Examen Partiel - Courbes Elliptiques

Vendredi 4 décembre 2915, 9h – 11h

Documents non-autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1

(1) Montrer que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^3 + X + 1$. Construire le corps $\mathbb{F}_8$ à l'aide de θ.
(3) Donner la forme de Weierstrass (longue) pour une courbe elliptique.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_8$, où $\theta \in \mathbb{F}_8$ satisfait $\theta^3 + \theta + 1 = 0$.

(4) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique.
(5) Calculer θ^n comme polynôme en θ de degré au plus deux, pour $1 \leq n \leq 6$. Énumérer les points de $E(\mathbb{F}_8)$.
(6) Calculer la valeur t de la trace du Frobenius.
(7) Donner la définition de supersingulière. La courbe E, est-elle supersingulière ?
(8) Donner une formule pour $|E(\mathbb{F}_{8^n})|$ en fonction de n.
(9) $E(\mathbb{F}_8)$, est-il cyclique ?
(10) Donner un point d'ordre 3.
(11) Donner la plus petite extension $\mathbb{F}_{8^n}$ de $\mathbb{F}_8$ telle que

$$E(\mathbb{F}_{8^n})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

Solution.

(1) Soit $P(X) = X^3 + X + 1$. 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 $\theta^3 + \theta + 1 = 0$ et (P) est l'idéal de $\mathbb{F}_2[X]$ engendré par P. On a

$$\mathbb{F}_8 = \{\ell + m\theta + n\theta^2 : \ell, m, n \in \mathbb{F}_2\}.$$

(3) Forme de Weierstrass longue :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(4) La courbe E est en forme de Weierstass courte en caractéristique 2, avec $a_1 = a_2 = a_4 = 0$ et $a_3 = a_6 = \theta$. D'après le formulaire,

$$b_2 = 0, \quad b_4 = 0, \quad b_6 = \theta^2, \quad b_8 = 0.$$

Donc

$$\Delta(E) = \theta^4 \qquad \text{et} \qquad j(E) = 0.$$

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

(5)

x	x^2	$x^2 + \theta x$	x^3	$x^3 + \theta$
0	0	0	0	θ
1	1	$\theta + 1$	1	$\theta + 1$
θ	θ^2	0	$\theta + 1$	1
θ^2	$\theta^2 + \theta$	$\theta^2 + 1$	$\theta^2 + 1$	$\theta^2 + \theta + 1$
$\theta^3 = \theta + 1$	$\theta^2 + 1$	$\theta + 1$	θ^2	$\theta^2 + \theta$
$\theta^4 = \theta^2 + \theta$	θ	$\theta^2 + 1$	$\theta^2 + \theta + 1$	$\theta^2 + 1$
$\theta^5 = \theta^2 + \theta + 1$	$\theta + 1$	$\theta^2 + \theta$	θ	0
$\theta^6 = \theta^2 + 1$	$\theta^2 + \theta + 1$	$\theta^2 + \theta$	$\theta^2 + \theta$	θ^2

On a donc

$$E(\mathbb{F}_8) = \{O, (1,1), (1,\theta+1), (\theta+1, \theta^2+1), (\theta+1, \theta^2+\theta+1), (\theta^2+\theta, \theta^2), (\theta^2+\theta, \theta^2+\theta), (\theta^2+\theta+1, 0), (\theta^2+\theta+1, \theta)\}$$

et $|E(\mathbb{F}_8)| = 9$.

(6) On a $t = 8 + 1 - |E(\mathbb{F}_8)| = 0$.

(7) Une courbe elliptique est supersingulière si $E[p] = \{O\}$, ssi la caractéristique p divise la trace t du Frobenius. Comme $2 \mid 0$ (ou puisque $j(E) = 0$ et la caractéristique est 2), la courbe est supersingulière.

(8) Le polynôme caractéristique de l'endomorphisme du Frobenius est

$$\chi_E(T) = T^2 - tT + q = T^2 + 8\,;$$

ses racines sont $\tau_{1/2} = \pm i\sqrt{8}$. On a

$$|E(\mathbb{F}_{8^n})| = 8^n + 1 - \tau_1^n - \tau_2^n = \begin{cases} 8^n + 1 & \text{si } n \text{ est impair} \\ 8^n + 1 - 2 \cdot (-8)^\ell & \text{si } n = 2\ell \text{ est pair.} \end{cases}$$

(9) $E(\mathbb{F}_8) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$, où $d_1 \mid d_2$ et $d_1 \mid q - 1 = 8 - 1 = 7$. Puisque $d_1 d_2 = |E(\mathbb{F}_8)| = 9$, on a $d_1 = 1$ et le groupe est cyclique.

(10) Un point d'ordre 3 est un point P avec $2P = -P$. Si $P = (x, y)$, alors

$$-P = (x, y + \theta)$$

et

$$2P = (\lambda^2, \lambda(x + \lambda^2) + y + \theta) \quad \text{avec} \quad \lambda = \frac{x^2}{\theta}.$$

Ainsi

$$x = \lambda^2 = \frac{x^4}{\theta^2} \quad \text{et} \quad y + \theta = \lambda(x + \lambda^2) + y + \theta.$$

Ainsi

$$x^4 = \theta^2\, x \quad \text{et} \quad \lambda(x + \lambda^2) = 0.$$

Remarquons que la deuxième condition est superflue, puisque la première implique $x + \lambda^2 = 0$.

Une solution est $x = 0$, mais il n'y a pas de point $(0, y) \in E(\mathbb{F}_8)$.

Si $x \neq 0$, alors $x^3 = \theta^2$. Il y a une seule solution $x = \theta + 1$ dans $\mathbb{F}_8$. Ainsi $(\theta + 1, \theta^2 + 1)$ et $(\theta + 1, \theta^2 + \theta + 1)$ sont les deux points d'ordre 3 dans $E(\mathbb{F}_8)$.

(11) $E(\mathbb{F}_{8^n})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$ si et seulement s'il y a au moins trois points d'ordre 3 dans $E(\mathbb{F}_{8^n})$ (et dans ce cas, tous les points d'ordre 3 sont dans $E(\mathbb{F}_{8^n})$, comme trois points non-triviaux engendrent $(\mathbb{Z}/3\mathbb{Z})^2$.

On a vu qu'un point de la forme $(0, y)$ sera d'ordre 3. Alors on aura

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

Puisque $Q(Y) = Y^2 + \theta Y + \theta$ est irréductible dans $\mathbb{F}_8$, une solution ξ engendre une extension

$$\mathbb{F}_8(\xi) \cong \mathbb{F}_8[Y]/(Q)$$

de degré 2. Ainsi $\mathbb{F}_8(\xi) = \mathbb{F}_{8^2} = \mathbb{F}_{64}$, et $(0, \xi) \in E(\mathbb{F}_{64})$ est un troisième point d'ordre 3. Alors $E(\mathbb{F}_{64})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, et c'est l'extension minimale avec cette propriété.