Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22 - Enseignement à distance
Alain Kraus

Second devoir

À rendre pour le vendredi 15 avril

Soit E la courbe projective définie sur $\mathbb{F}_7$ d'équation

$$y^2z = x^3 + xz^2 + z^3.$$

1) Montrer que E est une courbe elliptique sur $\mathbb{F}_7$.
2) Décrire l'ensemble $E(\mathbb{F}_7)$ des points de E rationnels sur $\mathbb{F}_7$.
3) Quel est le polynôme caractéristique de l'endomorphisme de Frobenius de E ?

Notons $\mathbb{F}_{7^n}$ le corps de cardinal 7^n dans une clôture algébrique de $\mathbb{F}_7$.

4) Quel est l'ordre du groupe $E(\mathbb{F}_{7^2})$?
5) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{7^2})$.
6) Quel est l'ordre du groupe $E(\mathbb{F}_{7^3})$?

Soit $E[2]$ le groupe des points de 2-torsion de E.

7) Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_7[X]$.
8) En déduire que $E[2]$ est contenu dans $E(\mathbb{F}_{7^3})$.
9) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{7^3})$.
10) Déterminer une base de $E[2]$ sur $\mathbb{Z}/2\mathbb{Z}$. Expliciter dans cette base la matrice de l'endomorphisme de Frobenius de E restreint à $E[2]$.

Soit $E[3]$ le groupe des points de 3-torsion de E. Notons $G \in \mathbb{F}_7[X]$ le polynôme de dont les racines sont les abscisses des points non nuls de $E[3]$.

11) Expliciter G (voir le lemme 4.6 du cours).
12) Montrer que $5G$ est le produit de deux polynômes irréductibles unitaires de degré 2 de $\mathbb{F}_7[X]$.
13) En déduire avec la question 4 le plus petit entier $n \geq 1$ tel que $\mathbb{F}_7(E[3]) = \mathbb{F}_{7^n}$ (voir le lemme 4.7).
14) Quel est l'ordre de $E(\mathbb{F}_{7^4})$?
15) Admettons qu'il existe un élément de $\mathbb{F}_{7^2}$, qui n'est pas dans $\mathbb{F}_7$ et qui soit l'abscisse d'un point de 5-torsion de E. En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{7^4})$.
