Examen - Courbes Elliptiques

vendredi 22 janvier 2016, 8h45 – 11h45

Documents non-autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^2 + X + 1$. Construire le corps $\mathbb{F}_4$ à l'aide de θ.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_4$, où $\theta \in \mathbb{F}_4$ satisfait $\theta^2 + \theta + 1 = 0$.

(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) Énumérer les points de $E(\mathbb{F}_4)$. La courbe $E(\mathbb{F}_4)$, est-elle cyclique ?
(5) Donner la table d'addition de $E(\mathbb{F}_4)$.
[Indication : Identifier d'abord les couples $(P, -P)$.]
(6) Calculer $|E(\mathbb{F}_{1024}|$.

Exercice 2. On admet que 2017 et 1009 sont premiers. 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 supersingulière..
(2) Donner $|E(\mathbb{F}_{2017})|$. En déduire que $E(\mathbb{F}_{2017})$ est cyclique.
(3) Quels sont les ordres possibles des éléments de $E(\mathbb{F}_{2017})$?
(4) Donner tous les éléments d'ordre au plus 100.

Exercice 3. On rappelle que le couplage de Tate-Lichtenbaum est une application bilinéaire non-dégénérée

$$\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n,$$

où μ_n est le groupe de racines n-mes de l'unité. En supposant que $P \in E(\mathbb{F}_q)$ est d'ordre n premier avec $\text{pgcd}(n, q) = 1$ et $\mu_n \subseteq \mathbb{F}_q$, donner un algorithme pour transformer le problème du logarithme discrèt dans $E(\mathbb{F}_q)$ avec point de base P en problème du logarithme discrèt dans $\mathbb{F}_q^\times$. Justifier l'algorithme.
[Indication : S'inspirer de l'attaque MOV.]

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

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

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

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