Examen Partiel - Courbes Elliptiques

mardi 26 novembre 2013, 9h – 11h

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.

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.