TP4 - Courbes anomales

L'objectif de cette feuille de TP est d'implémenter un algorithme qui prend en arguments deux points affines P et Q sur une courbe elliptique anomale E sur $\mathbb{F}_p$ et renvoie l'unique entier $m \leq p-1$ tel que $Q = mP$. Le TD5 nous permet de déterminer un tel algorithme qui n'est malheureusement pas efficace. Dans la dernière partie nous proposons de faire les calculs dans $\mathbb{Q}$ seulement modulo p^2 pour accélérer les calculs. Nous reprendrons les mêmes notations que dans le TD5.

On admet que pour E une courbe elliptique sur $\mathbb{F}_p$ on a un morphisme de groupes

$$\begin{array}{rccl} \pi\colon & \widetilde{E}(\mathbb{Q}) & \longrightarrow & E(\mathbb{F}_p) \\ & (x,y) \in \widetilde{E}_1 & \longmapsto & \infty \\ & (x,y) \notin \widetilde{E}_1 & \longmapsto & (x,y) \mod p \end{array}$$

tel que $\ker \pi = \widetilde{E}_1$.

Exercice 1 (Exemples).

1. On considère la courbe $E_0\colon y^2 = x^3 + 7x + 63$ sur $\mathbb{F}_{191}$.
   (a) Vérifier que les points $P = (55, 56)$ et $Q = (56, 55)$ sont des points de E_0.
   (b) Que vaut $191P$? En déduire que E_0 est une courbe anomale.
2. On considère la courbe $E_1\colon y^2 = x^3 + 108x + 4$ sur $\mathbb{F}_{853}$. En considérant les points $P = (0, 2)$ et $Q = (563, 755)$ montrer que E_1 est une courbe anomale.
3. On considère la courbe $E_2\colon y^2 = x^3 + 33999065x + 32001877$ sur $\mathbb{F}_{100000007}$. En considérant les points $P = (72780479, 44733347)$ et $Q = (92924266, 59959841)$ montrer que E_2 est une courbe anomale.

Exercice 2 (Un algorithme inefficace).

1. Déduire de la feuille de TD5 que l'algorithme 1 renvoie bien ce qu'on veut.
2. Où intervient l'hypothèse E anomale ?
3. Implémenter votre algorithme.
4. Tester votre algorithme pour les points P et Q de la courbe E_0 de l'Exercice 1.

Algorithm 1: Algorithme naïf

Data: $P, Q \in E$ avec E anomale sur $\mathbb{F}_p$.
Result: L'entier m tel que $Q = mP$.
Calculer $\widetilde{P}, \widetilde{Q}, \widetilde{E}$ des relevés sur $\mathbb{Z}$ de P, Q et E.;
Calculer $\widetilde{P}_1 = p\widetilde{P}$ et $\widetilde{Q}_1 = p\widetilde{Q}$ dans $\widetilde{E}_1$ (en reprenant les notations de la feuille de TD5).;
if $\widetilde{P}_1 \in \widetilde{E}_2$ **then**
    Choisir d'autres $\widetilde{P}, \widetilde{Q}$ et $\widetilde{E}$ et refaire les calculs précédents.;
    else
        Calculer $\ell_1 = \gamma(\widetilde{P}_1)$ et $\ell_2 = \gamma(\widetilde{P}_2)$.;
        Renvoyer $m = \ell_2/\ell_1 \mod p$.;
    end
end

Exercice 3 (Un algorithme efficace). Le problème avec l'Algorithme 1 est le calcul de $p\widetilde{P}$ et $p\widetilde{Q}$ qui sont des calculs très coûteux sur $\widetilde{E}$. L'idée est donc de faire les calculs modulo p^2. Le problème étant que $\widetilde{P}_1 = \infty \mod p^2$, on va donc calculer $(p-1)\widetilde{P} \mod p^2$ puis ajouter $\widetilde{P}$ en faisant attention à la valuation p-adique des dénominateurs. On obtient l'Algorithme 2.

Algorithm 2: Algorithme efficace

Data: $P, Q \in E$ avec E anomale sur $\mathbb{F}_p$.
Result: L'entier m tel que $Q = mP$.
Calculer $\widetilde{P} = (x_1, y_1), \widetilde{Q} = (x_2, y_2), \widetilde{E}$ des relevés sur $\mathbb{Z}$ de P, Q et E.;
Calculer $(x', y') = (p-1)\widetilde{P} \mod p^2$ et $(x'', y'') = (p-1)\widetilde{Q} \mod p^2$;
Calculer $m_1 = p\frac{y'-y_1}{x'-x_1}$ et $m_2 = p\frac{y''-y_2}{x''-x_2}$.;
if $\nu_p(m_1) < 0$ *ou* $\nu_p(m_2) < 0$ **then**
    Choisir d'autres $\widetilde{P}, \widetilde{Q}$ et $\widetilde{E}$ et refaire les calculs précédents.;
    else
        Renvoyer $m = m_1/m_2 \mod p$.;
    end
end

1. Implémenter cet algorithme et comparer les temps de calculs avec l'Algorithme 1 sur la courbe E_0.
2. Déterminer les entiers m tels que $Q = mP$ pour les P, Q des courbes E_1 et E_2 de l'Exercice 1.