Master CSI 1 — 2023-2024

Arithmétique : Examen du 18 décembre 2023

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 α un élément d'ordre 9 dans une extension de $\mathbb{F}_2$.

a) Quel est le degré du polynôme minimal de α dans $\mathbb{F}_2[X]$?

b) Quel est le polynôme minimal de α dans $\mathbb{F}_2[X]$?

c) Soit $\beta = \alpha + \alpha^{-1}$. Montrer que β est dans le sous-corps à 8 éléments de $\mathbb{F}_2(\alpha)$.

d) Quel est le polynôme minimal de β ?

– EXERCICE 2. Soit α un élément du corps $\mathbb{F}_{2^m}$ à 2^m éléments. On considère le polynôme $X^2 + X + \alpha$.

a) Montrer que si $X^2 + X + \alpha$ a au moins une racine β dans $\mathbb{F}_{2^m}$ alors il a exactement deux racines, soit β et $\beta + 1$, dans $\mathbb{F}_{2^m}$.

b) Montrer que si $X^2 + X + \alpha$ a une racine dans $\mathbb{F}_{2^m}$, alors $\mathrm{Tr}(\alpha) = 0$, où $\mathrm{Tr}()$ désigne l'application trace de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2$.

c) Montrer que lorsque t parcourt $\mathbb{F}_{2^m}$, l'expression $t + t^2$ parcourt un ensemble à 2^{m-1} éléments.

d) Combien y a-t-il d'éléments de $\mathbb{F}_{2^m}$ de trace nulle ?

e) En déduire que $X^2 + X + \alpha$ a une racine dans $\mathbb{F}_{2^m}$ si et seulement si $\mathrm{Tr}(\alpha) = 0$.

f) On réalise le corps à 16 éléments comme $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ où α est une racine du polynôme $X^4 + X + 1$. Trouver les racines de $X^2 + X + \alpha$: on les cherchera sous la forme $a + b\alpha + c\alpha^2 + d\alpha^3$ où $a, b, c, d \in \mathbb{F}_2$.

– EXERCICE 3. On représente tout 7-uple binaire $(c_0, c_1, \ldots, c_6)$ par le polynôme $c(X) = c_0 + c_1X + \cdots + c_6X^6$. Soit C le code cyclique de polynôme générateur $g(X) = X^3 + X + 1$.

a) Quelle est la dimension de C ? Quelle est sa distance minimale ?

b) Montrer que le n-uple (1001011) est un mot de C. Quel est le mot de C le plus proche de (1100010) ?

c) Donner le polynôme générateur $h(X)$ du code orthogonal $C^\perp$ de C.

d) Quelle est la distance minimale de $C^\perp$?

– EXERCICE 4. On réalise le corps à 16 éléments comme l'extension $\mathbb{F}_2(\alpha)$ de $\mathbb{F}_2$ où α est une racine du polynôme $X^4 + X + 1$.

a) Quelle est la période des suites binaires solutions de la récurrence linéaire

$$a_i = a_{i-1} + a_{i-2} + a_{i-3} + a_{i-4} \ ?$$

b) Donner une de ces solutions (a_i) sous la forme $\mathrm{Tr}(\beta^i)$ où β est un élément de $\mathbb{F}_2(\alpha)$ judicieusement choisi, et où $\mathrm{Tr}()$ désigne l'application trace de $\mathbb{F}_{16}$ vers $\mathbb{F}_2$.

c) Donner deux autres solutions (b_i) et (c_i) de la récurrence sous la forme $b_i = \mathrm{Tr}(x\beta^i)$ et $c_i = \mathrm{Tr}(y\beta^i)$ où $x, y \in \mathbb{F}_2(\alpha)$ et de sorte qu'aucune des suites binaires $(a_i), (b_i), (c_i)$ ne soit la décalée circulaire d'une autre.

– EXERCICE 5. Soit le polynôme $g(X) = (X^3+X+1)(X^4+X^3+X^2+X+1) = X^7 + X^6 + X^4 + X^3 + 1$ dans $\mathbb{F}_2[X]$.

a) Quel est la plus petite extension de $\mathbb{F}_2$ dans laquelle $g(X)$ se factorise en facteurs de degrés 1 ?

b) Quel est le plus petit n pour lequel il existe un code cyclique C de longueur n et de polynôme générateur $g(X)$? Quelle est la dimension de ce code ?

c) Donner les degrés des facteurs irréductibles sur $\mathbb{F}_2$ de $X^{35} + 1$.

d) Écrire $X^{35} + 1$ sous la forme $(X^5)^7 + 1$, en déduire une première décomposition de $X^{35} + 1$ en produit d'un facteur de degré 5 et de deux facteurs de degrés 15, puis factoriser les deux polynômes de degré 15 pour trouver la décomposition en facteurs irréductibles sur $\mathbb{F}_2$ de $X^{35} + 1$.