# TD5 - Courbes anomales

L'objectif de cette feuille est de comprendre comment on peut casser le logarithme discret sur une courbe elliptique anomale sur $\mathbb{F}_p$, i.e. sur une courbe elliptique $E$ définie sur $\mathbb{F}_p$ telle que $\#E(\mathbb{F}_p) = p$.

**Exercice 1.** On considère une courbe elliptique $E\colon y^2 = x^3 + Ax + B$ sur un corps fini $\mathbb{F}_p$. Soient $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{F}_p)$ tels que $P \neq \pm Q$ et $\widetilde{x_1}, \widetilde{y_1}, \widetilde{x_2}$ trois entiers tels que

$$\widetilde{x_1} = x_1 \mod p, \widetilde{y_1} = y_1 \mod p, \widetilde{x_2} = x_2 \mod p.$$

On pose $\widetilde{P} = (\widetilde{x_1}, \widetilde{y_1})$ et on considère le système de congruences suivant

$$(S)\colon \begin{cases} y^2 = \widetilde{y_1}^2 \mod \widetilde{x_2} - \widetilde{x_1} \\ y = y_1 \mod p. \end{cases}$$

1. Montrer que le système $(S)$ admet une solution $\widetilde{y_2} \in \mathbb{Z}$. On pose $\widetilde{Q} = (\widetilde{x_2}, \widetilde{y_2})$.
2. Trouver deux entiers $\widetilde{A}, \widetilde{B}$ tels que $\left(\widetilde{A}, \widetilde{B}\right) = (A, B) \mod p$ et tels que les points $\widetilde{P}$ et $\widetilde{Q}$ sont des points de la courbe elliptique $\widetilde{E}\colon y^2 = x^3 + \widetilde{A}x + \widetilde{B}$ définie sur $\mathbb{Q}$.

**Exercice 2.** Soit $\widetilde{E}\colon y^2 = x^3 + \widetilde{A}x + \widetilde{B}$ une courbe elliptique définie sur $\mathbb{Q}$ avec $\widetilde{A}, \widetilde{B} \in \mathbb{Z}$ et $p$ un nombre premier. On pose la valuation $p$-adique sur $\mathbb{Q}$ définie par

$$\begin{array}{rccl} \nu_p\colon & \mathbb{Q} & \longrightarrow & \mathbb{Z} \cup \{-\infty\} \\ & 0 & \longmapsto & -\infty \\ & p^r \frac{a_1}{b_1}, p \nmid a_1 b_1 & \longmapsto & r. \end{array}$$

On pose pour tout $k > 0$ l'ensemble $\widetilde{E}_k$ défini par

$$\widetilde{E}_k = \left\{(x, y) \in \widetilde{E}(\mathbb{Q}), \nu_p(x) \leq -2k \text{ et } \nu_p(y) \leq -3k\right\} \cup \{\infty\}.$$

On admet qu'il s'agit d'un sous-groupe de $\widetilde{E}(\mathbb{Q})$.

1. Soit $P = (x, y) \in \widetilde{E}(\mathbb{Q})$ tel que $\nu_p(x) < 0$ ou $\nu_p(y) < 0$. Montrer qu'il existe $r \geq 1, \nu_p(x) = -2r$ tel que et $\nu_p(y) = -3r$.
2. En déduire que

$$\widetilde{E}_r \setminus \widetilde{E}_{r+1} = \left\{(x, y) \in \widetilde{E}_r, \nu_p(x) = -2r, \nu_p(y) = -3r\right\} = \left\{(x, y) \in \widetilde{E}_r, \nu_p\left(\frac{x}{y}\right) = r\right\}.$$

3. On définit l'application

$$\begin{array}{rccl} \gamma\colon & \widetilde{E}_1/\widetilde{E}_5 & \longrightarrow & \mathbb{Z}/p^4\mathbb{Z} \\ & (x, y) & \longmapsto & p^{-1}\frac{x}{y} \mod p^4. \end{array}$$

   On admet qu'il s'agit d'un morphisme de groupes.
   (a) Montrer que $\gamma$ est bien définie et qu'elle est injective.
   (b) Soit $R = [x\colon y\colon 1] \in \widetilde{E}(\mathbb{Q})$. Donner un sens à $R \mod p$ puis montrer que si $R \mod p = \infty$ alors $R \in \widetilde{E}_1$.
   (c) Montrer que pour tout $(x, y) \in \widetilde{E}_1 \setminus \widetilde{E}_2$ on a $\gamma(x, y) \neq 0 \mod p$.

On admet que pour $E$ une courbe elliptique sur $\mathbb{F}_p$ et $\widetilde{E}$ un relevé de $E$ sur $\mathbb{Q}$ 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 3.** Soit $p$ un nombre premier impair et $E\colon y^2 = x^3 + Ax + B$ une courbe elliptique anomale sur $\mathbb{F}_p$. On souhaite résoudre le logarithme discret $Q = kP$ sur $E(\mathbb{F}_p)$ avec $Q \neq P$. Soient $\widetilde{A}, \widetilde{B}, \widetilde{P}, \widetilde{Q}$ et $\widetilde{E}$ les relevés resepctifs de $A, B, P, Q$ et $E$ dans $\mathbb{Z}$ définis dans l'Exercice 1. On pose $\widetilde{P}_1 = p\widetilde{P}$ et $\widetilde{Q}_1 = p\widetilde{Q}$.

1. Montrer que $\widetilde{P}_1, \widetilde{P}_2$ et $k\widetilde{P} - \widetilde{Q}$ appartiennent à $\widetilde{E}_1$ défini dans l'Exercice 2.
2. On suppose que $\widetilde{P}_1 \notin \widetilde{E}_2$. Calculer $k\gamma(\widetilde{P}_1) - \gamma(\widetilde{Q}_1) \mod p$. En déduire la valeur de $k$.