Cryptographie sur les courbes elliptiques

—

TIPE

Paul Chaudagne

Jeudi 04 décembre 2025

Table des matières

I - Les courbes elliptiques

1) Définition des courbes elliptiques

Lemme 1

La relation $\sim$, définie sur $\mathbb{K}^n \setminus \{(0, \dots, 0)\}$ par :

$$\forall((a_1, \dots, a_n), (a'_1, \dots, a'_n)) \in (\mathbb{K}^n \setminus \{(0, \dots, 0)\})^2,$$
$$(a_1, \dots, a_n) \sim (a'_1, \dots, a'_n) \iff (\exists \lambda \in \mathbb{K} \setminus \{0\}, (a_1, \dots, a_n) = \lambda(a'_1, \dots, a'_n))$$

est une relation d'équivalence.

Preuve :

Par définition d'un corps, on a :
- $1 \in \mathbb{K}$ donc $\sim$ est réflexive
- Pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, $\lambda^{-1} \in \mathbb{K}$ donc $\sim$ est symétrique
- Pour tous $\lambda, \mu \in \mathbb{K} \setminus \{0\}$, $\lambda\mu \in \mathbb{K}$ donc $\sim$ est transitive.

Définition 2 - Espace projectif

Soit $\mathbb{K}$ un corps, on appelle **espace projectif de dimension n** l'ensemble des classes d'équivalence pour la relation $\sim$, noté :

$$\mathbb{P}^n(\mathbb{K}) = (\mathbb{K}^{n+1} \setminus \{(0, \dots, 0)\}) / \sim$$

Pour $P = (x_1, \dots, x_{n+1}) \in \mathbb{K} \setminus \{(0, \dots, 0)\}$, on notera $[x_1 : \dots : x_{n+1}]$ la **classe d'équivalence** de P pour la relation $\sim$.

On appellera en particulier **plan projectif** l'espace projectif de dimension 2.

Cela revient à projeter l'espace sur une demi-sphère centrée en (0, 0, 0), où chaque classe d'équivalence correspond à une droite passant par l'origine et un unique point de la demi-sphère, soit en dimension 1 :

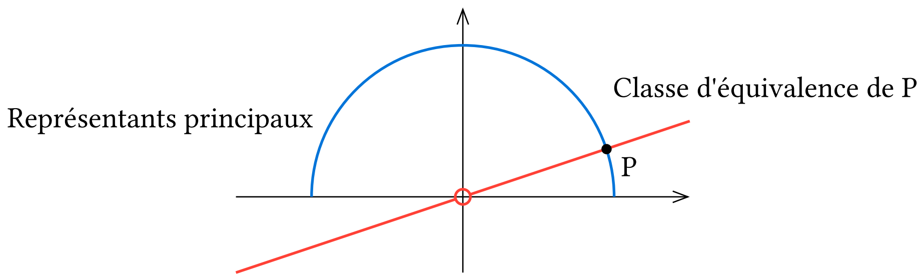

Fig. 1. – Représentation de l'espace projectif de dimension 1.

Définition 3 - Polynôme homogène

Un **polynôme homogène** est un polynôme en plusieurs indéterminées dont tous les monômes non nuls sont de même degré total.

Par exemple, un polynôme de degré 3 homogène en trois variables s'écrit sous la forme :

$$P(X, Y, Z) = aX^3 + bY^3 + cZ^3 + dX^2Y + eX^2Z + fY^2X + gY^2Z + hZ^2X + iZ^2Y + jXYZ$$

On remarque en particulier que si P est un polynôme homogène en trois variables de degré d, et que $P(x, y, z) = 0$, alors :

$$\forall (x', y', z') \in [x : y : z], P(x', y', z') = \lambda^d P(x, y, z) = 0$$

Dans le plan projectif, l'annulation d'un polynôme homogène ne dépend donc pas du représentant choisi.

Définition 4 - Courbe elliptique

On appelle **courbe elliptique sur un corps** $\mathbb{K}$, l'ensemble des solutions dans le plan projectif $\mathbb{P}^2(\mathbb{K})$ de l'équation $F(X,Y,Z)=0$, où F est un polynôme homogène de degré 3 en trois variables à coefficients dans $\mathbb{K}$.

Formellement, pour F polynôme homogène de $\mathbb{K}_3[X,Y,Z]$, on note :

$$E(\mathbb{K}) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{K}), F(x,y,z)=0\}$$

En l'absence d'ambiguïté sur le corps, on notera indistinctement $E(\mathbb{K})$ et E les courbes elliptiques considérées.

On notera que multiplier le polynôme par un scalaire non nul ne change pas la courbe elliptique considérée.

Définition 5 - Singularité

Un point $P=[x:y:z]$ d'une courbe elliptique est dit **singulier** lorsque :

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) = (0,0,0)$$

On dira d'une courbe elliptique qu'elle est **lisse** (ou **non singulière**) si elle ne possède aucun point singulier, soit :

$$\forall P \in E(\mathbb{K}), \left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) = (0,0,0)$$

Par la suite, nous ne considérerons que des courbes elliptiques non singulières définies sur un corps $\mathbb{K}$ de caractéristique différente de 2 ou 3.

Définition 6 - Tangente

Soit E une courbe elliptique, et $P \in E$ un point non singulier. Alors la **tangente à E en P** est donnée par :

$$\frac{\partial F}{\partial X}(P)(X-X_P) + \frac{\partial F}{\partial Y}(P)(Y-Y_P) + \frac{\partial F}{\partial Z}(P)(Z-Z_P) = 0$$

Définition 7 - Point d'inflexion

Soit E une courbe elliptique, on dit qu'un point $P \in E$ est un **point d'inflexion** si la tangente à E en P intersecte E en P avec une multiplicité égale à 3.

2) Forme de Weierstrass

Proposition 8

Soit E une courbe elliptique non singulière sur $\mathbb{K}$. Soit P un point d'inflexion de E.

Alors un changement de variables linéaire inversible permet de transformer P en $[0:1:0]$ et la tangente en P en $Z=0$.

Preuve :

Soit L la tangente à E en $P = [x_P : y_P : z_P]$. Soit $Q = [x_Q : y_Q : z_Q] \in L \setminus E$, les vecteurs (x_P, y_P, z_P) et $x_Q, y_Q, z_Q)$ sont linéairement indépendants car P et Q correspondent à deux points distincts du plan projectif.

On complète avec un vecteur C en une base de $\mathbb{K}^3$. On obtient alors :

$$M = \begin{pmatrix} x_Q & x_P & \\ y_Q & y_P & C \\ z_Q & z_P & \end{pmatrix}$$

M est inversible. M^{-1} envoie P sur le point $[0 : 1 : 0]$ et Q sur le point $[1 : 0 : 0]$. Donc M^{-1} envoie L sur $Z = 0$ car c'est l'unique droite passant par P et Q.

Théorème 9 - Mise sous forme de Weierstrass

Soit E une courbe elliptique non singulière. Soit $\mathcal{O}$ un point d'inflexion de E, si $\mathcal{O} = [0 : 1 : 0]$ et si la tangente à E en $\mathcal{O}$ est $Z = 0$, alors E est de la forme:

$$Y^2Z + a_1YXZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

Preuve :

La forme générale du polynôme qui définit une courbe elliptique est :

$$F(X, Y, Z) = aX^3 + bY^3 + cZ^3 + dX^2Y + eX^2Z + fY^2X + gY^2Z + hZ^2X + iZ^2Y + jXYZ$$

Montrons que certains termes s'annulent :

- F([0 : 1 : 0]) = 0 donc $b = 0$.
- La tangente à E en $[0 : 1 : 0]$ est $Z = 0$, donc $\frac{\partial F}{\partial X}([0 : 1 : 0]) = f = 0$ et $\frac{\partial F}{\partial Z}([0 : 1 : 0]) = g \neq 0$
- L'intersection de la tangente $Z = 0$ en $\mathcal{O}$ avec la courbe est donnée par l'équation $aX^3 + dX^2Y = 0$, pour avoir ensuite $\mathcal{O}$ point d'inflexion, il faut que ce point soit racine triple de $F(X : 1 : 0) = aX^3 + dX^2$, soit $d = 0$.
- Supposons $a = 0$, on se place alors dans le plan $Z = 0$. Donc :

$$\frac{\partial F}{\partial X} = 0 \qquad \frac{\partial F}{\partial Y} = 0 \qquad \frac{\partial F}{\partial Z} = eX^2 + jXY + gY^2$$

  En l'absence de conditions sur X, Y, ce polynôme s'annule dans la clôture algébrique $\mathbb{L}$ de $\mathbb{K}$, or $E(\mathbb{L})$ reste une courbe elliptique, donc $E(\mathbb{L})$ est singulière, d'où $a \neq 0$.

On choisit alors un représentant de F ayant un coefficient 1 devant X^3 (possible car $a \neq 0$). Ainsi, $F(X, Y, Z) = X^3 + \alpha Z^3 + \beta X^2Z + \gamma Y^2Z + \delta Z^2X + \varepsilon Z^2Y + \zeta XYZ; \gamma \neq 0$.

On pose ensuite le changement de variables $Z' = -\frac{Z}{\gamma}$, on obtient F sous forme de Weierstrass.

3) Forme de Weierstrass réduite

Théorème 10 - Mise sous forme réduite de Weierstrass

Si $\mathrm{Car}(K) \neq 2, 3$, on peut mettre une courbe elliptique sous forme de Weierstrass réduite :

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1}$$

Preuve :

Soit E une courbe elliptique sous forme de Weierstrass, on pose d'abord, pour annuler le terme en XYZ :

$$X' = X, Y' = Y + \frac{a_1}{2}X, Z' = Z$$

Puis pour éliminer les termes en X^2 et Y :

$$X' = X + \frac{a_2}{3}, Y' = Y + \frac{a_3}{2}, Z' = Z$$

On arrive alors à la forme souhaitée, on note que ces changements de variables sont possibles grâce à l'hypothèse sur la caractéristique.

Le refaire à la main au moins une fois

Corollaire 11 - Forme réduite affine

En coordonnées non homogènes ($x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$), on peut écrire cette équation :

$$E : y^2 = x^3 + ax + b \tag{2}$$

Ainsi que le point $\mathcal{O} = [0 : 1 : 0]$ qui est le seul point à l'infini.

Proposition 12 - Critère de singularité

Soit E une équation sous forme de Weierstrass, alors E est singulière si et seulement si la quantité $\Delta := 4a^3 + 27b^2$ est nulle.

Preuve :

E est une courbe de $\mathbb{P}^2(\mathbb{K})$ donnée par l'équation :

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$$

D'abord, $\dfrac{\partial F}{\partial Z}(\mathcal{O}) = 1 \neq 0$.

Passons maintenant en coordonnées affines :

$$E : f(x, y) = y^2 - x^3 - ax - b = 0$$

Si $P = (x_0, y_0)$ est un point singulier, alors $\dfrac{\partial f}{\partial y}(P) = 2y_0 = 0$, donc $y_0 = 0$ comme $\mathrm{Car}(K) \neq 2$.

$\dfrac{\partial f}{\partial x}(P) = 3x_0^2 - a = 0$, donc $x_0^2 = -\dfrac{a}{3}$. D'où $y_0^2 = 0 = x_0^3 + ax_0 + b = \dfrac{2}{3}ax_0 + b$.

On en déduit $x_0^2 = \dfrac{9b^2}{4a^2} = -\dfrac{a}{3}$. D'où $\Delta := 4a^3 + 27b^2 = 0$.

4) Structure de groupe abélien

a. Prémices

Proposition 13 - intersections avec une droite

Soient E une courbe elliptique et L une droite définies sur un corps $\mathbb{K}$.

Si E a au moins deux points d'intersection (comptés avec multiplicité) avec la droite L, alors E a exactement trois points d'intersection (comptés avec leur multiplicité) avec la droite L

Preuve :

> On prend E sous forme de Weierstrass, $E : F(X, Y, Z) = Y^2 Z - X^3 - aXZ^2 - bZ^3 = 0$. L est satisfait l'équation $\alpha X + \beta Y + \gamma Z = 0$. Sans perte de généralité, on peut supposer que $\alpha \neq 0$ et que l'équation est alors $X = -\beta' Y - \gamma' Z$. Le polynôme $P(Y, Z) = F(-\beta' Y - \gamma' Z, Y, Z)$ est un polynôme admettant

Racine réelle ? Et si verticale ? Preuve mat562 avec 4 racines ou + => nul ?

b. Approche géométrique

c. Approche analytique