Examen Partiel - Courbes Elliptiques

mardi 26 novembre 2013, 9h – 10h30

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^3 + X^2 + 1$. Construire le corps $\mathbb{F}_8$ à l'aide de θ.
(3) On considère la courbe $E : y^2 + y = x^3 + \theta$. Calculer son discriminant Δ et son j-invariant. En déduire que E est une courbe elliptique.
(4) Énumérer les points de $E(\mathbb{F}_8)$.
(5) Donner une formule pour $-P$ et pour $2P$, où $P = (x, y) \in E$. En déduire que $3P = 0$ si et seulement si $x = 1$.
(6) Montrer que $E(\mathbb{F}_8)$ est cyclique.

Solution.

(1) Soit $P(X) = X^3 + X^2 + 1$. On a $P(0) = P(1) = 1$. Donc P n'a pas de facteur linéaire sur $\mathbb{F}_2$; comme $\deg(P) = 3$, le polynôme est irréductible.
(2) $\mathbb{F}_8 = \mathbb{F}_2(\theta) \cong \mathbb{F}_2[X]/(P)$, où $\theta^3 + \theta^2 + 1 = 0$ et (P) est l'idéal de $\mathbb{F}_2[X]$ engendré par P.
(3) La coube E est en forme de Weierstass courte en caractéristique 2, avec $a_1 = a_2 = a_4 = 0$, $a_3 = 1$ et $a_6 = \theta$. D'après la formule du cours,

$$\Delta(E) = a_3^3 = 1 \qquad \text{et} \qquad j(E) = 0.$$

Comme $\Delta(E) \neq 0$, la coube est lisse et E est une courbe elliptique.
(4)

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

On a donc

$$\begin{aligned} E(\mathbb{F}_8) = \{&\mathcal{O}, (1, \theta^2), (1, \theta^2 + 1), (\theta + 1, 0), (\theta + 1, 1), \\ &(\theta^2 + 1, \theta), (\theta^2 + 1, \theta + 1), (\theta^2 + \theta, \theta^2 + \theta), (\theta^2 + \theta, \theta^2 + \theta + 1)\}. \end{aligned}$$

(5) D'apres la formule du cours,

$$\begin{aligned} -(x, y) &= (x, -y - a_1 x - a_3) = (x, y + 1), \\ 2(x, y) &= (\lambda^2 + a_1\lambda - a_2 - 2x, \lambda(x - x_3) - y - a_1 x_3 - a_3) \\ &= ((x^2)^2, x^2(x + x^4) + y + 1) = (x^4, x^3(1 + x^3) + y + 1), \end{aligned}$$

puisque $\lambda = x^2/1$. Alors $3(x, y) = 0$ ssi $-(x, y) = 2(x, y)$ ssi $x = x^4$ ssi $x = 0$ ou $x = 1$.
(6) $|E(\mathbb{F}_8)| = 9$ et il n'y a que deux éléments d'ordre 3 : $(1, \theta^2)$ et $(1, \theta^2 + 1)$. Donc $E(\mathbb{F}_8) \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $E(\mathbb{F}_8) \cong \mathbb{Z}/9\mathbb{Z}$ est bien cyclique.

Exercice 2. Soit n impair et $a \in \mathbb{F}_{3^n}^\times$. Soit E la courbe sur $\mathbb{F}_{3^n}$ d'équation $y^2 = x^3 + a\,x$.

(1) Montrer que -1 n'est pas un carré dans $\mathbb{F}_3$, mais que -1 est un carré dans $\mathbb{F}_9$. En déduire que si -1 est un carré dans $\mathbb{F}_{3^k}$, alors k est pair. En déduire que -1 n'est pas un carré dans $\mathbb{F}_{3^n}$.
(2) En considérant l'application $x \mapsto x^2$, montrer qu'il y a $(3^n+1)/2$ carrés dans $\mathbb{F}_{3^n}$. Montrer que si $b \in \mathbb{F}_{3^n}^\times$, alors b et $-b$ ne sont pas simultanément des carrés. En déduire que pour tout $b \in \mathbb{F}_{3^n}^\times$, soit b soit $-b$ est un carré.
(3) Calculer le discriminant et le j-invariant de E. En déduire que E est une courbe elliptique.
(4) Calculer $|E(\mathbb{F}_{3^n})|$. En déduire la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ?
(5) Donner une formule simple pour $|E(F_{3^{nk}})|$ en fonction de k.

Solution.

(1) On a $0^2 = 0$ et $(\pm 1)^2 = 1$. Donc -1 n'est pas un carré dans $\mathbb{F}_3$. Si $\theta^2 + 1 = 0$, alors $\mathbb{F}_3(\theta) = \mathbb{F}_{3^2} = \mathbb{F}_9$, et -1 a une racine carrée θ dans $\mathbb{F}_9$. Or, $\mathbb{F}_{3^\ell} \subseteq \mathbb{F}_{3^k}$ ssi $\ell \mid k$. Donc k est pair ssi $\mathbb{F}_3(\theta) \subseteq \mathbb{F}_{3^k}$ ssi $\theta \in \mathbb{F}_{3^k}$ ssi -1 a une racine carrée dans $\mathbb{F}_{3^k}$. Puisque n est impair, -1 n'a pas de racine carrée dans $\mathbb{F}_{3^n}$.
(2) Le noyau de l'homomorphisme $x \mapsto x^2$ de $\mathbb{F}_{3^n}^\times$ est $\{\pm 1\}$. Donc l'image est de taille $(3^n-1)/2$. Comme 0 est aussi un carré, il y a au total $(3^n+1)/2$ carrés dans $\mathbb{F}_{3^n}$.

Supposons que b et $-b$ sont des carrés dans $\mathbb{F}_{3^n}^\times$. Alors $-b/b = -1$ est aussi un carré, contradiction. Donc b et $-b$ ne sont pas simultanément des carrés. Mais il y a $(3^n-1)/2$ carrés dans $\mathbb{F}_{3^n}^\times$, et au total $3^n - 1$ éléments. Ainsi pour tout $b \in \mathbb{F}_{3^n}^\times$, soit b soit $-b$ est un carré.
(3) On a $a_1 = a_2 = a_3 = a_6 = 0$ et $a_4 = a$. D'après la formule du cours, puisque $a \neq 0$,

$$\Delta(E) = -a_4^3 = -a^3 \neq 0 \qquad \text{et} \qquad j(E) = 0.$$

Comme $\Delta(E) \neq 0$, la coube est lisse et E est une courbe elliptique.
(4) Pour tout $x \in \mathbb{F}_{3^n}^\times$, soit $x^3 + ax$, soit $-(x^3+ax) = (-x)^3 + a\,(-x)$ est un carré, de la forme $y^2 = (-y)^2$. Donc il y a $2 \cdot (3^n-1)/2 = 3^n - 1$ points sur la courbe, outre que $\mathcal{O}$ et $(0,0)$. Ainsi, $|E(\mathbb{F}_{3^n})| = 3^n + 1$.

La trace t du Frobenius vaut

$$t = 3^n + 1 - |E(\mathbb{F}_{3^n})| = 3^n + 1 - (3^n+1) = 0\ ;$$

comme $\mathrm{car}(\mathbb{F}_{3^n}) = 3$ divise $t = 0$, la courbe E est supersingulière.
(5) Le polynôme caractéristique de l'endomorphisme de Frobenius est

$$\chi_E(T) = T^2 - tT + 3^n = T^2 + 3^n$$

avec zéros $\tau_1 = i\sqrt{3^n}$ et $\tau_2 = -i\sqrt{3^n}$. Ainsi

$$|E(\mathbb{F}_{3^{nk}})| = 3^{nk} + 1 - \tau_1^k - \tau_2^k = \begin{cases} 3^{nk}+1 & \text{si } k \text{ est impair} \\ 3^{nk} + 1 - 2\,(-3^n)^{k/2} & \\ \qquad = 3^{nk} + 1 + (-3^n)^{k/2} & \text{si } k \text{ est pair.} \end{cases}$$