Master CSI 1 — 2019-2020

Arithmétique : Examen du 12 décembre 2019

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. On considère le polynôme $X^3 - X^2 + 1$ dans $\mathbb{F}_3[X]$.

a) Donner une relation de récurrence linéaire dont $X^3 - X^2 + 1$ est le polynôme de rétroaction.

b) Donner explicitement une suite ternaire engendrée par cette récurrence linéaire : quelle est sa période ?

c) Que peut-on en déduire sur la nature du polynôme $X^3 - X^2 + 1$?

d) Soit α une racine de $X^3 - X^2 + 1$ dans $\mathbb{F}_{27}$. Donner la suite $(\mathrm{Tr}(\alpha^i))_{i \geqslant 0}$.

– EXERCICE 2. Soit α un élément d'ordre 33 dans une extension de $\mathbb{F}_2$. Quel est le degré du polynôme minimal de α dans $\mathbb{F}_2[X]$?

– EXERCICE 3. Utilisez ce que vous savez sur les corps finis pour montrer que si p est premier alors $2^{p-1} - 1$ est divisible par p.

– EXERCICE 4. Soit $f(X) = X^7 + X^3 + 1$ dans $\mathbb{F}_2[X]$.

a) Étudier les valeurs de X^{2^i}, $i = 1, 2, \ldots$, modulo $Xf(X)$ et en déduire que $f(X)$ est irréductible.

b) Montrer que l'ensemble des racines de $f(X)$ dans $\mathbb{F}_{128}$ augmenté de 0 forme un espace vectoriel sur $\mathbb{F}_2$. Quel est sa dimension ?

– EXERCICE 5.

a) Montrer que le polynôme $X^5 + X^2 + 1$ est irréductible dans $\mathbb{F}_2[X]$. Est-il primitif ?

b) Soit α une racine de $X^5 + X^2 + 1$ dans $\mathbb{F}_{32}$. Trouver le polynôme minimal de α^3.

– EXERCICE 6.

a) Combien le polynôme $X^{17} + 1$ a-t-il de facteurs irréductibles dans $\mathbb{F}_2[X]$?

b) Montrer que si α est une racine d'un facteur irréductible de $\mathbb{F}_2[X]$ (dans une extension appropriée de $\mathbb{F}_2$), alors α^{-1} l'est aussi.

c) En déduire le degré du polynôme minimal de $\alpha + \alpha^{-1}$.

d) En parcourant les polynômes minimaux possibles pour $\alpha + \alpha^{-1}$, en déduire explicitement les facteurs irréductibles de $X^{17} + 1$.

e) Soit $g(X) = (X+1)P(X)$ où $P(X)$ est un facteur irréductible de $X^{17}+1$. On considère le code cyclique C de longueur 17 de polynôme générateur $g(X)$. Quelle est la dimension de C ?

f) En exhibant 5 racines judicieusement choisies de $g(X)$ montrer que la distance minimale de C est au moins 6.

g) Caractériser les multiples de $X+1$. En déduire que tous les mots de C sont de poids pair.

h) On représente le n-uple $u = (u_0, u_1, \ldots, u_{n-1})$ par le polynôme $u(X) = u_0 + u_1 X + \cdots + u_{n-1}X^{n-1}$. Soit α une racine de $g(X)$ différente de 1. Supposons $u(\alpha) = a$ et $u(\alpha^{-1}) = b$. Montrer que si $u = c + e_i + e_j$, où c est un mot du code C, c'est-à-dire si u est obtenu à partir d'un mot du code en modifiant les symboles de coordonnées i et j, alors α^i et α^j sont des racines du polynôme :

$$X^2 + aX + ab^{-1}.$$

i) Montrer que la distance minimale de C est exactement 6.

j) Soit C' le code de polynôme générateur $P(X) = g(X)/(X+1)$. Quelle est la dimension de C' ? Montrer que sa distance minimale vaut 5.