb{F}_q$, ni plus ni moins. De là on conclura aisément. Soient $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}_q})$:

— Si $x_1 \neq x_2$, la somme (x_3, y_3) est tel que :

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

Il est clair après exponentiation par q que : $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$

— Si $x_1 = x_2$ cette fois :

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{3x_1^3 + a}{2y_1}$$

Or $2, 3, a \in \mathbb{F}_q$ donc l'exponentiation agit sur eux comme l'identité et la formule d'addition reste tout aussi vraie.

Enfin, la dérivée de x^q est identiquement nulle donc ϕ_q n'est pas séparable. □

Les théorèmes suivants reposent sur un lemme portant sur l'addition d'endomorphismes. Je me permet d'en omettre la démonstration, fastidieuse. Les deux théorèmes en découlant s'obtiennent alors presque immédiatement.

Lemme 3.6. Admis Soit E une courbe elliptique, $\alpha_1, \alpha_2, \alpha_3 \in \text{End}(E)\backslash\{0\}$ / $\alpha_1 + \alpha_2 = \alpha_3$. Alors en écrivant $\alpha_i(x, y) = (R_i(x), yS_i(x))$ et avec $c_i = \dfrac{R_i'}{S_i}$, si c_1, c_2 sont constants alors $c_1 + c_2 = c_3$.

Théorème 3.7. Admis *Multiplication par un entier*

Soit E une courbe elliptique définie sur $\mathbb{K}$ et n un entier non nul. La multiplication d'un point par un entier n, notée m_n, est un endomorphisme de E, séparable si et seulement si $p = \text{car}(\mathbb{K}) \nmid n$. En effet, en écrivant $m_n(x, y) = (r_1(x), yr_2(x))$, $\dfrac{r_1'}{r_2} = n$.

Démonstration. Récurrence à l'aide du lemme 3.6, le cas n = 1 étant trivial. On obtient ainsi aisément le résultat pour les n positifs, et si on note $m_n(x, y) = (r_{1,n}(x), yr_{2,n}(x))$, alors $r_{1,n} = r_{1,-n}$ et $r_{2,n} = -r_{2,-n}$ donc $\frac{r_{1,n}'}{r_{2,n}} = -\frac{r_{1,-n}}{r_{2,-n}}$ et le résultat tient pour les négatifs. □

Théorème 3.8. Admis Soit $E(\mathbb{F}_q)$ une courbe elliptique définie sur $\mathbb{F}_q$, $q = p^n$. L'endomorphisme $r\phi_q + s$ est séparable si et seulement si $p \nmid s$.

Démonstration. On note $m_r(x, y) = (R_{1,r}(x), yR_{2,r}(x))$.

Alors $(r\phi_q)(x, y) = (R_{1,r\phi_q}(x), yR_{2,r\phi_q}(x)) = (R_{1,r}(x^q), yR_{2,r}(x^q))$ et $\dfrac{R'_{1,r\phi_q}}{R_{2,r\phi_q}} = \dfrac{qx^{q-1}R'_{1,r}(x^q)}{R_{2,r}(x^q)} = 0$ (corps de caractéristique p). Dès lors, avec $(r\phi_q + s)(x, y) = (R_{1,r\phi_q+s}(x), yR_{2,r\phi_q+s}(x))$ on a $\dfrac{R'_{1,r\phi_q+s}}{R_{2,r\phi_q+s}} = 0 + s$ ce qui conclut. □

3.3 Polynômes de Division

Définition 3.5. *Polynômes de Division*

L'ensembles des polynômes de division est une suite de polynôme $(\psi_n)_{n\in\mathbb{N}} \in \mathbb{K}[X, Y, A, B]$ définie récursivement par :

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2Y$$

$$\psi_3 = 3X^4 + 6AX^2 + 12BX - A^2$$

$$\psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A3)$$

$$\begin{cases} \psi_{2n+1} = & \psi_{n+2}\psi_n^3 - \psi_{n+1}\psi_{n-1} \quad \text{pour } n \geq 2 \\ \psi_{2n} = & \dfrac{\psi_n}{2Y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad \text{pour } n \geq 3 \end{cases}$$

Le polynôme ψ_n est appelé le n-ième polynôme de division.

Remarque Une récurrence immédiate montre que $\psi_{2n} \in Y\mathbb{K}[X], \psi_{2n+1} \in \mathbb{K}[X]$.

Théorème 3.9. Admis Une récurrence permet de montrer que :

$$\begin{cases} n \text{ pair} : \deg(\dfrac{\psi_n}{y}) = \dfrac{n^2-4}{2} \\ n \text{ impair} : \deg(\psi_n) = \dfrac{n^2-1}{2} \end{cases}$$

Le théorème suivant révèle tout l'intérêt de cet objet.

Théorème 3.10. Admis Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur $\mathbb{K}$. En notant $m_n \in \mathrm{End}(E)$ l'endomorphisme correspondant à la multiplication par un entier n :

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right) = \left(x - \frac{\psi_{n-1}(x)\psi_{n+1}(x)}{\psi_n^2(x)}, \frac{\psi_{2n}(x,y)}{2\psi_n^4(x)}\right)$$

Où $\phi_n(X) = X\psi_n^2 - \psi_{n+1}\psi_{n-1}$ et $\omega_n(X,Y) = \dfrac{\psi_{2n}}{2\psi_n}$.

Corollaire 3.10.1. Admis Soit $E : y^2 = x^3 + Ax + B$ définie sur $\mathbb{K}$ une courbe elliptique. En notant $m_n \in \mathrm{End}(E)$ l'endomorphisme correspondant à la multiplication par un entier n. Alors $\deg(m_n) = n^2$.

La partie délicate de la démonstration de ce corollaire est le fait que $\phi_n \wedge \psi_n = 1$. En effet, dès lors, $\deg(m_n) = \max(\deg(\phi_n), \deg(\psi_n^2)) = n^2$.

4 Points de torsion

Définition 4.1. *Sous-groupe des points de n-torsion* Soit E une courbe elliptique. On définit $E[n]$ le sous-groupe des points de n-torsion de E par : $E[n] = \{P \in E(\overline{\mathbb{K}}) \ / \ nP = \mathcal{O}\}$

Exemple Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique. Caractérisons $E[2]$. Comme on travaille dans $\overline{\mathbb{K}}$, on peut se donner $e_1, e_2, e_3 \in \overline{\mathbb{K}}$ tel que $y^2 = (x - e_1)(x - e_2)(x - e_3)$. On l'avait déjà vu auparavant, les racines de $x^3 + ax + b$ sont forcément simple ; autrement, avec x_0 une racine multiple et $F : (x, y) \mapsto y^2 - x^3 - ax - b$ on a $(\dfrac{\partial F}{\partial x}(x_0, 0), \dfrac{\partial F}{\partial y}(x_0, 0)) = (0, 0)$. Cela est impossible car $(x_0, 0) \in E(\overline{\mathbb{K}})$ mais $E(\overline{\mathbb{K}})$ n'est pas singulière. Il est alors clair que $E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$ et comme on a aussi $(e_1, 0) + (e_2, 0) = (e_3, 0)$ en fait :

$$E[2] \cong \mathbb{F}_2 \times \mathbb{F}_2$$

Il s'avère que ce résultat se généralise.

Théorème 4.1. Soit E une courbe elliptique, $\mathbb{K}$ un corps de caractéristique p. Alors :
- Si $p \nmid n$ alors $E[n] \cong \mathbb{Z}_{/n\mathbb{Z}} \times \mathbb{Z}_{/n\mathbb{Z}}$.
- Sinon, avec $n = n'p^r$: $E[n] \cong \mathbb{Z}_{/n'\mathbb{Z}} \times \mathbb{Z}_{/n'\mathbb{Z}}$ ou bien $E[n] \cong \mathbb{Z}_{/n'\mathbb{Z}} \times \mathbb{Z}_{/n\mathbb{Z}}$.

Démonstration. Supposons d'abord $p \nmid n$. Alors m_n l'endomorphisme de multiplication par n est séparable et $\#E[n] = \#ker(m_n) = \deg(m_n) = n^2$. Or le théorème de structure des groupes abéliens finis nous permet d'écrire que :

$$E[n] \cong \mathbb{Z}_{/n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}_{/n_k\mathbb{Z}}$$

où $n_i | n_{i+1}$. Soit $p' \in \mathbb{P}$ un nombre premier tel que $p' | n_1$. Il est alors clair que $E[p'] \subseteq E[n]$. Comme p' est premier, le théorème de structure permet cette fois d'écrire $E[p'] \cong (\mathbb{Z}_{/p'\mathbb{Z}})^k$ donc $\#E[p'] = p'^k$. Or $p' | n$ donc $p' \neq p$ et comme on vient de le voir : $\#E[p'] = p'^2$. Ainsi $k = 2$ et $E[n] \cong \mathbb{Z}_{/n_1\mathbb{Z}} \times \mathbb{Z}_{/n_2\mathbb{Z}}$ où $n_1 | n_2 | n$. Enfin la relation $\#E[n] = n^2$ permet de conclure : $E[n] \cong \mathbb{Z}_{/n\mathbb{Z}} \times \mathbb{Z}_{/n\mathbb{Z}}$

Désormais, supposons que $p | n$. Déterminons les cardinaux de $E[p^k]$. Comme m_p n'est pas séparable, $\#ker(m_p) < \deg(m_p) = p^2$. Donc $\#E[p] = \#ker(m_p) \in \{1, p\}$. Si $\#E[p] = 1$ alors quel que soit k, $\#E[p^k] = 1$. Sinon, montrons que $E[p^k]$ est cyclique d'ordre p^k. Soit P un point d'ordre p^i. Comme tout endomorphisme de courbe elliptique est surjectif on se donne $Q \in m_p^{-1}(P)$. Dès lors, $p^i Q = p^{i-1} P \neq \mathcal{O}$ mais $p^{i+1} Q = \mathcal{O}$. On conclut par une récurrence immédiate.

Enfin, comme $p \nmid n'$ on peut écrire

$$E[n] \cong E[n'] \oplus E[p^r]$$

De plus $E[n'] \cong \mathbb{Z}_{/n'\mathbb{Z}} \times \mathbb{Z}_{/n'\mathbb{Z}}$ et comme $E[p^r] \cong \{0\}$ ou $(\mathbb{Z}_{/p^r\mathbb{Z}})$ avec $p \wedge n' = 1$,par théorème des restes chinois $E[n]$ possède bien la structure annoncée. □

5 Accouplement de Weil

Définition 5.1. Existence admise *Accouplement de Weil*

Soit $E(\mathbb{K}) : y^2 = x^3 + ax + b$ une courbe elliptique et n entier tel que $\text{car}(\mathbb{K}) \nmid n$. Alors en notant $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité, il existe $e_n : E[n] \times E[n] \to \mathbb{U}_n$ tel que :

1. e_n est bilinéaire.
2. e_n est non dégénéré en chaque variable.
3. $\forall P \in E[n], e_n(P, P) = 1$
4. $\forall P, Q \in E[n], e_n(P, Q) = e_n(Q, P)^{-1}$
5. $\forall P, Q \in E[n], \sigma \in \text{Aut}(\overline{\mathbb{K}}), \sigma_{|\{a,b\}} = Id \Longrightarrow e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q))$
6. $\forall P, Q \in E[n], \alpha \in \text{End}(E)$ separable , $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg(\alpha)}$

Théorème 5.1. Soit (P, Q) une base de $E[n]$. Alors $e_n(P, Q)$ est une racine primitive de $\mathbb{U}_n$.

Démonstration. Posons $\zeta = e_n(P, Q)$ et donnons-nous d tel que $\zeta^d = 1$. Alors $e_n(P, dQ) = 1$. Soit $R = aP + bQ \in E[n]$. $e_n(S, dQ) = e_n(P, dQ)^a e_n(Q, dQ)^b = 1$. Or en sa deuxième variable fixée, e_n n'est pas dégénérée donc forcément $dQ = \mathcal{O}$ et $n|d$. ζ est un racine primitive de l'unité. □

Théorème 5.2. Soit $\alpha \in \text{End}(E)$, n entier tel que $\text{car}(\mathbb{K}) \nmid n$. Alors $\det(\alpha_n) \equiv \deg(\alpha) \bmod n$ où α_n est une matrice de α dans $E[n] \cong (\mathbb{Z}_{/n\mathbb{Z}})^2$

Démonstration. Soit (P, Q) une base de $E[n]$. $\zeta = e_n(P, Q)$ est alors une racine primitive de n-ième de l'unité. Dès lors :

$$\zeta^{\deg(\alpha)} = e_n(\alpha(P), \alpha(Q)) = e_n(aP + cQ, bP + dQ) = e_n(P, Q)^{ad} e_n(Q, P)^{bc} = e_n(P, Q)^{\det(\alpha_n)}$$

Donc $\det(\alpha_n) \equiv \deg(\alpha) \bmod n$. □

Deuxième partie
Étude sur les Corps Finis

6 Théorème de Hasse sur les Courbes Elliptiques

On invite le lecteur à relire les propriétés de l'endomorphisme de Froebenius. On remarque en particulier que sur $\mathbb{F}_q$, où $q = p^n$, $\ker(\phi_q - 1) = E(\mathbb{F}_q)$ pour E une courbe elliptique. De plus, ϕ_q n'est pas séparable tandis que $\phi_q - 1$ l'est car $p \nmid -1$. On a besoin d'un petit lemme :

Lemme 6.1. En dimension 2, l'application det est une forme quadratique associée à la forme polaire $(N, M) \mapsto \dfrac{1}{2} tr({}^t com(N)M)$. Dès lors, pour N, M deux matrices carrées de taille 2, $a, b \in \mathbb{K}$: $\det(aN + bM) = a^2\det(N) + b^2\det(M) + ab(\det(N + M) - \det(N) - \det(M))$

Théorème 6.2. *Théorème de Hasse sur les courbes elliptiques*

Soit E une courbe elliptique. Alors : $|a| = |q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$

Démonstration. D'après le lemme précédent, avec $\phi_{q,n}$ l'automorphisme de $E[n]$ associé à ϕ_n : $\det(r\phi_{q,n} - s) = r^2\det(\phi_{q,n}) + s^2 - rs(\det(\phi_{q,n} - 1) - \det(-1) - \det(\phi_{q,n})$. Or on avait démontré à l'aide de l'accouplement de Weil que $\deg(\alpha) \equiv \det(\alpha_n) \bmod n$ pour tout $\alpha \in \text{End}(E), n \in \mathbb{N}^*$. Comme la congruence tient quel que soit n, il y a en fait égalité. Ainsi :

$$\deg(r\phi_q - s) = r^2 q + s^2 + rs(q + 1 - \deg(\phi_q - 1))$$

car $\deg(\phi_q) = q$ et $\deg(-1) = 1$. Or $\phi_q - 1$ est séparable donc $\deg(\phi_q - 1) = \#E(\mathbb{F}_q)$ et $\deg(r\phi_q - s) = r^2 q + s^2 + rsa$. Comme $\deg(r\phi_q - s) \geq 0$, on a donc :

$$q(\frac{r}{s})^2 + a\frac{r}{s} + 1 \geq 0$$

Sur $\{\dfrac{r}{s} \ / \ s \wedge q = 1, \dfrac{r}{s} \in \mathbb{Q}\}$ dense dans $\mathbb{R}$. Ainsi $qX^2 + aX + b \geq 0$ et $a^2 - 4q \leq 0$ ce qui conclut.

□

7 Structure

Théorème 7.1. Soit E une courbe elliptique. Alors :

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{/n\mathbb{Z}} \quad \text{ou} \quad E(\mathbb{F}_q) \cong \mathbb{Z}_{/n_1\mathbb{Z}} \times \mathbb{Z}_{/n_2\mathbb{Z}} (n_1 | n_2)$$

Démonstration. Le théorème de structure des groupes abéliens finis permet d'affirmer que $E(\mathbb{F}_q) \cong \mathbb{Z}_{/n_1\mathbb{Z}} \times \cdots \times \mathbb{Z}_{/n_r\mathbb{Z}}$, où $n_i | n_{i+1}$. Dès lors, comme $E[n_1] \subset E(\mathbb{F}_q)$ il est clair que $\#E[n_1] = n_1^r$. Mais $\#E[n_1] = \#\ker(m_{n_1}) \leq \deg(m_{n_1}) = n_1^2$ donc $r \leq 2$ ce qui conclut. □

8 Calcul d'ordre

8.1 Naïf

Une première manière de déterminer l'ordre d'une courbe $E(\mathbb{F}_q)$ est de procéder naïvement. il suffit de savoir si x^3+ax+b est un résidu quadratique modulo q. On n'oublie pas de compter le point à l'infini : $E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3+ax+b}{q}\right)\right)$. Le calcul du symbole de Legendre s'exécute en $O(log^4(q))$. La complexité de cet algorithme est donc en $O(q\log^4(q))$. Les autres manières de calculer l'ordre de la courbe tirent profit du théorème de Hasse que nous avons présenté précédemment. Une adaptation fine de Baby step Giant step permet de réduire la complexité à $O(q^{1/4})$ par exemple.

8.2 Baby Step Giant Step

On peut se donner un meilleur algorithme pour trouver l'ordre de la courbe. On trouve l'ordre de différents sous-groupes (ce qui est réalisé plus efficacement grâce à Baby Step Giant Step) puis on en déduit l'ordre de la courbe grâce au théorème de Hasse et au théorème de Lagrange.

1. On choisit un point P de la courbe $E(\mathbb{F}_q)$ au hasard.
2. Il s'agit de trouver k tel que $kP = \mathcal{O}$. Dés lors on pourra s'intéresser à la factorisation de k et en déduire l'ordre n de $\langle P \rangle$. Posons $N = |E(\mathbb{F}_q)|$. D'après le théorème de Lagrange, $n|N$ donc $NP = \mathcal{O}$. De plus, d'après le théorème de Hasse : $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. Ainsi il y a forcément au moins un entier k compris entre $q+1-2\sqrt{q}$ et $q+1+2\sqrt{q}$ tel que $kP = \mathcal{O}$. C'est pour trouver ce k que l'on met en place Baby Step Giant Step, qui nous permet de passer d'une complexité en $O(\sqrt{q})$ (tester naïvement chaque valeur) à une complexité en $O(q^{1/4})$. Pour se faire :
   (a) On pose $Q = (q+1)P$.
   (b) On pose $m = \lceil q^{1/4} \rceil$. On calcul et on stocke $\{jP\}_{0 \leq j \leq m}$ (Baby Steps).
   (c) On calcule successivement $Q - i(2mP)$, $-m \leq i \leq m$ jusqu'à collision pour un certain i_0 avec un des éléments $j_0 P$ de $\{jP\}_{0 \leq j \leq m}$ (Giant Steps).
   (d) On pose $k = q+1+2mi_0 - j_0$ donc tel que $kP = \mathcal{O}$
3. On factorise $k = p_1^{\alpha_1} ... p_n^{\alpha_2}$ et on trouve l'ordre p_i de P, i.e l'unique premier et le plus petit entier, ce que l'on prouve facilement, tel que $p_i P = \mathcal{O}$.
4. Pour trouver $N = |E(\mathbb{F}_q)|$, on répète les opérations précédentes en stockant successivement $n_1, ..., n_i$ les ordres de différents sous-groupes distincts. L'algorithme s'arrête lorsque $ppcm(n_1, ..., n_i)$ divise un unique nombre $N \in [\![q+1-2\sqrt{q}\ ,\ q+1+2\sqrt{q}]\!]$: c'est forcément l'ordre de $E(\mathbb{F}_q)$.

Remarque Un résultat de Mestre sur ce qui est appelé le *twist quadratique* d'une courbe pourrait être utile dans ce cas de figure. Donnons-le après avoir défini cette transformation.

Définition 8.1. *Twist quadratique* Soit $E : y^2 = x^3 + ax + b$. Soit $d \in \mathbb{F}_q^*$. Le twist quadratique de E par d est la courbe $E' : y^2 = x^3 + ad^2x + bd^3$.

Propriétés

— Si $\#E(\mathbb{F}_q) = q+1-a$, alors $\#E(\mathbb{F}_q) = q+1-\left(\frac{d}{q}\right)a$.

— Pour $p \in \mathbb{P}, p > 229$, soit E soit E' possède un point d'ordre strictement supérieur à $4\sqrt{q}$, ce qui détermine complétement l'ordre de E et de E'.

8.3 L'algorithme de Schoof

Enfin, nous allons parler de l'algorithme de Schoof. Publié en 1985 par René Schoof, il a constitué une avancée théorique majeure en étant le premier algorithme déterministe en temps polynomial permettant de trouver l'ordre d'une courbe elliptique.

On a besoin de quelques résultats préliminaires.

Théorème 8.1. Soit $E : x^2 = y^3 + Ax + B$. Alors, en se plaçant sur $\overline{\mathbb{F}_q}$: $\phi_q^2 - a\phi_q + q = 0$ avec $a = tr(\phi_q)$ et $q = \det(\phi_q)$. L'entier a est unique et est tel que $\#E(\mathbb{F}_q) = q + 1 - a$.

Démonstration. Pour $\alpha \neq 0 \in \mathrm{End}(E)$, $\deg(\alpha) \geq \#ker(\alpha)$ donc $ker(\alpha)$ est fini. Il suffit donc de montrer que $ker(\phi_q^2 - a\phi_q + q)$ est infini. Soit $m \geq 1$ un entier tel que $m \wedge q = 1$. Rappelons que ϕ_q induit sur $E[m]$ une matrice $(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$. Comme $\phi_q - 1$ est séparable :

$$\#ker(\phi_q - 1) = \deg(\phi_q - 1) \equiv \det((\phi_q)_m - I_2) \equiv sv - tu - (s + v) + 1[m]$$

Or $sv - tu = \det((\phi_q)_m) \equiv \deg(\phi_q) \equiv q[m]$. De plus $ker(\phi_q - 1) = E(\mathbb{F}_q) = q + 1 - a$. Donc $tr((\phi_q)_m) = s + v \equiv a[m]$ et par Cayley-Hamilton on obtient le résultat désiré modulo m. Comme cela tient pour tout m vérifiant $m \wedge q = 1$, $ker(\phi_q^2 - a\phi_q + q)$ est infini ce qui conclut.

Montrons que a est unique. Soit a' un entier tel que la relation est vérifiée avec a'. Alors $(a' - a)\phi_q = \phi_q^2 - a\phi_q + q + \phi_q^2 - a'\phi_q + q = 0$. Mais rappelons que les endomorphismes de courbe elliptique sont surjectifs et en particulier pour tout entier m tel que $E[m] \neq \{\mathcal{O}\}$ on peut prendre $P \neq \mathcal{O} \in \phi_q^{-1}(E[m])$ et dès lors $(a' - a)P = 0$ et $m|(a' - a)$ car il y a des points d'ordre m lorsque $m \wedge q = 1$ ($E[m] \cong (\mathbb{Z}_{/n\mathbb{Z}})^2$). □

On considère une courbe $E(\mathbb{F}_q)$ où $q = p^n$, p premier impair. Le théorème de Hasse nous assure que $|E(\mathbb{F}_q)| = q + 1 - a$ où $|a| \leq 2\sqrt{q}$. L'idée est alors de calculer a mod N avec $N > 4\sqrt{q}$; il est possible de calculer a mod l avec l un petit nombre premier plutôt efficacement. On peut alors ensuite tirer parti du théorème des restes chinois.

Une approche un peu naïve serait de tenter de calculer formellement les points (x^{q^2}, y^{q^2}), $q(x, y)$ et (x^q, y^q), c'est-à-dire en considérant x et y comme des fonctions dans l'anneau des coordonnées $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$ (en effet les coordonnées vérifient l'équation de Weierstrass réduite donc $y^2 = x^3 + Ax + B$). Cependant, les degrés de ces polynômes deviennent vite très grand, ce qui fait que cette approche est peu pratique.

L'idée de Schoof est donc de ramener ce calcul aux points d'ordre l pour différents petits premiers l. Cela va nous permettre de limiter le nombre total d'opérations (en particulier les additions de point si coûteux dans $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$).

On fait appel à l'endomorphisme de Froebenius et aux polynômes de division. Donnons-nous $l \neq 2, p$ premier. Si $P = (x, y) \in E[l]$, alors :

— $qP = \overline{q}P$ où $q \equiv \overline{q}[l]$. De même, $a(x^q, y^q) = \overline{a}(x^q, y^q)$ où $a \equiv \overline{a}[l]$.

— $\psi_l(x) = 0$ car $m_l(P) = \mathcal{O}$. La réciproque est vraie.

Ainsi, pour $l \in S$, $l \neq p$, il suffit de trouver $\overline{a} \in [\![-\frac{l-1}{2}, \frac{l-1}{2}]\!]$ tel que $(X^{q^2}, Y^{q^2}) + \overline{q}(X, Y) = \overline{a}(X^q, Y^q)$ dans $\mathbb{F}_q[X, Y]_{/(Y^2 - X^3 - aX - b, \psi_l)}$. Les égalités sont vérifiées mod ψ_l car on travaille sur les points de l-torsion. Dès lors $a \equiv \overline{a}$ mod l. Remarque importante si l'on veut implémenter l'algorithme : il est évidemment peu pratique et coûteux d'effectuer les calculs dans $\mathbb{F}_q[X, Y]$. Il est cependant possible de faire tourner l'algorithme seulement avec des polynômes dans $\mathbb{F}_q[X]$ en s'intéressant à l mod 4 pour les ψ_l.

Bref, décrivons désormais comment on détermine a mod l. On se place donc dans $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B, \psi_l)$, où l'on rappelle que ψ_l est le l-ème polynôme de division. On sépare le problème en deux cas, selon que $(x^{q^2}, y^{q^2}) = \pm q(x, y)$ ou $(x^{q^2}, y^{q^2}) \neq \pm q(x, y)$ (car on utilisera deux formules d'addition différentes). Ajoutons que ces égalités sont donc vérifiées mod ψ_l car pour $P = (x, y) \in E(\overline{\mathbb{K}}), \psi_l(x) = 0 \iff P \in E[l]$.

1. **Cas** $(x^{q^2}, y^{q^2}) \neq \pm q(x, y)$
   Posons $(x', y') = (x^{q^2}, y^{q^2}) + q(x, y) = \pm a(x^q, y^q) = \bar{t}(x^q, y^q) \neq \mathcal{O}$. Déjà, comme $a(x^q, y^q) \neq \mathcal{O}$, on sait que $a \not\equiv 0$ mod l. Les deux points étant distincts, on utilise la formule d'addition par rapport à la coordonnées en x. En notant $q(x, y) = \overline{q}(x, y) = (x_{\overline{q}}, y_{\overline{q}})$ on peut écrire : $x' =$

$\left(\frac{y^{q^2}-y_{\overline{q}}}{x^{q^2}-x_{\overline{q}}}\right)^2 - x^{q^2} - x_{\overline{q}}$. On se rappelle que x' est en fait une fonction rationnelle de x.

Maintenant, si $x' = x_{\overline{t}}^q \bmod \psi_l$ pour un certain $\overline{t} \in [\![0\ ,\ \frac{l-1}{2}]\!]$, alors $(x', y') = (x_{\overline{t}}^q, \pm y_{\overline{t}}^q) = \pm\overline{t}(x^q, y^q)$ et donc $\overline{t}$ satisfait $\phi_q^2(P) \mp \overline{t}\phi_q(P) + \overline{q}P = \mathcal{O}$ pour tout $P \in E[l]$. Enfin, pour déterminer le signe de a, il faut s'intéresser au signe de $y_{\overline{t}}^q$. Comme y'/y et $y_{\overline{t}}^q/y$ peuvent être écrites comme des fonctions de x, on peut affirmer que $\frac{y'-y_{\overline{t}}^q}{y} \equiv 0[\psi_l(x)] \Leftrightarrow a \equiv \overline{t}[l]$ car alors $y' = y_{\overline{t}}^q$ sur tout $E[l]$. Sinon forcément $a \equiv -\overline{t}[l]$.

2. **Cas** $(x^{q^2}, y^{q^2}) = \pm q(x, y)$
   (a) **Si** $(x^{q^2}, y^{q^2}) = +q(x, y)$
   Alors, pour tout $P \in E[l]$: $a\phi_q(P) = \phi_q^2(P) + qP = 2qP$, d'où $a^2\phi_q^2(P) = (2q)^2P = a^2qP$. Donc $a^2q \equiv 4q^2[l]$. On en déduit que q est un carré mod l, notons ω une de ses deux racines carrées. Comme $\phi_q^2(P) = qP = \omega^2P$, on a $\Leftrightarrow (\phi_q - \omega)(\phi_q + \omega) = \mathcal{O}$. Si $\phi_q(P) = \omega P$, alors $\mathcal{O} = (\phi_q^2 - a\phi_q + q)(P) = (q - a\omega + q)P$ donc $a \equiv 2\omega[l]$. Sinon forcément $a \equiv -2\omega[l]$.

   (b) **Si** $(x^{q^2}, y^{q^2}) = -q(x, y)$
   Dans ce cas, pour tout $P \in E[l]$, $a\phi_q(P) = \phi_q^2(P) + qP = qP - qP = \mathcal{O}$ et évidemment $a \equiv 0[l]$.

Dans le cas où $l = 2$. Il suffit de savoir si $(x^q - x) \wedge (x^3 + Ax + b) = 1$, auquel cas les deux polynômes n'ont pas de racine commune et donc $a \equiv 1[2]$. Sinon $a \equiv 0[2]$.

Complexité On a $v(n) = \sum_{p\in\mathbb{P}, p\leq n} \ln(p) = \ln(\prod_{p\in\mathbb{P}, p\leq n} p) \approx n$ (fonction de Chebyshev). Or $\prod_{l\in S} l \approx 4\sqrt{q}$ donc $l = O(\log(q))$. Le produit de deux entiers mod q se fait en $O(\log(q)\log(\log(q)))$. Mais $\deg(\psi_l) = O(l^2)$. La complexité du calcul de ψ_l est donc : $O(l^2\log(l)\log(q)\log(\log(q)) = O(\log(q)^{3+\varepsilon})$. Enfin la suite de l'algorithme de Schoof nécessite le calcul de x^q, x^{q^2}... : cela demande $O(\log(q))$ opérations (exponentiation rapide), et ce pour chaque $l \in S$. On est en $O(\log(q)^{5+\varepsilon})$, ou en $O(\log(q)^8)$ sans optimisations arithmétiques.

$$\begin{cases} \psi_{4n} &= \frac{1}{2}\psi_{2n}(\psi_{2n+2}\psi_{2n-1}^2 - \psi_{2n-2}\psi_{2n+1}^2) \\ \psi_{4n+1} &= (X^3 + aX + b)^2\psi_{2n+2}\psi_{2n}^3 - \psi_{2n+1}\psi_{2n-1} \\ \psi_{4n+2} &= \frac{1}{2}\psi_{2n+1}(\psi_{2n+3}\psi_{2n}^2 - \psi_{2n-1}\psi_{2n+2}^2) \\ \psi_{4n+3} &= \psi_{2n+3}\psi_{2n+1}^3 - (X^3 + aX + b)^2\psi_{2n+2}\psi_{2n} \end{cases}$$

Elkies et Atkins améliorent cet algorithme dans la fin des années 90, en identifiant une classe particulière de premiers permettant de manipuler des polynômes de degré $O(l)$ et atteignant une complexité en $\Theta(\log(q)^4)$.

Troisième partie

Exemples d'Utilisation

9 ECDSA (Elliptic Curve Digital Signature Algorithm)

On se donne une courbe $E(\mathbb{F}_q) : y^2 =^3 +ax + b$ et un point générateur G. On va travailler sur $\langle G \rangle$, on note n son ordre.
Le scénario est le suivant : Alice veut signer un message avec sa clé privée k_A et Bob souhaite valider la signature adjointe au message. Personne excepté Alice ne devrait pouvoir produire de signature valide. Tout le monde devrait pouvoir vérifier une signature. Tout le monde connaît donc les paramètres de la courbe elliptique ainsi que le point générateur sur lesquelles on travaille. Décrivons cette algorithme :

— **Signature**

1. Choisir de manière aléatoire un nombre k entre 1 et $q-1$. C'est une étape à ne pas négliger, car utiliser le même k pour deux signatures différentes permet de déterminer la clé privée ; cela a été à l'origine d'un hack de la PS3 forçant ce dernier à lire du contenu non validé par Sony.
2. Calculer $(i, j) = kG$, puis $x = i \bmod q$. Si $x = 0$, retourner à la première étape.
3. Calculer $y = k^{-1}(h(m) + k_A x) \bmod q$ où h est une fonction de hachage et m le message à signer. Si $y = 0$, retourner à la première étape. Sinon, on a obtenu notre signature qui est le point $Q = (x, y)$.

— **Vérification**

1. Vérifier que $Q = (x, y) \neq \mathcal{O}$, que Q appartient à la courbe sur laquelle on travaille (i.e $y^2 = x^3 + ax + b$) et que $nQ = \mathcal{O}$.
2. Vérifier que $x, y \in [\![1\ ,\ n-1]\!]$
3. Calculer $(i, j) = (h(m)y^{-1})G + (xy^{-1})Q$ et vérifier que $x = i \bmod n$. En effet : $(h(m)y^{-1})G + (xy^{-1})Q = (h(m)y^{-1} + k_A xy^{-1})G = (h(m) + k_A x)k(h(m) + k_A x)^{-1}G = kG = (i, j)$.

Puisque les meilleurs algorithmes connus pour résoudre le problème du logarithme discret sont en $O(\sqrt{n})$ (Baby Step Giant Step, l'algorithme rho de Pollard), la taille du corps sur lequel on travaille doit donc être deux fois plus grande (en terme de bits) que le paramètre de sécurité voulu. Ainsi pour un niveau de sécurité de 128-bits, on prendra une courbe définie sur un corps fini $\mathbb{F}_q$ de taille $q \approx 2^{256}$ puisqu'il s'agira approximativement de l'ordre de la courbe d'après le théorème de Hasse. On fera toujours attention à ce que le cofacteur du point générateur ne soit pas trop grand, et dans la pratique, l'ordre de la courbe étant très souvent premier on aura $h = 1$, ce qui nous dispense d'en évaluer l'impact sur la sécurité.

10 ECDH (Elliptic Curve Diffie-Hellman)

Cet algorithme permet à deux utilisateurs Alice et Bob de générer en sécurité une clé partagée à travers un réseau non sécurisé qu'une troisième personne est susceptible de surveiller. Avant d'engager la communication, tout le monde se met d'accord sur les paramètres publics (q, a, b, G, n, h) où (q, a, b) définissent la courbe $E(\mathbb{F}_q) : y^2 = x^3 + ax + b$, G le point générateur sur lequel on travaille, n son cardinal et h son cofacteur (l'ordre de la courbe est donc nh). Ensuite :

1. Alice et Bob choisissent deux clés privées k_A et k_B aléatoirement dans l'intervalle $[\![1, n-1]\!]$ qu'eux seuls connaissent, puis calculent leurs clés publiques $K_A = k_A G$ et $K_B = k_B G$. Ils sont donc en possession d'un couple de clés privée/public (k_A, K_A) et (k_B, K_B).
2. Alice et Bob s'échangent leurs clés publics K_A et K_B sur le réseau non sécurisé, et peuvent chacun de leur côté calculer la même clé partagée P : $P_A = k_A K_B = k_A k_B G$ du côté d'Alice et $P = k_B K_A = k_B k_A G = P_B$ du côté de Bob. Effectivement, $P_A = P_B = P$. Un individu relevant les informations échangées sur le réseau ne connaîtra que $K_A = k_A G$ et $K_B = k_B G$; pour retrouver $P = k_A k_B G$ il n'a d'autres choix que de s'attaquer au problème du logarithme discret.

$$
\begin{aligned}
\mathbb{P}\left(X_n = i \text{ et } X_{n+k} = j\right) &= \sum_{\ell \in E} \mathbb{P}\left(X_n = i,\, X_{n+k-1} = \ell \text{ et } X_{n+k} = j\right) \\
&= \sum_{\ell \in E} \mathbb{P}\left(X_n = i,\, X_{n+k-1} = \ell\right)\ \mathbb{P}\left(X_{n+k} = j \mid X_n = i,\, X_{n+k-1} = \ell\right) \\
&= \sum_{\ell \in E} \mathbb{P}\left(X_n = i,\, X_{n+k-1} = \ell\right)\ p_{\ell,j} \\
&= \mathbb{P}\left(X_n = i\right)\ \sum_{\ell \in E} p_{i,\ell}^{(k-1)}\ p_{\ell,j} \\
&= \mathbb{P}\left(X_n = i\right)\ p_{i,j}^{(k)},
\end{aligned}
$$

Références

[1] H.W Lenstra, *Factoring integers with elliptic curves*. Annals of Mathematics, 1986.

[2] Edwars Curve, Wikipedia, Courbes ellpitiques ayant des propriétés particulières

[3] Pollard, Wikipedia, Algorithme p - 1 ; Algorithme rho

[4] aby steps, giant steps

[5] éomètrie Projective, Wikipedia

[6] ttps ://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2

https ://www.certicom.com/content/certicom/en/ecc-tutorial.html

http ://alexis.bonnecaze.perso.luminy.univ-amu.fr/CryptoAvancee.pdf

http ://www.ai.univ-paris8.fr/ elmrabet/These.pdf

$https : //fr.wikipedia.org/wiki/Ellipticcurve_digital_signature_algorithm$

https ://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2

H.W Lenstra,Factoring integers with elliptic curves, Annals of Mathematics, 1986.