Examen - Courbes Elliptiques

mardi 28 janvier 2014, 9h – 12h

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1 Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$.

(1) Donner une estimation de $|E(\mathbb{F}_q)|$ en fonction de q.
(2) Donner la structure générale du groupe $E(\mathbb{F}_q)$.
(3) Montrer que si $q-1$ est premier et $q \geq 5$, alors $E(\mathbb{F}_q)$ est un groupe cyclique.
(4) Donner un exemple d'un corps fini $\mathbb{F}_q$ et d'une une courbe elliptique cyclique sur $\mathbb{F}_q$ de taille au moins 100. Justifier que la courbe est bien elliptique et cyclique, et de la bonne taille !
[Indication : Si $q-1$ est premier et au moins 4, alors q est pair.]
(5) Que peut-on dire si $\frac{q-1}{p-1}$ est premier, avec $q-3 \geq 3(p-1)^2$, où $p = \mathrm{car}(\mathbb{F}_q)$?

Exercice 2

(1) On considère la courbe $E : y^2 = x^3 + 2x$ sur le corps fini $\mathbb{F}_{13}$. Calculer son discriminant Δ et son j-invariant. En déduire que E est une courbe elliptique.
(2) Énumérer les points de $E(\mathbb{F}_{13})$. Donner la structure de $E(\mathbb{F}_{13})$.
(3) Donner les points de $E(\mathbb{F}_{13})$ d'ordre 2.
(4) Soit $P = (1, 4)$. Calculer $2P$ et $4P$, et donner un point d'ordre 5.
(5) On considère $\mathbb{F}_{13^2} = \mathbb{F}_{13}(\theta)$ avec $\theta^2 = -2$. Quels sont les points d'ordre 2 de $E(\mathbb{F}_{13^2})$? Le groupe $E(\mathbb{F}_{13^2})$, est-il cyclique ?
(6) Calculer $|E(\mathbb{F}_{13^2})|$.

Exercice 3 Soit E une courbe elliptique sur un corps fini k et n un entier tel que $\mathrm{car}(k)$ ne divise pas n. Soit μ_n le groupe multiplicatif des racines n-mes d'unité, et $e_n : E[n] \times E[n] \to \mu_n$ le couplage de Weil. Montrer que si $S, T \in E[n]$ alors l'ordre $o(e_n(S, T))$ divise $\mathrm{pgcd}(o(S), o(T))$. Est-ce qu'on a toujours égalité ?