Examen - Courbes Elliptiques

Lundi 28 janvier 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 $\mathbb{F}_2$. En déduire que $\mathbb{F}_8 = \mathbb{F}_2(\theta)$ où θ est un zéro de $X^3 + X^2 + 1$.
(2) Calculer θ^i pour $0 \leq i < 7$. En déduire que θ est un générateur pour le groupe multiplicatif $\mathbb{F}_8^\times$.
(3) On considère la courbe $E : y^2 + xy = x^3 + \theta$ sur $\mathbb{F}_2(\theta)$. Montrer que E est une courbe elliptique, et calculer son discriminant Δ et son j-invariant.
(4) Enumérer les points de $E(\mathbb{F}_8)$.
[Indication : Pour $x \neq 0$ on pourra se servir de l'équation $z^2 + z = x + \theta x^{-2}$ avec $z = yx^{-1}$; pour le calcul de x^{-2} il sera utile de transformer x en puissance de θ.]
(5) Le groupe $E(\mathbb{F}_8)$, est-il cyclique ?
(6) Calculer la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ? Est-elle anormale ?
(7) Donner une formule pour $|E(\mathbb{F}_{8^k})|$.
(8) Quelle est la plus petite extension k de $\mathbb{F}_8$ tel que $E(k)$ soit anormale ?

Exercice 2. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, telle que la trace t du Frobenius soit 0. Supposons que $E(\mathbb{F}_q)$ contiennne un point d'ordre n. Soit $\phi_q : x \mapsto x^q$ l'endormorphisme de Frobenius.

(1) Montrer que $\phi_q^2(S) = -qS$ pour tout point $S \in E$.
[Indication : ϕ_q satisfait le polynôme caractéristique $\chi_E(T)$.]
(2) Montrer que n divise $q + 1$. En déduire que $\phi_q^2(S) = S$ pour tout $S \in E[n]$.
(3) En déduire que $E[n] \subseteq E(\mathbb{F}_{q^2})$.
(4) En déduire que si $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ où d_1 divise d_2 , alors $d_1 d_2$ divise $q^2 - 1$. Quel est donc le degré MOV de E ?

[Rappel : On a $x \in \mathbb{F}_q$ si et seulement si $x^q = x$.]

Exercice 3. On considère le groupe $G = \mathbb{F}_{2011}^\times$. On cherche k tel que $2k \equiv 206 \mod 2010$. Donner en détail deux algorithmes rapides pour trouver k et expliquer pourquoi ils marchent.