Examen Partiel - Courbes Elliptiques

Vendredi 9 janvier 2915, 9h – 11h

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.
(3) Calculer θ^{-1} en fonction de θ.

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

(4) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique.
(5) Énumérer les points de $E(\mathbb{F}_9)$.
(6) Calculer la valeur t de la trace du Frobenius.
(7) La courbe E, est-elle supersingulière ?
(8) Donner une formule pour $|E(\mathbb{F}_{9^n})|$ en fonction de n.
(9) Montrer que $E(\mathbb{F}_9)$ n'a que deux involutions. En déduire que $E(\mathbb{F}_9)$ est cyclique.

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) Comme $1 = \theta^2 + \theta$, on a $\theta^{-1} = \theta + 1$.
(4) La courbe E est en forme de Weierstass courte en caractéristique 3, avec $a_1 = a_3 = a_4 = 0$, $a_2 = 1$ et $a_6 = \theta$. D'après la formule du cours,
$$\Delta(E) = -a_2^3 a_6 = -\theta \qquad \text{et} \qquad j(E) = -a_2^3 a_6^{-1} = -\theta^{-1} = -\theta - 1.$$
Comme $\Delta(E) \neq 0$, la courbe est lisse et E est une courbe elliptique.
(5)

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

On a donc
$$\begin{aligned} E(\mathbb{F}_9) = \{&O, (\theta - 1, 0), (1, \theta + 1), (1, -\theta - 1), (-\theta, \theta + 1), (-\theta, -1 - \theta), (\theta + 1, \theta + 1), \\ &(\theta + 1, -\theta - 1), (-\theta - 1, \theta - 1), (-\theta - 1, 1 - \theta), (1 - \theta, \theta), (1 - \theta, -\theta)\} \end{aligned}$$
et $|E(\mathbb{F}_9)| = 12$.
(6) On a $t = 9 + 1 - |E(\mathbb{F}_9)| = -2$.
(7) Comme $3 \nmid -2$, la courbe n'est pas supersingulière.

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

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

ses racines sont

$$\tau_{1/2} = -1 \pm i\sqrt{9-1} = -1 \pm i2\sqrt{2} = 3e^{\pm i\alpha}$$

avec $\alpha \in \arg(-1 + i2\sqrt{2})$. On a

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

(9) Une involution est un point de la forme $(x, 0)$; il n'y en a qu'un seul dans $E(\mathbb{F}_9)$, soit $(\theta - 1, 0)$. Puisque $|E(\mathbb{F}_9)| = 12 = 2^2 \cdot 3$, et

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$$

avec $d_1 \mid d_2$, $d_1 \mid q-1$ et $d_1 d_2 = |E(\mathbb{F}_q)|$, les seuls possibilités pour $E(\mathbb{F}_9)$ sont $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$. Or, le premier groupe a trois involutions. Ainsi $E(\mathbb{F}_9) \cong \mathbb{Z}/12\mathbb{Z}$.

Exercice 2

(1) Montrer que 101 est premier.

Soit E la courbe elliptique sur $\mathbb{F}_{101}$ d'équation $y^2 = x^3 + 1$. D'après le cours, on sait que E est supersingulière.

(2) Donner $|E(\mathbb{F}_{101}|$ est montrer que $E(\mathbb{F}_{101})$ est un groupe cyclique.
(3) Quels sont les ordres possibles des éléments de $E(\mathbb{F}_{101})$?
(4) Donner les éléments de $E(\mathbb{F}_{101})$ d'ordre deux et trois.

Solution.

(1) Ni 2, 3, 5 ni 7 divisent 101, et $11^2 = 121 > 101$. Donc 101 est premier.
(2) Puisque E est supersingulière sur un corps premier $\mathbb{F}_p$ avec $p \geq 5$, la trace t du Frobenius vaut zéro. Ainsi

$$|E(\mathbb{F}_{101})| = 101 + 1 - t = 102 = 2 \cdot 3 \cdot 17.$$

Comme il n'y a pas de facteur carré, le groupe est cyclique.
(3) Les ordres possibles sont les diviseurs de 102, soit 1, 2, 3, 6, 17, 34, 51 et 102.
(4) Les éléments d'ordre deux sont ceux de la forme $(x, 0)$. On doit donc resoudre $x^3 + 1 = 0$. Il y a une solution écidente $x = -1$, et $(-1, 0)$ est une involution. Comme $E(\mathbb{F}_{101})$ est cyclique, il n'y a qu'une seule involution.

Soit $P = (x, y)$ un point d'ordre trois. Alors $2P = -P = (x, -y)$. On calcule $2P$:

$$\lambda = \frac{3x^2}{2y} \quad \text{et} \quad x = \lambda^2 - 2x = \frac{9x^4}{4y^2} - 2x.$$

Ainsi $9x^4 = 12xy^2$, et soit $x = 0$, soit $4y^2 = 3x^3 = 3(y^2 - 1)$ et $y^2 = -3$. Il y a une solution évidente $(x, y) = (0, \pm 1)$. Comme $E(\mathbb{F}_{101})$ est cyclique, il n'y a que ces deux éléments d'ordre trois.