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.

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 $E(\mathbb{F}_{13})$.

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.