UNIVERSITÉ de BORDEAUX

ANNÉE UNIVERSITAIRE 2014/2015

Session 1 d'Automne

Master Sciences et Technologies, Mention Mathématiques ou Informatique

Spécialité Cryptologie et Sécurité Informatique

UE M1MA7W01 : Arithmétique

Responsable : M. Jean-Paul Cerri

Date : 15/12/2014. Durée : 3h.

Exercice 1 – Soit A l'anneau $\mathbb{F}_{11}[X]/(X^3+2X^2+2X+2)$.

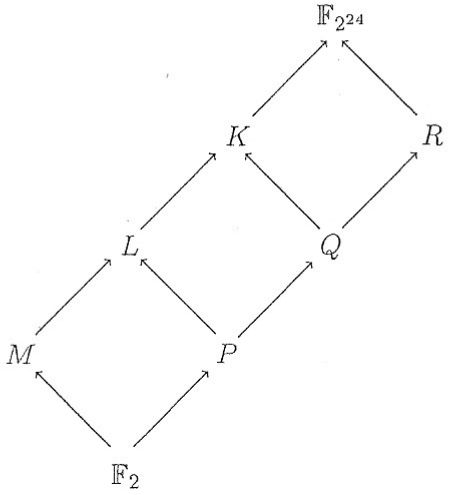
1) Montrer que A n'est pas un corps.

2) Dans $\mathbb{F}_{11}[X]$ combien y a-t-il de polynômes de degré $\leqslant 1$ premiers avec $X-2$?

3) À l'aide du théorème chinois, déterminer le cardinal de $A^\times$.

Exercice 2 –

1) Figure ci-dessous le schéma des sous-corps de $\mathbb{F}_{2^{24}}$. Dans ce schéma $A \longrightarrow B$ signifie que A et B sont des sous-corps de $\mathbb{F}_{2^{24}}$ vérifiant $A \subsetneq B$ et qu'il n'y a pas de sous-corps C de $\mathbb{F}_{2^{24}}$ vérifiant $A \subsetneq C \subsetneq B$.



Préciser quels sont les corps K, L, M, P, Q, R.

2) Que valent les degrés $[Q : P]$, $[K : P]$, $[\mathbb{F}_{2^{24}} : P]$?

3) Soit α un élément primitif de $\mathbb{F}_{2^{24}}$. Déterminer des entiers a, b, c tels que $P = \mathbb{F}_2(\alpha^a)$, $L = \mathbb{F}_2(\alpha^b)$, $K = \mathbb{F}_2(\alpha^c)$.

Exercice 3 – Soit α un élément primitif de $\mathbb{F}_4$. On a alors $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$. Soit M la matrice de $M_{3\times 9}(\mathbb{F}_4)$ définie par

$$M = \begin{pmatrix} \alpha & 0 & 0 & 1+\alpha & 0 & 0 & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 1+\alpha & 0 & 0 & 1 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 1+\alpha & 0 & 0 & 1 \end{pmatrix}$$

1) Montrer que les lignes de cette matrice sont linéairement indépendantes sur $\mathbb{F}_4$.

2) On considère le code linéaire $\mathcal{C} \subseteq \mathbb{F}_4^9$ de matrice génératrice M.
Montrer que $(1, 0, 0, \alpha, 0, 0, 1+\alpha, 0, 0) \in \mathcal{C}$ et en déduire que $\mathcal{C}$ est cyclique.

3) Quelle est la dimension k de $\mathcal{C}^\perp$ le code dual de $\mathcal{C}$?

4) Trouver k éléments de $\mathcal{C}^\perp$ linéairement indépendants sur $\mathbb{F}_4$ et en déduire une matrice de contrôle de $\mathcal{C}$.

5) Quels sont les paramètres de $\mathcal{C}$ et $\mathcal{C}^\perp$?

Exercice 4 –

1) Combien y a-t-il de polynômes irréductibles de degré 10 dans $\mathbb{F}_2[X]$?

2) Combien y a-t-il de polynômes irréductibles primitifs de degré 10 dans $\mathbb{F}_2[X]$?

Soit $n \geqslant 2$ un entier.

3) Montrer que si $2^n - 1$ est premier alors n est premier.

4) On suppose désormais que $2^n - 1$ est premier. Soit $\alpha \in \mathbb{F}_{2^n}$ différent de 0 et 1. Montrer que α est un élément primitif de $\mathbb{F}_{2^n}$.

5) Combien y a-t-il de polynômes irréductibles de degré n dans $\mathbb{F}_2[X]$?

6) Montrer que tous ces polynômes sont primitifs.

7) On considère la suite $(s_i)_{i\geqslant 0}$ définie par $(s_0, s_1, s_2, s_3, s_4) = (1, 0, 0, 0, 0)$ et par la relation de récurrence linéaire $s_{i+5} = s_{i+2} + s_i$ pour tout $i \geqslant 0$. Expliquer, sans calculer les premiers termes de cette suite, pourquoi il s'agit d'une MLS. Quelle est sa période ?

8) On considère le polynôme $P(X) = X^5 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Montrer qu'il est irréductible primitif.

9) Soit $\alpha \in \mathbb{F}_{32}$ une racine de $P(X)$. Exprimer les racines de $P(X)$ comme combinaisons linéaires de la forme $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$ où les a_i sont des éléments de $\mathbb{F}_2$.

10) Soit $\mathcal{H}$ le code de Hamming de longueur 31 engendré par $P(X)$. Quels sont les paramètres de $\mathcal{H}$? Le code $\mathcal{H}$ est-il un code MDS ?

11) On désire améliorer l'ordre de la condition de décodage de $\mathcal{H}$. On considère le code BCH défini par $\mathcal{H}' = \{Q(X) \in \mathbb{F}_2[X]/(X^{31} + 1);\ Q(\alpha) = Q(\alpha^3) = 0\}$. Pourquoi le polynôme minimal de α^3, noté $R(X)$ est-il de degré 5 et distinct de $P(X)$?

12) Déterminer $R(X)$.

13) On rappelle que $\mathcal{H}'$ est un code cyclique. Quel est son polynôme générateur ?

14) Quels sont les paramètres de $\mathcal{H}'$? Ce nouveau code est-il MDS ?

Exercice 5 –

1) Montrer que $P(X) = X^6 + X^5 + 1$ est un polynôme irréductible de $\mathbb{F}_2[X]$.

2) Expliquer pourquoi $P(X)$ divise le polynôme $X^{63} + 1$ dans $\mathbb{F}_2[X]$.

3) Le polynôme $P(X)$ est-il primitif ?

4) Soit α une racine de $P(X)$ dans $\mathbb{F}_{64}$. On considère la suite $(s_i)_{i\geqslant 0}$ à éléments dans $\mathbb{F}_2$ définie par $s_i = \mathrm{Tr}(\alpha^i)$. Rappeler pourquoi (s_i) est définie par une relation de récurrence linéaire que l'on explicitera.

5) Montrer que (s_i) est périodique et qu'il s'agit d'une MLS (maximum length sequence) de période π à préciser.

6) On considère l'ensemble $\mathcal{C}$ dont les éléments sont :

- le π-uplet $(s_0, s_1, \ldots, s_{\pi-2}, s_{\pi-1})$,
- ses $\pi - 1$ décalés $(s_{\pi-1}, s_0, \ldots, s_{\pi-3}, s_{\pi-2}), \ldots, (s_1, s_2, \ldots, s_{\pi-1}, s_0)$,
- le π- uplet nul $(0, 0, \ldots, 0, 0)$.

Montrer que $\mathcal{C}$ est un code linéaire. Quelle est sa dimension ?

7) Montrer que $\mathcal{C}$ est un code cyclique.

8) Montrer que $\mathcal{C}$ est le code dual du code cyclique de longueur π engendré par $P(X)$.

9) En déduire le polynôme générateur de $\mathcal{C}$. On pourra admettre que dans $\mathbb{F}_2[X]$,

$$\frac{X^{63}+1}{X^6+X^5+1} = 1 + X^5 + X^6 + X^{10} + X^{12} + X^{15} + X^{16} + X^{17} + X^{18} + X^{20} + X^{24} + X^{25} + X^{26} + X^{29} + X^{32} + X^{34} + X^{35} + X^{37} + X^{38} + X^{39} + X^{41} + X^{42} + X^{45} + X^{46} + X^{48} + X^{50} + X^{52} + X^{53} + X^{54} + X^{55} + X^{56} + X^{57}.$$

10) Quels sont les paramètres du code dual de $\mathcal{C}$?