Examen - Courbes Elliptiques

vendredi 6 février 2015, 8h45 – 11h45

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^2 - X - 1$ est irréductible dans $\mathbb{F}_3$.
(2) Soit θ une racine de $X^2 - X - 1$. Construire le corps $\mathbb{F}_9$ à l'aide de θ.

On considère la courbe $E : y^2 = x^3 + x + \theta$ sur $\mathbb{F}_9$, où $\theta \in \mathbb{F}_9$ satisfait $\theta^2 - \theta - 1 = 0$.

(3) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique. La courbe E, est-elle supersingulière ?
(4) Énumérer les points de $E(\mathbb{F}_9)$. La courbe $E(\mathbb{F}_9)$, est-elle cyclique ?
(5) Calculer la valeur t de la trace du Frobenius.
(6) Donner une formule pour $|E(\mathbb{F}_{9^n})|$ en fonction de n, et donner la valeur minimale de n pour que $E(\mathbb{F}_{9^n})$ possède une involution.

Solution.

(1) Soit $P(X) = X^2 - X - 1$. On a $P(0) = P(1) = -1$ et $P(-1) = 1$. Donc P n'a pas de facteur linéaire sur $\mathbb{F}_3$; comme $\deg(P) = 3$, le polynôme est irréductible.
(2) $\mathbb{F}_9 = \mathbb{F}_3(\theta) \cong \mathbb{F}_3[X]/(P)$, où $\theta^2 - \theta - 1 = 0$ et (P) est l'idéal de $\mathbb{F}_3[X]$ engendré par P. On a
$$\mathbb{F}_9 = \{m + n\theta : m, n \in \mathbb{F}_3\}.$$
(3) La courbe E est en forme de Weierstass courte en caractéristique 3, avec $a_1 = a_3 = a_2 = 0$, $a_4 = 1$ et $a_6 = \theta$. D'après la formule du cours,
$$\Delta(E) = -a_4^3 = -1 \qquad \text{et} \qquad j(E) = 0.$$
Comme $\Delta(E) \neq 0$, la courbe est lisse et E est une courbe elliptique. Puisque $\mathrm{car}(\mathbb{F}_9) = 3$ et $j(E) = 0$, la courbe est supersingulière.
(4)

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

On a donc
$$E(\mathbb{F}_9) = \{\mathcal{O}, (-1, \theta), (-1, -\theta), (\theta, \theta), (\theta, -\theta), (1 - \theta, \theta), (1 - \theta, -\theta)\}.$$
Ainsi $|E(\mathbb{F}_9)| = 7$ est premier, et $E(\mathbb{F}_9)$ est cyclique.
(5) On a $t = 9 + 1 - |E(\mathbb{F}_9)| = 3$. On note que $3 \mid 3$, ce qui confirme que la courbe est supersingulière.

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

$$\chi_E(T) = T^2 - tT + q = T^2 - 3T + 9\,;$$

ses racines sont

$$\tau_{1/2} = \frac{3 \pm i\sqrt{4 \cdot 9 - 3^2}}{2} = 3\,\frac{1 \pm i\sqrt{3}}{2} = 3e^{\pm i\pi/3}.$$

On a

$$|E(\mathbb{F}_{9^n})| = 9^n + 1 - \tau_1^n - \tau_2^n = 9^n + 1 - 2\,\mathrm{Re}(3^n e^{in\pi/3}) = 9^n + 1 + 2 \cdot 3^n \cos(n\pi/3).$$

Ainsi

$$\begin{aligned}
&|E(\mathbb{F}_{9^1})| = 7,\\
&|E(\mathbb{F}_{9^2})| = 9^2 + 1 - 2 \cdot 3^2 \cos(2\pi/3) = 81 + 1 - 18 \cdot (-\frac{1}{2}) = 91,\\
&|E(\mathbb{F}_{9^3})| = 9^3 + 1 - 2 \cdot 3^3 \cos(\pi) = 729 + 1 - 54 \cdot (-1) = 784.
\end{aligned}$$

Donc $n = 3$ est le plus petit entier pour que $|E(\mathbb{F}_{9^n})|$ soit pair, et $E(\mathbb{F}_{9^n})$ possède une involution.

Exercice 2. On considère la courbe $E : y^2 = x^3 + x + 1$ sur le corps fini $\mathbb{F}_{13}$.

(1) Calculer le discriminant $\Delta(E)$. En déduire que E est une courbe elliptique.
(2) Soit $P = (-6, 0)$. Vérifier que $P \in E(\mathbb{F}_{13})$ et donner l'ordre de P.
(3) Soit $Q = (-5, -1)$. Vérifier que $Q \in E(\mathbb{F}_{13})$. Calculer $-Q$ et $8Q$. En déduire l'ordre de Q. Donner un point R d'ordre 18.
(4) Donner une borne supérieure pour $|E(\mathbb{F}_{13})|$. En déduire que R est un générateur du groupe $E(\mathbb{F}_{13})$.

Solution.

(1) La courbe E est en forme de Weierstass courte en caractéristique 13 (donc différente de 2 et de 3), avec $a_1 = a_3 = a_2 = 0$ et $a_4 = a_6 = 1$. D'après la formule du cours,

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) = -16(4 + 27) \equiv -3 \cdot 5 \equiv -2 \mod 13.$$

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

$$(-6)^3 + (-6) + 1 = 36 \cdot (-6) - 5 \equiv (-3)(-6) - 5 \equiv 5 - 5 = 0 = 0^2 \mod 13.$$

Donc $P = (-6, 0) \in E(\mathbb{F}_{13})$. On a $-P = (-6, -0) = P$, et l'ordre de P est deux.
(3) On a

$$(-5)^3 + (-5) + 1 = 25 \cdot (-5) - 4 \equiv ((-1)(-5) - 4 = 1 = (-1)^2 \mod 13.$$

Donc $Q = (-5, -1) \in E(\mathbb{F}_{13})$, et $-Q = (-5, 1)$. Pour doubler un point (x, y), la formule du cours donne

$$\lambda = \frac{3x^2 + 1}{2y}, \quad x' = \lambda^2 - 2x \quad \text{et} \quad y' = \lambda(x - x') - y.$$

Ainsi (tout modulo 13) on obtient

$Q = (-5, -1)$
$\lambda = \frac{3(-5)^2+1}{2(-1)} \equiv 1, \qquad x' = 1^2 - 2(-5) \equiv -2, \quad y' = 1(-5-(-2)) - (-1) = -2$
$2Q = (-2, -2)$
$\lambda = \frac{3(-2)^2+1}{2(-2)} \equiv 0, \qquad x' = 0^2 - 2(-2) = 4, \qquad y' = 0(-2-4) - (-2) = 2$
$4Q = (4, 2)$
$\lambda = \frac{3 4^2+1}{2 \cdot 2} = \frac{5}{2} \equiv -4, \quad x' = (-4)^2 - 2 \cdot 4 \equiv -5, \quad y' = (-4)(4-(-5)) - 2 \equiv 1$
$8Q = (-5, 1)$

Alors $8Q = -Q$ et $9Q = \mathcal{O}$. D'autre part, $4Q \neq Q$. L'ordre de Q vaut donc 9. Puisque 9 et 2 sont premiers entr'eux, $R = P + Q$ est d'ordre $2 \cdot 9 = 18$. Les formules du cours donnent pour R

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-1-0}{-5-(-6)} = -1,$$
$$x' = \lambda^2 - x_1 - x_2 = (-1)^2 - (-5) - (-6) \equiv -1,$$
$$y' = \lambda(x_1 - x_3) + y_1 = -(-6-(-1)) - 0 = 5, \quad \text{et} \quad R = (-1, 5).$$

(4) $|E(\mathbb{F}_{13})| \leq q + 1 + 2\sqrt{q} = 13 + 1 + 2\sqrt{13} = 14 + \sqrt{52}$.
Ainsi $|E(\mathbb{F}_{13})| \leq 14 + 7 = 21 < 2 \cdot 18$. Comme $o(R) = 18$, on a $|E(\mathbb{F}_{13})| = 18$ et R en est un générateur.

Exercice 3. Soit E une courbe elliptique supersingulière définie sur un corps $\mathbb{F}_p$ avec $p \geq 5$ premier. Calculer le degré MOV de E.

Solution Puisque E est supersingulière sur un corps premier de caractéristique $p \geq 5$, sa trace de l'endomorphisme de Frobenius vaut $t = 0$, et $|E(\mathbb{F}_p)| = p + 1$. Or, $p + 1$ divise $p^2 - 1 = (p+1)(p-1)$, et $p + 1$ ne divise pas $p^1 - 1$. Donc le degré MOV de E vaut 2.