Examen - Courbes Elliptiques

Lundi 6 janvier 2012, 9h – 11h

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^3 + X + 1$. Construire le corps $\mathbb{F}_8$ à l'aide de θ.
(3) On considère la courbe $E : y^2 + y = x^3 + \theta$. Montrer que E est une courbe elliptique, et calculer son discriminant Δ et son j-invariant.
(4) Énumérer les points de $E(\mathbb{F}_8)$.

Exercice 2. Soit $E : y^2 = x^3 - x + 1$ sur $\mathbb{F}_1 1$.

(1) Montrer que E est une courbe elliptique.
(2) Étant donné que $|E(\mathbb{F}_{11})| = 10$, en déduire la valeur de t, la trace du Frobenius.
(3) Donner une formule pour $|E(\mathbb{F}_{11^n})|$ en fonction de n. Calculer et factoriser $|E(\mathbb{F}_{11^3})|$.
(4) Donner un algorithme pour trouver un point d'ordre 139 dans $E(\mathbb{F}_{11^3})$, et expliquer pourquoi il marche.

Exercice 3. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et n un entier non divisible par $\mathrm{car}(\mathbb{F}_q)$. Soit μ_n le groupe des racines $n$mes de 1.

(1) Montrer que le couplage de Weil $e_n : E[n] \times E[n] \to \mu_n$ est surjectif. [On peut utiliser le fait qu'il est non dégénéré.]
(2) En déduire que $\mu_n \leq \mathbb{F}_q$, et que n divise $q - 1$.
(3) 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 divise $q - 1$.

Exercice 4. Soit E une courbe elliptique sur un corps k.

(1) Si f est une fonction rationnelle sur E et $D = \sum_i n_i[P_i]$ un diviseur tel qu'aucun P_i est un zéro ou un pôle de f, donner la définition de $f(D)$.
(2) Soit F' une deuxième fonction rationnelle sur E, et D' un deuxième diviseur. Montrer que
$$(f \cdot f')(D) = f(D) \cdot f'(D) \quad \text{et} \quad f(D + D') = f(D) \cdot f(D').$$
(3) Donner la définition du couplage de Tate $\langle P, Q \rangle_n$ pour deux points $P, Q \in E[n]$.
(4) Montrer que le couplage de Tate est bilinéaire.
(5) Exprimer le couplage de Weil en termes du couplage de Tate. En déduire que le couplage de Weil est bilinéaire.