Master CSI 1 2021-2022

Arithmétique : Examen du 16 décembre 2021

Master Sciences et Technologies, mention Mathématiques ou Informatique, parcours Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

Durée : 3h. Sans document. Les exercices sont indépendants.

– Exercice 1. Soit A l'anneau $\mathbb{F}_2[X]/(X^4+X^2+1)$.

a) Combien A contient-il d'éléments ? Combien d'éléments contient le groupe A^* des éléments inversibles de A ?

b) Montrer qu'il y a dans A^* quatre éléments dont le carré vaut 1.

c) Dans un groupe cyclique $(G,\times)$ noté multiplicativement, combien y a-t-il au maximum d'éléments g tels que $g^2=1$? En déduire que $(A^*,\times)$ n'est pas cyclique.

d) Quel est l'ordre maximal d'un élément de A^* ? Donner un exemple d'un tel élément.

– Exercice 2.

a) Quels sont les degrés des facteurs irréductibles de $X^{25}+1$ dans $\mathbb{F}_2[X]$?

b) En écrivant que $X^{25}=(X^5)^5$, et en utilisant la décomposition de X^5+1 en facteurs irréductibles dans $\mathbb{F}_2[X]$, trouver la décomposition en facteurs irréductibles de $X^{25}+1$.

c) Combien l'anneau $A=\mathbb{Z}/125\mathbb{Z}$ a-t-il d'éléments inversibles ?

d) Calculer 2^{20} et 2^{50} dans A et en déduire que 2 est un générateur du groupe multiplicatif des éléments inversibles de A.

e) En déduire la décomposition en facteurs irréductibles de $X^{125}+1$.

– Exercice 3. On considère la suite binaire $a=(a_i)_{i\geqslant 0}$ engendrée par la récurrence linéaire

$$a_i = a_{i-2}+a_{i-3}$$

et commençant par $a_0=a_1=a_2=1$. Écrire la suite a sous sa forme algébrique $a_i=\mathrm{Tr}(\alpha^{i+k})$ où Tr() désigne l'application trace de $\mathbb{F}_8$ dans $\mathbb{F}_2$ et où k est un entier à déterminer.

– Exercice 4. Soit n un entier de la forme $n=2^m+1$.

a) Montrer que $\mathbb{F}_{2^{2m}}$ est la plus petite extension de $\mathbb{F}_2$ dans laquelle il existe un élément α d'ordre n.

b) Soit $P(X)$ le polynôme minimal d'un tel α. Montrer que α^{-1} est une racine de $P(X)$.

c) Soit $g(X) = (X+1)P(X)$. Pourquoi $g(X)$ est-il le polynôme générateur d'un code cyclique C de longueur n ? Quelle est la dimension de ce code ?

d) Étudier les racines de $g(X)$ pour en déduire que la distance minimale de C est au moins 6.

– Exercice 5. On considère le polynôme $g(X) = (X^3+X+1)(X^4+X+1) = X^7+X^5+X^3+X^2+1$ dans $\mathbb{F}_2[X]$.

a) Quelle est la plus petite extension de $\mathbb{F}_2$ dans laquelle $g(X)$ a une racine ?

b) Quelle est la plus petite extension de $\mathbb{F}_2$ dans laquelle $g(X)$ a 7 racines ?

c) Montrer que 105 est le plus petit entier n tel que $g(X)$ soit le polynôme générateur d'un code cyclique de longueur n.

d) Montrer que toute suite (a_i) satisfaisant la récurrence linéaire sur $\mathbb{F}_2$

$$a_i = a_{i-2} + a_{i-4} + a_{i-5} + a_{i-7} \tag{1}$$

a pour période 105 ou un diviseur de 105.

e) Soit $h(X) = (X^{105}+1)/g(X)$. Quelle est la dimension du code cyclique C de longueur 105 de polynôme générateur $h(X)$?

f) Montrer que le polynôme $G(X) = (X^4+X+1)h(X)$ s'écrit sous la forme

$$G(X) = (1+X+X^2+X^4)(1+X^7+X^{14}+\cdots+X^{7i}+\cdots+X^{7.14}).$$

g) Montrer que le sous-code cyclique de C de polynôme générateur $G(X)$ a pour mots non nuls des mots de la forme $(x, x, \ldots, x)$ où x est un septuplet répété 15 fois.

h) Donner un exemple de suite de période 7 vérifiant la récurrence linéaire (1).

i) Donner un exemple de suite de période 15 vérifiant la récurrence linéaire (1).