Centre universitaire Abdelhafid Boussouf - Mila -

Institut des Sciences et de la Technologie

Département des Mathématique et informatique

Module : Courbes elliptiques - **Année universitaire : 2020 - 2021**

Série 02 : Les courbes elliptiques

Exercice 01

On considère la courbe $E : y^2 = x^3 + 2x$ sur le corps fini $\mathbb{F}_{13}$.

1. Calculer son discriminant Δ et son j-invariant. En déduire que E est une courbe elliptique.

2. Énumérer les points de $E(\mathbb{F}_{13})$. Donner la structure de $E(\mathbb{F}_{13})$.

3. Donner les points de $E(\mathbb{F}_{13})$ d'ordre 2.

4. Soit $P = (1, 4)$. Calculer $2P$ et $4P$, et donner un point d'ordre 5.

5. On considère $\mathbb{F}_{13^2} = \mathbb{F}_{13}(\theta)$ avec $\theta^2 = -2$. Quels sont les points d'ordre 2 de $E(\mathbb{F}_{13^2})$? Le groupe $E(\mathbb{F}_{13^2})$, est-il cyclique ?

6. Calculer $|E(\mathbb{F}_{13^2})|$.

Exercice 02

1. On considère le corps $\mathbb{F}_9 = \mathbb{F}_3(\theta)$, où θ vérifie $\theta^2 + \theta + 2$.

(a) Donner les éléments de $\mathbb{F}_9$.

(b) Montrer que θ est générateur du groupe $\mathbb{F}_9^\times$.

(c) Donner l'ensemble des éléments qui sont des carrés dans $\mathbb{F}_9$.

2. On s'intéresse maintenant à la courbe elliptique E définit sur $\mathbb{F}_9$ par l'équation

$$y^2 = x^3 + x + \theta.$$

(a) Donner l'ensemble des points de $\mathbb{F}_9 \times \mathbb{F}_9$ vérifiant l'équation de la courbe E. Montrer que le groupe commutatif construit a partir de E est d'ordre 7.

(b) Quelle est la nature du groupe construit a partir de E ?