Examen Partiel - Courbes Elliptiques

lundi 12 décembre 2011, 9h – 10h30

Documents de cours autorisés

Corrigé

Exercice 1 Soit p un nombre premier impair, $a, b \in \mathbb{F}_{2^p}^*$ et E la courbe sur $\mathbb{F}_{2^p}$ donné par l'équation

$$y^2 + ay = x^3 + b.$$

.

(1) Montrer que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ et se scinde sur $\mathbb{F}_4$. En déduire que l'application $x \mapsto x^3$ est bijective sur $\mathbb{F}_{2^p}$. En conclure que tout élément de $\mathbb{F}_{2^p}$ est le cube d'un unique élément dans $\mathbb{F}_{2^p}$.
(2) Montrer que E est une courbe elliptique. Calculer son discriminant et son j-invariant. La courbe E est-elle supersingulière ?
(3) Calculer $|E(\mathbb{F}_{2^p})|$ et en déduire la valeur t de la trace du Frobenius.
(4) Donner une formule simple pour $|E(\mathbb{F}_{2^q})|$ où q est un multiple de p.

Solution.

(1) Soit $P(X) = X^2 + X + 1$. Alors $P(0) = P(1) = 1$. Aini P n'a pas de facteur linéaire ; comme il est de degré deux, il est irréductible sur $\mathbb{F}_2$. On a donc $\mathbb{F}_4 = \mathbb{F}_2(\theta)$ où $P(\theta) = 0$. Alors $X - \theta$ divise P, et P se scinde sur $\mathbb{F}_4$. Comme $\mathbb{F}_{2^2} \leq \mathbb{F}_{2^n}$ si et seulement si $2 \mid n$ et p est impair, P n'a pas de solution dans $\mathbb{F}_{2^p}$. Ainsi la seule solution de $0 = X^3 - 1 = (X-1)(X^2+X+1)$ dans $\mathbb{F}_{2^p}$ est 1, et le noyau
$$\ker(x \mapsto x^3) = \{x \in \mathbb{F}_{2^p} : x^3 = 1\} = \{1\}.$$
L'application est alors injective, et donc surjective de $\mathbb{F}_{2^p}^\times \to \mathbb{F}_{2^p}^\times$. Comme 0 a une unique racine cubique 0, tout élément de $\mathbb{F}_{2^p}$ a une unique racine cubique dans $\mathbb{F}_{2^p}$.
(2) D'après le cours, $\Delta(E) = a_3^3 = a^3 \neq 0$ et $j(E) = 0$. Donc E est lisse, et est une courbe elliptique. Comme $j(E) = 0$, la courbe est supersingulière.
(3) On a $x^3 = y^2 + ay - b$. Pour chaque valeur de $y \in \mathbb{F}_{2^p}$ il y a donc une unique valeur de $x \in \mathbb{F}_{2^p}$ tel que $(x, y) \in E(\mathbb{F}_{2^p})$. Ainsi $|E(\mathbb{F}_{2^p})| = 2^p + 1$, et la trace du Frobenius est
$$t = 2^p + 1 - |E(\mathbb{F}_{2^p})| = 0.$$
(4) Le polynôme caractéristique de l'endomorphisme de Frobenius est
$$\chi_E(T) = T^2 - tT + 2^p = T^2 + 2^p.$$
Ses deux racines sont $\tau_{1/2} = \pm i 2^{p/2}$. Alors si $q = kp$ on a

$$|E(\mathbb{F}_{2^q})| = |E(\mathbb{F}_{(2^p)^k})| = 2^q + 1 - \tau_1^k - \tau_2^k = \begin{cases} 2^q + 1 & \text{si } k \text{ est impair,} \\ 2^q + 1 - 2\,(-2^p)^{k/2} & \text{si } k \text{ est pair.} \end{cases}$$

Exercice 2 Soit E une courbe elliptique sur un corps fini $\mathbb{F}_p$.

(1) Montrer que l'automorphisme de Frobenius induit une bijection involutive sans point fixe de l'ensemble
$$E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p).$$
(2) En déduire que $|E(\mathbb{F}_{p^2})| - |E(\mathbb{F}_p)|$ est pair.

Solution.

(1) Soit $\sigma_p : x \mapsto x^p$ l'automorphisme de Frobenius. Comme E est défini sur $\mathbb{F}_p$ et σ_p fixe les points de $\mathbb{F}_p$ et donc les coefficients de E, l'application induite
$$\sigma_p : (x, y) \mapsto (\sigma_p(x), \sigma_p(y) = (x^p, y^p)$$

envoit les points de E sur des points de E, et fixe précisément les points $E(\mathbb{F}_p)$. Comme σ_p est injective sur le corps, σ_p est injective sur la courbe elliptique, et donc surjective. De plus, pour $x \in \mathbb{F}_{p^2}$ on a $\sigma_p(x) \in \mathbb{F}_{p^2}$. Ainsi σ_p permute les points de $E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)$ sans point fixe.

Ensuite, $\sigma_p \circ \sigma_p = \sigma_{p^2}$ fixe les points de $\mathbb{F}_{p^2}$, et donc les points de $E(\mathbb{F}_{p^2})$. Donc l'action de σ_p est involutive : $\sigma_p^2(P) = P$ pour tout $p \in E(\mathbb{F}_{p^2})$.

(2) Sur $E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)$ je considère la relation $P \sim Q$ si $P = Q$ ou $P = \sigma_p(Q)$. Alors $\sim$ est une relation d'équivalence dont toutes les classes sont de taille deux, de la forme $\{P, \sigma_p(P)\}$ pour un point $P \in E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)$. Donc

$$|E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)| = 2\,|E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)|$$

est pair.

Exercice 3 On considère la courbe

$$E : y^2 = x^3 + x^2 + \theta$$

sur le corps $\mathbb{F}_9 = \mathbb{F}_3(\theta)$, où $\theta^2 = -1$.

(1) Montrer que E est une courbe elliptique; calculer son discriminant et son j-invariant. La courbe, est-elle supersingulière ?
(2) Déterminer les points de $E(\mathbb{F}_9)$.
(3) En déduire la valeur t de la trace du Frobenius. La courbe, est-elle anormale ?
(4) Le groupe $E(\mathbb{F}_9)$, est-il cyclique ?

Solution.

(1) On a $\Delta(E) = -a_2^3 a_6 = -\theta \neq 0$ et $j(E) = -a_2^3/a_6 = -1/\theta = \theta$. Donc E est lisse, et est une courbe elliptique. On a $t = 1$ (voir 3.). Donc $\mathrm{car}(\mathbb{F}_9) = 3 \nmid t$ et E n'est pas supersingulière.

(2) On a

x	x^2	x^3	$x^3 + x^2 + \theta$
0	0	0	θ
1	1	1	$\theta - 1$
-1	1	-1	θ
θ	-1	$-\theta$	-1
$-\theta$	-1	θ	$-1 - \theta$
$1 + \theta$	$-\theta$	$1 - \theta$	$1 - \theta$
$1 - \theta$	θ	$1 + \theta$	1
$\theta - 1$	θ	$-1 - \theta$	$\theta - 1$
$-1 - \theta$	$-\theta$	$\theta - 1$	$\theta - 1$

Donc

$$E(\mathbb{F}_9) = \{\mathcal{O}, (0, 1-\theta), (0, \theta-1), (-1, 1-\theta), (-1, \theta-1), (\theta, \theta), (\theta, -\theta), (1-\theta, 1), (1-\theta, -1)\}.$$

(3) La valeur t de la trace du Frobenius est

$$t = 9 + 1 - |E(\mathbb{F}_9)| = 10 - 9 = 1.$$

La courbe est donc anormale.

(4) On a $E(\mathbb{F}_9) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, où $d_1 \mid d_2$ et $d_1 \mid 9 - 1 = 8$. Comme d_1 divise aussi $|E(\mathbb{F}_9)| = 9$, on a $d_1 = 1$ et $E(\mathbb{F}_9) \cong \mathbb{Z}/9\mathbb{Z}$ est cyclique.