TD 3

Le modèle de Weierstrass d'une courbe elliptique E est une équation

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

où les coefficients $(a_i)_{i\in\{1,\cdots,4,6\}}$ sont des éléments d'un corps $\mathbb{K}$. En abrégé, $E = [a_1, a_2, a_3, a_4, a_6]$.

On peut cependant utiliser un autre système de coordonnées, les coordonnées d'Edwards, basé sur un modèle du type

$$x^2 + y^2 = c^2(1 + dx^2y^2).$$

où on impose $cd(1 - dc^4) \neq 0$. Il n'y a plus que deux paramètres, donc ici $E = [c, d]$.

La loi d'addition est alors donnée par

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}\right).$$

On remarque que les formules d'addition fournissent directement la formule de duplication, contrairement au cas du modèle de Weierstrass où on utilise la loi corde-tangente. Par contre le modèle d'Edwards est singulier, pour être complètement rigoureux il faut donc résoudre les singularités pour obtenir une courbe elliptique. On peut cependant utiliser ces coordonnées pour gagner un peu de temps dans les calculs explicites.

Le neutre pour l'addition est le point $(0, c)$. (À vérifier !)

L'opposé d'un point (x_1, y_1) est $-(x_1, y_1) = (-x_1, y_1)$. (À vérifier !)

Exercice 1.

1. Écrire une fonction $Edwardsinit(c, d)$ qui crée un modèle d'Edwards de paramètres c et d.
2. Étant donné une courbe elliptique E et deux points P et Q de E, écrire une fonction $Edwardsadd(E, P, Q)$ qui calcule $P + Q$ sur le modèle d'Edwards E en utilisant la nouvelle loi d'addition.
3. Sur un modèle $E = [c, d]$, calculer l'ordre des points $(0, -c)$, $(c, 0)$ et $(-c, 0)$.

Exercice 2. On va étudier un exemple de passage d'une forme de Weierstrass à une forme d'Edwards. Tout repose sur la remarque suivante : génériquement, une équation du type $x^2 + y^2 = 1 + dx^2y^2$ est birationnellement équivalente à une équation du type

$$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u.$$

Il suffit d'utiliser le changement de coordonnées $(u, v) \mapsto (x, y)$ avec $x = 2u/v$ et $y = (u - 1)/(u + 1)$.

1. On consière la courbe d'équation $E_1 : t^2 = s^3 + 3s^2 - s$. Montrer qu'elle est équivalente à la courbe $E_2 : x^2 + y^2 = 1 + 5x^2y^2$.
2. Écrire une fonction qui transforme les points de E_1 en des points de E_2.
3. Comparer sur de nombreux exemples de corps finis (si possible en grande caractéristique et en petite caractéristique) la vitesse de calcul d'additions et d'itérations de points sur E_1 et sur E_2.