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.

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.