Examen Partiel - Courbes Elliptiques

Vendredi 4 décembre 2915, 9h – 11h

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.
(3) Donner la forme de Weierstrass (longue) pour une courbe elliptique.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_8$, où $\theta \in \mathbb{F}_8$ satisfait $\theta^3 + \theta + 1 = 0$.

(4) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique.
(5) Calculer θ^n comme polynôme en θ de degré au plus deux, pour $1 \leq n \leq 6$. Énumérer les points de $E(\mathbb{F}_8)$.
(6) Calculer la valeur t de la trace du Frobenius.
(7) Donner la définition de supersingulière. La courbe E, est-elle supersingulière ?
(8) Donner une formule pour $|E(\mathbb{F}_{8^n})|$ en fonction de n.
(9) $E(\mathbb{F}_8)$, est-il cyclique ?
(10) Donner un point d'ordre 3.
(11) Donner la plus petite extension $\mathbb{F}_{8^n}$ de $\mathbb{F}_8$ telle que

$$E(\mathbb{F}_{8^n})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

Formulaire

Discriminant et j-invariant :

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

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

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

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

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

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