UNIVERSITÉ BORDEAUX 1 Sciences Technologies

ANNÉE UNIVERSITAIRE 2011/2012
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 : 14/12/2011. Durée : 3h.

Les exercices 4 et 5 sont fortement liés mais peuvent être faits indépendamment.

Exercice 1 – On considère dans $\mathbb{F}_7[X]$ le polynôme $P(X) = X^2 + 2X + 6$ et on note A l'anneau $\mathbb{F}_7[X]/(P(X))$.

1) Quelle est la caractéristique de A ? Quel est le cardinal de A ?

2) L'anneau A est-il un corps ?

3) Quel est le cardinal du groupe multiplicatif $A^\times$?

4) Montrer que tout $a \in A$ vérifie $a^7 = a$.

5) Le groupe $A^\times$ est-il cyclique ?

Exercice 2 –

1) En utilisant les polynômes $X^9 - X$ et $X^{81} - X$ déterminer le nombre de polynômes unitaires irréductibles de degrés 2 et 4 dans $\mathbb{F}_3[X]$.

2) Dans chaque cas, quel est le nombre de polynômes primitifs ?

Exercice 3 – Combien la décomposition en produit d'irréductibles de $X^{21} + 1$ dans $\mathbb{F}_2[X]$ comporte-t-elle de facteurs ? Quels sont leurs degrés respectifs ?

Exercice 4 –

1) Montrer que $P(X) = X^4 + X^3 + 1$ est un polynôme irréductible de $\mathbb{F}_2[X]$. Est-il primitif ?

2) Soit α une racine de $P(X)$ dans $\mathbb{F}_{16}$. On pose $\beta = \alpha^3$. L'élément β est-il primitif dans $\mathbb{F}_{16}$?

3) Quels sont les sous-corps de $\mathbb{F}_{16}$? L'élément β appartient-il à un sous-corps strict de $\mathbb{F}_{16}$?

4) Mêmes questions avec l'élément $\gamma = \alpha^5$.

5) 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.

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

7) 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 $(s_{\pi-1}, s_0, \ldots, s_{\pi-3}, s_{\pi-2}), \ldots, (s_1, s_2, \ldots, s_{\pi-1}, s_0)$ et le π- uplet nul $(0, 0, \ldots, 0, 0)$. Montrer que $\mathcal{C}$ est un code linéaire.

8) Montrer que $\mathcal{C}$ est un code cyclique et déterminer sa dimension.

9) Quel est le polynôme générateur de $\mathcal{C}$.

10) Quelle est la distance minimale de $\mathcal{C}$?

Exercice 5 – Soit $P(X) = X^4 + X + 1$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{F}_2[X]$ et rappeler pourquoi $P(X)$ divise $X^{15} + 1$ dans $\mathbb{F}_2[X]$ sans avoir recours à la division euclidienne.

2) À tout 15-uplet binaire $\mathbf{c} = (c_0, c_1, \ldots, c_{14}) \in \mathbb{F}_2^{15}$ on associe le polynôme $\mathbf{c}(X) = c_0 + c_1 X + \cdots c_{14} X^{14} \in \mathbb{F}_2[X]$. On considère le code $\mathcal{C}$ constitué par les $\mathbf{c}$ tels que $\mathbf{c}(X)$ soit un multiple de $P(X)$. Expliquer pourquoi $\mathcal{C}$ est cyclique et déterminer sa dimension.

3) Montrer que $\mathcal{C}$ est un code de Hamming.

4) Sachant qu'un code de Hamming a pour distance minimale 3 (théorème du cours), quel est l'ordre de la condition de décodage vérifiée par $\mathcal{C}$?

5) ~~Montrer que $\mathcal{C}^\perp$ code dual de $\mathcal{C}$ est aussi un code de Hamming et déterminer ses paramètres.~~

6) Soit α une racine de $P(X)$ dans $\mathbb{F}_{16}$. Quel est le polynôme minimal sur $\mathbb{F}_2$ de α^3 ? On note ce polynôme $Q(X)$.

7) On considère maintenant le code $\mathcal{C}'$ constitué des 15-uplets $\mathbf{c}$ tels que $\mathbf{c}(\alpha) = \mathbf{c}(\alpha^3) = 0$. Montrer que $\mathcal{C}'$ est cyclique. Déterminer sa dimension et son polynôme générateur.

8) L'ordre de la condition de décodage de $\mathcal{C}'$ est-il meilleur que celui de $\mathcal{C}$?

Exercice 6 – On considère le code de Reed-Solomon C défini sur $\mathbb{F}_5$ de longueur 4, de dimension 2 et de matrice génératrice

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

On a pris 2 pour élément primitif de $\mathbb{F}_5$. On sait que C est MDS (théorème du cours), donc que sa distance minimale est 3. C vérifie donc la condition de décodage d'ordre 1.

1) Un mot c est envoyé à l'aide du polynôme $P(X)$ de degré < 2. On reçoit le mot $(4, 2, 0, 0)$. Calculer le polynôme interpolateur $R(X) \in \mathbb{F}_5[X]$ de degré $\leqslant 3$ qui vérifie $R(1) = 4$, $R(2) = 2$, $R(4) = 0$ et $R(3) = 0$.

2) À l'aide du début du développement en fraction continue de $\frac{R(X)}{X^4-1}$, retrouver $P(X)$ et le mot envoyé.