Examen - Courbes Elliptiques

vendredi 6 janvier 2017, 9h – 12h

Documents non-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.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_8 = \mathbb{F}(\theta)$.

(3) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique. La courbe E, est-elle supersingulière ?
(4) Pourquoi sait-on en avance que θ est un générateur multiplicatif de $\mathbb{F}_8^\times$? Écrire les éléments de $\mathbb{F}_8$ comme puissance de θ.
(5) Énumérer les points de $E(\mathbb{F}_8)$.
(6) Identifier les points de $E(\mathbb{F}_8)$ d'ordre 3, et identifier le groupe $E(\mathbb{F}_8)$.
(7) Calculer la trace t du Frobenius, et donner une formule pour $|E(\mathbb{F}_{8^n})|$.

Exercice 2. On admet que 2017 est premier. On considère la courbe $E : y^2 = x^3 + 1$ sur le corps fini $\mathbb{F}_{2017}$.

(1) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique.
(2) Montrer que $\mathbb{F}_{2017}$ contient des racines 3^{mes} de l'unité.
(3) En déduire que $E(F_{2017})$ contient trois involutions.
(4) La courbe $E(\mathbb{F}_{2017})$, est-elle cyclique ? Est-elle supersingulière ?
(5) Donner une condition suffisante et nécessaire pour qu'un point (x, y) de E soit d'ordre 3.

Exercice 3. On admet que 2017 est premier. Est-ce que 1720 est un carré modulo 2017 ?

Exercice 4.

(1) Donner la définition du couplage de Weil, et ses propriétés principales.
(2) On suppose que E est une courbe elliptique sur un corps k, et que S et T dans $E(k)$ sont indépendants (c'est-à-dire si $mS+nT = \mathcal{O}$, alors $mS = \mathcal{O}$ et $nT = \mathcal{O}$). Donner l'ordre de $e_n(S, T)$ en fonction de $o(S)$ et $o(T)$.

Formulaire

Discriminant et j-invariant :

$$\begin{array}{ll} b_2 = a_1^2 + 4a_2 & b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 & b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ \Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 & j(E) = (b_2^2 - 24b_4)^3/\Delta(E). \end{array}$$

Inverse additif : $-(x, y) = (x, -y - a_1x - a_3)$.

Addition : $(x_1, y_2) + (x_2, y_2) = (x_3, y_3)$ avec

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{si } (x_1, y_1) = (x_2, y_2) \end{cases}$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3.$$