Examen Partiel - Courbes Elliptiques

Vendredi 2 décembre 2016, 9h – 11h

Documents non-autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1. Quel algorithme utilisiez-vous pour trouver un facteur d'un nombre n si vous saviez que

(1) n a un petit facteur premier.
(2) n a un facteur premier p tel que $p-1$ n'a que des petits facteurs premiers (p est *powersmooth*.

Dans les deux cas, décrire l'algorithme (en pseudo-code).

Exercice 2 Décrire l'algorithme de Dixon.

Exercice 3. On considère le polynôme $P(X) = X^4 + X^3 - 1$ sur $\mathbb{F}_3$, et une racine ϑ de P dans une extension $K \geq \mathbb{F}_3$.

(1) Montrer que le polynôme $P(X) = X^4 + X^3 - 1$ est irréductible dans $\mathbb{F}_3[X]$.
(2) Construire le corps $\mathbb{F}_{81}$ à l'aide de P.
(3) Montrer que $\mathbb{F}_{81} = \mathbb{F}_3(\vartheta)$, et donner la forme des éléments de $\mathbb{F}_3(\vartheta)$.
(4) Calculer ϑ^{16} et ϑ^{40}. En déduire que ϑ est un générateur de $\mathbb{F}_{81}^{\times}$.
(5) Quels sont les sous-corps de $\mathbb{F}_{81}$? Donner une générateur sur $\mathbb{F}_3$ pour chacun.
(6) Donner ϑ^{-1}.
(7) Calculer $(1+\vartheta)^{-1}$.
(8) Résoudre le problème de logarithme discrèt $\vartheta^n = 1 + \vartheta$.