Arithmétique et applications - L3 - MI

UBO – 25 mai 2009

examen - durée : 3 heures

Tout document manuscrit ou imprimé, téléphone portable, ordinateur personnel interdit.

Partie I

Le but de cette partie est de voir sous quelle condition -1 possède une racine carrée dans un corps fini de la forme $\frac{\mathbb{Z}}{p\mathbb{Z}}$ et d'en faire le calcul.

Une condition d'existence

Supposons qu'il existe un élément y de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ tel que $y^2 = -1$. On note θ un élément primitif de $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

1. Rappeler les propriétés vérifiées par θ.
2. On note k l'entier $1 \leq k \leq p-1$ tel que $y = \theta^k$. Montrer que $4k = p-1$.
3. En déduire qu'une condition nécessaire d'existence d'une racine carrée de -1 dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est d'avoir $p \equiv 1 \bmod 4$.

On supposera remplie cette condition dans toute la suite de cette partie.

Un algorithme

On étudie une méthode pour trouver une racine carrée de -1 dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ sous la condition précitée $p \equiv 1 \bmod 4$.

1. Montrer qu'il existe m, entier impair, et $k > 1$ tel que $p - 1 = 2^k m$.
2. Soit y un élément de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ tel que $y^{2m} \neq 1$.
   On construit alors la suite finie $y_1 = y^{2m}$, $y_i = y_{i-1}^2$, i prenant les valeurs de 2 à k.
3. Montrer que $y_k = 1$.
4. Soit i_0 le plus petit indice pour lequel $y_{i_0} = 1$, $i_0 > 1$. Montrer que y_{i_0-2} est alors racine carrée de -1 dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$, si $i_0 > 2$.
5. Nous sommes donc ramenés à la recherche d'un élément $y \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ tel que $y^{2m} \neq 1$. Ceci se fait simplement par tirage au hasard.
   Combien l'équation $X^{2m} = 1$ a-t-elle de solutions dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$?
6. Quelle est alors la probabilité, par tirage au hasard dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$, de trouver un élément y tel que $y^{2m} \neq 1$.
7. Exemple : soit $p = 2113$, en utilisant les idées précédentes, trouver une racine de -1 dans $\frac{\mathbb{Z}}{2113\mathbb{Z}}$.
8. Écrire alors le pseudo-code d'un algorithme qui prend en entrée $p \equiv 1 \bmod 4$ et qui retournera une racine carrée de -1 avec une probabilité supérieure à $1 - \frac{1}{2^{20}}$ c'est-à-dire quasi-certainement !
   Quel en est le coût binaire au pire de cet algorithme ?

Partie II

Exercice 1

Soit f le polynôme dans $\mathbb{Q}[X]$ défini par

$$f(X) = X^5 - X^3 + 3X^2 - 2X + 1.$$

En utilisant l'algorithme de Schubert-Kronecker, décomposer f en facteurs irréductibles dans $\mathbb{Q}[X]$.

Exercice 2

Soit $m(X) = X^7 + X + 1 \in \mathbb{F}_2[X]$.

1. Montrer que m est irréductible dans $\mathbb{F}_2[X]$.
2. Soit $K = \mathbb{F}_2[X]/m$, et notons $\alpha = X \bmod m$. Quel est le cardinal de K ?
3. L'élément α de $K^\star$ est-il générateur ?
4. Déterminer les sous-corps de K.
5. Déterminer les racines de m dans K.
6. Décomposer m dans $K[X]$.
7. Quel est le polynôme minimal n de α^3 sur $\mathbb{F}_2$?
8. Déterminer les racines de n dans K.
9. Décomposer n dans $K[X]$.
10. Quel est le nombre de polynômes irréductibles de degré 7 dans $\mathbb{F}_2[X]$?

Exercice 3

Déterminer le plus petit corps $\mathbb{F}_q$ de la forme $\mathbb{F}_2[\alpha]$ où α n'est pas générateur du groupe multiplicatif $\mathbb{F}_q^\star$.