Examen Partiel - Courbes Elliptiques

lundi 12 décembre 2011, 9h – 10h30

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1 Soit p un nombre premier impair, $a, b \in \mathbb{F}_{2^p}^*$ et E la courbe sur $\mathbb{F}_{2^p}$ donné par l'équation

$$y^2 + ay = x^3 + b.$$

.

(1) Montrer que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ et se scinde sur $\mathbb{F}_4$. En déduire que l'application $x \mapsto x^3$ est bijective sur $\mathbb{F}_{2^p}$. En conclure que tout élément de $\mathbb{F}_{2^p}$ est le cube d'un unique élément dans $\mathbb{F}_{2^p}$.
(2) Montrer que E est une courbe elliptique. Calculer son discriminant et son j-invariant. La courbe E est-elle supersingulière ?
(3) Calculer $|E(\mathbb{F}_{2^p})|$ et en déduire la valeur t de la trace du Frobenius.
(4) Donner une formule simple pour $|E(\mathbb{F}_{2^q})|$ où q est un multiple de p.

Exercice 2 Soit E une courbe elliptique sur un corps fini $\mathbb{F}_p$.

(1) Montrer que l'automorphisme de Frobenius induit une bijection involutive sans point fixe de l'ensemble

$$E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p).$$

(2) En déduire que $|E(\mathbb{F}_{p^2})| - |E(\mathbb{F}_p)|$ est pair.

Exercice 3 On considère la courbe

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

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. La courbe, est-elle supersingulière ?
(2) Déterminer les points de $E(\mathbb{F}_9)$.
(3) En déduire la valeur t de la trace du Frobenius. La courbe, est-elle anormale ?
(4) Le groupe $E(\mathbb{F}_9)$, est-il cyclique ?