TD n° 4 — Méthode rho de Pollard

La méthode « rho » de Pollard est un algorithme de calcul de logarithmes discrets.

Soient E une courbe elliptique sur un corps K. Soit $P \in E(K)$ un point d'ordre fini, et soit Q un point appartenant au sous-groupe cyclique $\langle P \rangle$ engendré par P. On cherche à déterminer un entier n tel que $[n]P = Q$.

On commence par se donner une partition de $\langle P \rangle$ en trois sous-ensembles

$$\langle P \rangle = S_1 \amalg S_2 \amalg S_3$$

où les S_i sont tous les trois de taille semblable, avec $O \notin S_2$. On définit une marche aléatoire w_i sur $\langle P \rangle$ en posant $w_0 = P$ et

$$w_{i+1} = \Phi(w_i) = \begin{cases} w_i + Q & \text{si } w_i \in S_1, \\ [2]w_i & \text{si } w_i \in S_2, \\ w_i + P & \text{si } w_i \in S_3. \end{cases}$$

Il est clair que w_i peut s'écrire sous la forme

$$w_i = a_i P + b_i Q$$

où (a_i, b_i) est un couple d'entiers naturels que l'on peut calculer au fur et à mesure.

1. On suppose que $K = \mathbb{F}_p$. Imaginer une facon de partitionner $\langle P \rangle$.
2. Programmer l'application Φ correspondante qui, étant donné le vecteur $[a_i, b_i, w_i]$, renvoie le vecteur $[a_{i+1}, b_{i+1}, w_{i+1}]$. Appellez-la `PollardPhi`$(E, P, Q, W)$.
3. En supposant connu l'ordre de P, montrer que si cette marche aléatoire w_i présente une collision, alors vous êtes capable de trouver l'entier n cherché.
4. Montrer qu'il existe un entier naturel k grand satisfaisant $w_k = w_{2k}$. Sachant cela, écrire une procédure qui, étant donnés P et Q, renvoie n. Appelez-la `Pollard`(E, P, Q).
5. Tester cette procédure sur l'exemple suivant : E est la courbe elliptique définie sur $\mathbb{F}_{9000011}$ par les coefficients
$$E = [0, 0, 0, 1, 0]$$
les points P et Q sont donnés par
$$P = (2851369, 7079826) \qquad \text{et} \qquad Q = (3160451, 3437706)$$
6. Imaginer une façon de partitionner $\langle P \rangle$ dans le cas où K est un corps fini non premier.