Examen Partiel - Courbes Elliptiques

mardi 18 décembre 2012, 9h – 11h

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que le polynôme $P(X) = X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$. En déduire que $\mathbb{F}_{125} = \mathbb{F}_5(\theta)$ où $\theta^3 + \theta^2 + 1 = 0$.
(2) Calculer θ^{-1} en fonction de θ.
(3) Calculer θ^{30}, puis θ^{31}. En déduire que θ et $-\theta$ sont des carrés dans $\mathbb{F}_{125}$.

On considère la courbe E définie sur $\mathbb{F}_{125}$ d'équation

$$y^2 = x^3 + \theta x.$$

(4) Calculer le discriminant et le j-invariant de E. En déduire que E est une courbe elliptique.
(5) Montrer qu'il existent trois points dans $E(\mathbb{F}_{125})$ de la forme $(x, 0)$. En déduire que $E(\mathbb{F}_{125})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(6) Montrer que les points $P_1 = (\theta, 3)$, $P_2 = (1, 2\theta + 2\theta^2)$ et $P_3 = (-1, \theta + \theta^2)$ sont sur E. Calculer $P_2 + P_3$.

Exercice 2. On considère la courbe

$$E : y^2 = x^3 + \theta x^2 + \theta$$

sur le corps $\mathbb{F}_9 = \mathbb{F}_3(\theta)$, où $\theta^2 = -1$.

(1) Montrer que E est une courbe elliptique; calculer son discriminant et son j-invariant.
(2) Déterminer les points de $E(\mathbb{F}_9)$.
(3) En déduire la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ?
(4) Le groupe $E(\mathbb{F}_9)$, est-il cyclique ?
(5) Quelle est la plus petite extension k de $\mathbb{F}_9$ tel que $E(k)$ ait un point d'ordre 2 ?