

TD n° 3 — Courbes elliptiques (suite)

Exercice 1

Soit E la courbe elliptique sur \mathbb{Q} définie par l'équation

$$y^2 + xy = x^3 - x^2 - x + 1$$

1. Vérifier que le point $P = (0, 1)$ est un point d'ordre infini dans $E(\mathbb{Q})$. On admet que P engendre $E(\mathbb{Q})$, qui est donc isomorphe à \mathbb{Z} .
2. Pour tous les premiers p de 31 à 1000, calculer $\overline{E}_p(\mathbb{F}_p)$, et déterminer l'ordre de la réduction \overline{P} de P modulo p . Que peut-on observer ?
3. Soit F la courbe elliptique sur \mathbb{Q} définie par l'équation

$$y^2 = x^3 + 109858299531561$$

Que peut-on dire des points $P_1 = (735532, 630902573)$, $P_2 = (49704, 15252915)$, $P_3 = (-4578, 10476753)$, $P_4 = (-15260, 10310419)$ et $P_5 = (197379, 88314450)$?

4. Faire des expériences similaires à celles de la question 2 avec cette nouvelle courbe et ces cinq points.

Exercice 2

L'objectif de cet exercice est d'avoir en stock des procédures permettant de calculer l'ordre d'un point sur une courbe elliptique E sur un corps \mathbb{K} .

1. Écrire une procédure `ellpointorder(E, P, m)` qui détermine l'ordre d'un point P à partir d'un entier m tel que $[m]P = 0$ (se servir de la factorisation de m).
2. Appliquer les procédures précédentes à la courbe elliptique définie sur \mathbb{F}_{173} par

$$y^2 = x^3 + 146x + 33$$

et aux points $P = (168, 133)$ et $Q = (147, 74)$.

Exercice 3

L'objectif de cet exercice est de rechercher des points d'ordre grand sur une courbe elliptique sur un corps fini. Dans tout l'exercice, p est un premier et $q = p^n$ est une puissance de p .

1. Soit E une courbe elliptique sur \mathbb{F}_p . Écrire une fonction `GenPoint(E, n)` qui renvoie un point aléatoire $P \in E(\mathbb{F}_q)$.
2. Soit $P \in E(\mathbb{F}_q)$. Montrer que si l'ordre m de P satisfait

$$q + 1 - 2\sqrt{q} \leq m \leq q + 1 + 2\sqrt{q}$$

alors $E(\mathbb{F}_q)$ est cyclique d'ordre m , engendré par P (on pourra supposer que q est suffisamment grand).

3. En déduire une procédure $\text{ChercheGen}(E, n)$ qui cherche un générateur potentiel du groupe $E(\mathbb{F}_q)$ et un entier $m \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ satisfaisant $[m]P = 0$.
4. Tester sur la courbe $E = [0, -1, 1, 0, 0]$ sur \mathbb{F}_{2^n} avec n de plus en plus grand.

Exercice 4

L'objectif de cet exercice est de calculer quelques logarithmes discrets via la méthode « *baby-step giant-step* » (Pas de bébés-Pas de géants). Soient E une courbe elliptique sur un corps \mathbb{K} . Soient P et Q deux points tel que Q appartienne au sous-groupe cyclique engendré par P . On cherche à déterminer un entier n tel que $[n]P = Q$.

1. Étant donné une courbe elliptique, $Q \in \langle P \rangle$ sur celle-ci et deux réels i_{min} et i_{max} , écrire une procédure déterminant un entier relatif n satisfaisant $[n]P = Q$ et $i_{min} \leq n \leq i_{max}$. Appelez-la $\text{babygiant}(E, P, Q, min, max)$.
2. En déduire une procédure déterminant l'ordre d'un point connaissant un encadrement d'un multiple de l'ordre.
3. En déduire une procédure déterminant l'ordre d'un point sur une courbe elliptique sur un corps fini.
4. Appliquer la procédure suivante à la courbe elliptique définie sur \mathbb{F}_{173} par

$$y^2 = x^3 + 146x + 33$$

et aux points $P = (168, 133)$ et $Q = (147, 74)$.

Exercice 5

L'objectif de cet exercice est de tracer graphiquement les trajectoires des itérés de points choisis aléatoirement sur une courbe elliptique définie sur \mathbb{F}_p où p est un nombre premier.

1. Écrire une procédure représentant graphiquement une courbe elliptique sur \mathbb{F}_p , puis représentant graphiquement l'arc

$$P \rightarrow [2]P \rightarrow [3]P \rightarrow \dots \rightarrow [n]P$$

où n est bien choisi et P est un point aléatoire sur la courbe elliptique. Conseil : vous pourriez représenter \mathbb{F}_p sur l'axe des abscisses par $\{0, 1, \dots, p-1\}$ et sur l'axe des ordonnées par $\{-(p-1)/2, \dots, (p-1)/2\}$.

2. Tester sur quelques courbes elliptiques et sur plusieurs points pour voir si des choses intéressantes se passent.
3. Changer de point de vue : fixer une courbe elliptique E sur \mathbb{Q} et un point P à coefficients dans \mathbb{Z} sur E d'ordre infini. Pour chaque nombre premier p , représenter graphiquement la courbe elliptique \overline{E}_p ainsi que la trajectoire des itérés de \overline{P} (la réduction modulo p de P). Prendre p de plus en plus grand. Que se passe-t-il ?